Cybersecurity: a Navy and CSUCI collaboration

Socrates Frangis, Jorge Lacoste, Michael Soltys

February 5, 2021

Abstract

This whitepaper is a result of active collaboration between the Naval Surface Warfare Center, Port Hueneme Division and Dr. Michael Soltys from the California State University Channel Islands. This paper was developed in part during the Office of Naval Research, Summer Faculty Research Program while Professor Soltys was engaged with Cyber Security Leadership at the Command. This paper summarizes the need for cyber security professionals in the Navy workforce and provides potential methods in which the California State University Channel Islands and the Naval Surface Warfare Center Port Hueneme Division can leverage the existing Education Partnership Agreement as well as potential other contract mechanisms to further the mutual goals of the organizations. Additionally reccomendations are provided to create opportunities of scholarship and employment for graduating students.

Contents

1 Introduction

Over the last decades the demand for Cybersecurity professionals has grown steadily, and has now reached a critical point. In the state of California there are currently 35,000 unfilled positions in Cybersecurity and most companies, both in the private and public sector, are struggling to hire. The situation is similar nation-wide, with about 1.2 million unfilled positions, and world-wide, with about 3.5 million unfilled positions ([1]).

This paper tackles the above problem at a local level. It is the desired intent to attract Cybersecurity trained personnel to the Naval Sea Systems Command (NAVSEA), Naval Surface Warfare Center (NSWC), Port Hueneme Division (PHD) from the regional university, California State University Channel Islands (CSUCI), from the community colleges in the area, and indeed from anywhere. Ventura County candidates have the advantage of having roots in the area, and are accustomed to the high cost of living in SoCal, and therefore make long-term commitments when starting a job at PHD.

In this paper, the authors heed the admonition in the California Cybersecurity Workforce Development and Education Strategy[1] (CCWDES) [2]:

> *To be successful, public and private sector key partners/major stakeholders must collaborate and work together earnestly to design education and workforce development programs that assure prospective employers program graduates can demonstrate the necessary knowledge, skills, abilities, and competencies to get the job done upon pipeline/pathway graduation.*

The needs of the Navy are examined, the Cybersecurity related career pathways in the Navy, as well as the Cybersecurity offering at CSUCI, and recommendations presented for creating a bridge from CSUCI graduates to a Navy Cybersecurity work-force.

1.1 Paper context and history

The first version of this paper was produced during the summer 2020, while Soltys was an “Office of Naval Research” (ONR) fellow with NAVSEA at PHD. One of the projects undertaken during the fellowship was a collaboration with Socrates Frangis, Director of Afloat Cybersecurity at PHD,

[1] The third author is on the CCWDES committee.

who proposed the writing of a whitepaper on Navy Cybersecurity work-force development. The paper highlights the collaboration between PHD, and CSUCI especially the department of Computer Science (CS), where Soltys is a professor and chair.

The collaboration between PHD and CSUCI dates back to an educational agreement between the two institutions crafted in 2014 [3].

1.2 What is Cybersecurity?

Cybersecurity, also called Information Security, is a burgeoning field of Computer Science (CS). It focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change, or destruction. It is an interdisciplinary field which is traditionally housed under Computer Science, but additionally spans Engineering, Information Technology, Mathematics, Management, Psychology, Social Sciences and Law.

2 Background

The intent of this section is to provide a background of NSWC PHD, its role in the United States Navy (USN) enterprise, how cybersecurity activities are organized, and the type of cybersecurity work done at the warfare center.

2.1 NSWC Port Hueneme Division

Like many large enterprises, the USN is composed in a hierarchy of sub-organizations each focused on the execution of a certain mission. One such sub-division of the USN are called the system commands (SYSCOM). These are material agencies responsible for the design, construction, and maintenance of facilities, ships, and systems.

NAVSEA is a SYSCOM particularly focused on surface and sub-surface vessels, their weapons, sensors, and vehicles. Additionally, NAVSEA has sub-organizations known as warfare center divisions, where each division specializes in certain weapons, sensors, and vehicles and their role in the defense acquisition life-cycle. PHD's mission focuses on surface weapon systems, combat systems, radars, underway replenishment systems, their formal test and evaluation, logistics, and sustainment throughout the systems life-cycle until retirement. This means the workforce at PHD has a unique role in the acceptance, maintenance, issue resolution, and modernization of these systems.

PHD is therefore designated as the In Service Engineering Agent (ISEA) of the systems they support, not just from an engineering perspective, but with Fleet engagement as well. The workforce is therefore distributed and works in an variety of office, lab, industrial, and boots on deck in an operational shipboard environment alongside Sailors. Additionally the workforce is diverse and encompasses a multitude of roles, from military, to contractors, to civil servants. A common misconception is that everyone who works for the Navy is an officer or enlisted member of the military. A multitude of the work and jobs available at NSWC PHD, are actually civil servant positions.

2.2 Navy Control Systems

While PHD is focused on specific types of systems (e.g., combat systems, weapon systems, radars, underway replenishment systems), generically these are categorized by NAVSEA as Navy Control Systems (NCS). This is partly due to their function as well as mixture of component types at the subsystem level. Information Technology (IT) typically consists of servers, network switches, and end user workstations. Their primary functions is to store, transmit, and process data. Similarly Operational Technology (OT) is a combination of hardware and software that detects or causes state change, through direct monitoring or control of industrial equipment, typically composed of program logic controllers (PLC), industrial control systems (ICS), and supervisory control and data acquisition systems (SCADA).

The culmination of IT and OT in a shipboard environment is referred to as NCS. For example, one can imagine a sailor at a fire control workstation engaging a target to activate a gun weapon system. This extends beyond the workstation computer, through networking equipment, to servers, to SCADA systems, to ICS and PLC which mechanically move the gun to a firing solution. Therefore the application of systems engineering and cybersecurity, is unique in that it involves multiple types of system components and disciplines to sustain it throughout the life-cycle.

2.3 DoD Cyber Workforce Framework

A general description of the type of work performed at NSWC PHD for cybersecurity, can be grouped in the Department of Defense (DoD) Cyber

Workforce Framework taxonomy. The DoD Cyber Workforce Framework (DCWF) establishes the DoD's authoritative lexicon based on the work an individual is performing, not their position titles, occupational series, or designator. The DCWF describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01.

The DCWF leverages the original National Initiative for Cybersecurity Education (NICE), National Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCTCS).[2] Below, an application of the DCWF is listed below in context with traceability to the categories and specialty areas.

2.4 Cybersecurity Knowledge Elements of NCS at PHD

Overall the NSWC PHD ISEAs provide cybersecurity engineering support to ensure that the security requirements of systems are met. This includes, but is not limited to, assessing existing system vulnerabilities and determining mitigation strategies; support systems security architecture and design analysis, system implementation assessment, penetration testing, assessment and authorization, and risk management; determine the feasibility and impact to systems when engineering changes, software mod and security fixes are applied; ensure cybersecurity tools are operational to maintain cybersecurity baseline through deployment cycle; provide onsite and distance support to cybersecurity incidents; support cybersecurity training and manning; develop/update technical manuals, operating manuals, and maintenance procedures to include cybersecurity.

In alignment, this shows overall that the workforce aligns closely to the DCWF lexicon for Operate & Maintain, Oversee & Govern, Protect & Defend, and Securely Provision.

2.4.1 Security Engineering

Security Engineering refers to the approach of integrating cybersecurity in the systems engineering life-cycle. The DCWF work roles which align to this knowledge area are Systems Developer, Systems Administrator, Network Operations Specialist, Systems Security Analyst, and Cyber Defense Infrastructure Support:

[2] Reference https://public.cyber.mil/cw/dcwf/ .

- Provide cybersecurity engineering support to ensure that the security requirements of systems are met
- Assess existing system vulnerabilities and determine mitigating strategies
- Support systems security architecture and design analysis, system implementation assessment, security test and evaluation, assessment and authorization, and risk management
- Determine the feasibility and impact to systems when engineering changes, software mod and security fixes are applied
- Ensure cybersecurity tools are operational to maintain the security baseline through deployment cycle
- Provide onsite and distance support to cybersecurity incidents
- Support cybersecurity training and manning
- Develop/update technical manuals, operating manuals, and maintenance procedures to include cybersecurity.

2.4.2 Security Test & Evaluation

Security Test & Evaluation refers to the verification and validation of cybersecurity requirements in addition to characterization, vulnerability assessments, and penetration testing. The DCWF work roles which align to this knowledge area are the System Testing and Evaluation Specialist:

- Develop and conduct security tests afloat and ashore, including interoperability, of systems to evaluate compliance with Risk Management Framework
- Ensure requirements for cybersecurity testing are in the Test and Evaluation Master Plan (TEMP) and Operational Test plans
- Table top scenarios
- characterize attack surface
- cooperative vulnerability identification, adversarial cybersecurity developmental testing, penetration assessment.

2.4.3 Security Incident Response

Security Incident Response refers to direct Fleet Support, responding to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. The DCWF work roles which align to this knowledge area are the Cyber Defense Incident Responder:

- Respond to urgent incidents from combat systems to contain, eradicate, recover and restore systems to operational states
- Coordinate with and provide technical support to Fleet to resolve incidents
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.

2.4.4 Security RMF Vulnerability Assessment and Management

The Risk Management Framework (RMF) Vulnerability Assessment and Management refers to implementing technical statutory controls and includes the assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy. DCWF work roles which align to this knowledge area are the Vulnerability Assessment Analyst:

- Conduct assessments of threats and vulnerabilities, determine deviations from ATO security baseline, assess the level of risk, and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations
- Support the selection of security controls to mitigate risk
- Sustainment of systems through patches, antivirus, and malware definition updates being installed in labs in addition to Fleet media distribution for Navy Control Systems.

2.4.5 Security Development & Operations (SecDevOps)

The Security Development & Operations (SecDevOps) refers to the streamlined integration from development, to automated security review, to staging for operational test. The DCWF work roles which align to this knowledge area are the Software Developer:

- Secure coding implementation and source code review

- Execution of both static analysis and dynamic analysis to identify potential software defects or vulnerabilities. Overall integration and execution of secure coding practices to development and deployment of software.

2.4.6 Security Education and Training

Security Education and Training refers to conducting training of personnel within pertinent subject domain as well as developing systems to deliver training. It develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate. The DCWF work roles which align to this knowledge area are the Cyber Instructional Curriculum Developer, Cyber Instructor, Systems Developer, and Software Developer.

- Conduct interactive training exercises to create an effective learning environment; correlate mission requirements to training; deliver

- Training courses tailored to the audience and physical environment design training curriculum and course content; write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce

- Support the design and execution of exercise scenarios

- Design and support embedded or schoolhouse training systems for the purposes of building and maintaining perishable cyber hygiene and incident response skill-sets

2.5 Cybersecurity at CSUCI

CSUCI is the newest campus in the California State University system, founded in 1999, and the Computer Science department is only 15 years old. However, Cybersecurity has been an offering in the department since the beginning. In 2015 Soltys spearheaded the formation of a new minor in Cybersecurity, which, for historical reasons, is named *Security Systems Engineering.*

The Department of Computer Science at CSUCI has been growing steadily from its inception, at about 8% to 10% every year, and currently there are about 500 majors in Computer Science. This means that almost 80 students will graduate this year; of these students, about 15 to 20 have a minor in Cybersecurity, and these students are prime candidates for Cybersecurity positions at the Navy. Indeed, in 2019 out of 15 students with a minor in Cybersecurity, 7 were employed by PHD.

Since August 2019, CSUCI has had a second faculty, Dr. Reza Abdolee, with expertise in Cybersecurity. In the spring 2020 Dr. Abdolee taught a graduate class in the Cybersecurity of the Internet of Things (IoT), his main area of research.

At CSUCI, cybersecurity classes tend to be taught in a dedicated lab, Sierra 1131 (Networks & Security lab). There is also an active student-led cybersecurity club, with about 20 members, where instructor Kevin Scrivnor is the mentor.

Assemblymember Jacqui Irwin is a champion of the university, and she has set up a Cybersecurity Advisory board; Soltys is a member. Soltys is now also on the Governor's Cybersecurity Task Force, working in the educational track ([2]). The mandate of this track is to answer the following question: "how do we form the cadre for the 35K positions in Cybersecurity in California?" This is the same problem that PHD encounters at the local level.

Additionally there exists a strong collaboration with the Ventura DA Cybersecurity Taskforce, in virtue of the CSUCI membership in the SoCal High Technology Task force (SoCal HTTF). CSUCI's role is to consult on technical aspects of digital forensics, and student engagement in R&D for the Taskforce; several capstones and masters theses have arisen from this partnership.

In the spring of 2018 CSUCI became a member of CyberWatch West (CWW), an educational institution with the mandate of increasing the quantity and quality of the cybersecurity workforce throughout the western United States. So far the full potential of this partnership has not been realized.

The CI campus itself has an active Chief Security Office (CSO), Neal Fisch.

2.5.1 Cybersecurity Minor

CSUCI has a Computer Science minor in Cybersecurity, called *Security Systems Engineering*,[3] which is built around COMP 424 (Cybersecurity) and MATH 482 (Cryptography), and this class is traditionally taken by students who major in Computer Science or IT; indeed, it is necessary to have a broad understanding of CS/IT in order to work in the field of Cybersecurity.

COMP 424 has been taught by one of CSUCI's most seasoned instructors, Sami Al-Salman, who is also part of the CSUCI AWS committee, certified as an AWS instructor. Al-Salman is able to introduce aspects of Cloud Computing, the new paradigm of IT, into this class. The course is very popular, not only with Cybersecurity minors, and therefore CSUCI offers several sections each semester. This course has now been taken over by Dr. Reza Abdulee, who has plans to upgrade it, specifically to make it a lab-based course (like many other core Computer Science courses).

As the minor is traditionally taken by CS/IT majors, most students also take COMP 350 (Software Engineering) and COMP 429 (Networks), which present material fundamental to Cybersecurity, and there are also electives such as Chemistry's CHEM 343 (Forensic Science). This is useful as many of the CSUCI Cybersecurity capstones are taken through the collaboration if the SoCal HTTF, and so they have a distinct "digital forensics" flavor. However, this is not a great relevance to the Navy, where the emphasis is to prevent penetrations, rather than conduct post-mortems on them.

2.5.2 Masters level offering in Cybersecurity

CSUCI offers a graduate Computer Science course in Cybersecurity, COMP 524,[4] which is intended for an advanced audience. Permission to enroll can be given to interested potential students who are not in the CI Masters in CS program: in 2019 there were several personnel from PHD. The arrangement to offer Cybersecurity training to the PHD personnel at CSUCI has been worked out initially with Vance Brahosky (Deputy Technical Director, Naval Surface Warfare Center-PHD) & Anabell Ramos (NSWC PHD Workforce Development).

COMP 524 is traditionally taught by Soltys, and it emphasizes four aspects of Cybersecurity: Software Engineering (defensive programming),

[3] `http://bit.ly/CSUCISSE`

[4] `http://prof.msoltys.com/?page_id=3505`

Cryptography (from mathematical foundations to implementations of cryptographic schemes and protocols), Sys Admin and Digital Forensics. The course has been revamped and new material has been added in light of CSUCI's partnership with AWS: the new material is related to Cybersecurity in the Cloud, and is described by Soltys in this paper [4], and in Section 3.4.

The partnership with SoCal HTTF plays a role in COMP 524 as well. For example, in the 2017 summer term, CSUCI developed the SEAKER Digital Forensic tool.[5]

3 Security Certifications

In recent years there has been a push for what has been coined by Brandon Busteed ([5]) as a *Credegree*, a *portmanteau* word from "Credential" and "Degree." The idea, as discussed also in [6, 7], is that an effective modern workforce combines a traditional bachelor degree as well as an industry-recognized skill or credential. Thus, many Computer Science and Information Technology majors strengthen their degree with industry certification, and PHD certainly values the combination of both.

A typical ranking of top InfoSec certifications would contain the following five: Certified Ethical Hacker (CEH), Certified InfoSec Manager (CISM), CompTIA Security+, Certified InfoSec Security Professional (CISSP), Cisco Certified Network Professional (CCNP) and Certified Information Security Auditor (CISA). In this section the paper describes broadly three of those certifications, as well as a certification that is becoming more popular with the advent of the cloud: AWS Security Specialty. These are being addressed purely as reference for foundational industry certifications and do no way imply endorsement from either the DON or CSUCI. Per the DCWF government employees are provided training applicable to the systems they support in accordance with the required knowledge, skillsets, and abilities.

3.1 CompTIA Security+

Per the CompTIA vendor, CompTIA Security+ is a global certification that validates the baseline skills you need to perform core security functions and pursue an IT security career. It establishes the core knowledge required

[5] https://prof.msoltys.com/?p=2713

of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Successful candidates will have the following skills:

- Detect various types of compromise and understand penetration testing and vulnerability scanning concepts
- Install, configure, and deploy network components while assessing and troubleshooting issues to support organizational security
- Implement secure network architecture concepts and systems design
- Install and configure identity and access services, as well as management controls
- Implement and summarize risk management best practices and the business impact
- Install and configure wireless security settings and implement public key infrastructure

Overall this is a certification which provides foundational knowledge to the lexicon of baseline concepts in the InfoSec industry.

3.2 RHCSA

Per the Red Hat vendor, "An IT professional who has earned the Red Hat Certified System Administrator (RHCSA) is able to perform the core system administration skills required in Red Hat Enterprise Linux environments." An RHCSA is able to perform the following tasks:

- Understand and use essential tools for handling files, directories, command-line interfaces (CLI), and documentation
- Create simple shell scripts
- Operate running systems, including booting into different run levels, identifying processes, starting and stopping virtual machines, and controlling services
- Configure local storage using partitions and logical volumes

- Create and configure file systems and file system attributes, such as permissions, encryption, access control lists, and network file systems
- Deploy, configure, and maintain systems, including software installation, update, and core services
- Manage users and groups
- Manage security, including basic firewall and SELinux[6] configuration
- Perform basic container management

Overall this is a certification which provides foundational Linux systems administration knowledge and skillsets, which is essential to anyone pursuing a career in InfoSec.

3.3 CCNA

Per the CISCO vendor, "The Implementing and Administering Cisco Solutions (CCNA) v1.0 course gives you a broad range of fundamental knowledge for all IT careers. Through a combination of lecture, hands-on labs, and self-study, you will learn how to install, operate, configure, and verify basic IPv4 and IPv6 networks." The course covers:

- Configuring network components such as switches, routers, and wireless LAN controllers; managing network devices
- Identifying basic security threats
- Gives a foundation in network programmability, automation, and software-defined networking

Overall this is a certification which provides foundational network administration knowledge and skillsets, which is essential to anyone pursuing a career in InfoSec.

[6] Security Enhanced Linux (SELinux)

3.4 AWS Security Specialty

The Cloud is the new paradigm of IT, as organizations are taking advantage of a model of procuring IT where resources are accessed on demand, via the Internet, in a pay-as-you-go fashion. Businesses are reporting vast savings (up to 80%) in comparison to running their IT operations on premises.

This new paradigm of computing has tremendous advantages, not only financial; for example, it democratizes technologies such as Machine Learning which, until recently, where accessible only to a few well funded institutions. However, there are challenges as well, since most decision makers are weary of parting with data which may contain intellectual property or sensitive customer information. Thus, security is often cited as the biggest concern of companies moving into the cloud.

As mentioned elsewhere in this paper, at CSUCI there exists a partnership with AWS, and offer a certification in the Cloud Security, namely the *AWS Security Specialty*, which has been integrated with the other cybersecurity offerings (including the two classes in cybersecurity: COMP 424 and COMP 524). The details related to the curriculum and certification in the area can be found here: [8]. The details related to the certification classes taught at CSUCI can be found here: `http://prof.msoltys.com/awscert` . At this time most of these classes are taught by Soltys, but as their popularity grows, other instructors will also be teaching this offering.

4 Recommendations

PHD and CSUCI are well positioned for a collaboration; for example, the immediate proximity, and the fact that CSUCI is a regional university, where the vast majority of students are from the three counties of Ventura, LA and Santa Barbara, and those are the preferred candidates at PHD since employees with local roots tend to stay long-term.

CSUCI is an institution attended by students who are local, as pointed out in the above paragraph, who want to use their university degree to find a job upon graduation, and preferably stay in the area. As Naval Base Ventura County is one of the largest employers in Ventura County, and civil service is attractive to many students, PHD becomes a top choice for many young careers.

Most importantly however, there is a mutual desire between PHD and

CSUCI for a close cooperation, as reflected by the active educational agreement between these two institutions. In this section, proposals are put forth to examine how to strengthen the pipeline between PHD and CSUCI, especially from the perspective of Computer Science graduates.

4.1 Pathways to work in Cybersecurity at PHD

Numerous internship opportunities and scholarship programs exist as a path towards civil servant employment at NSWC Port Hueneme Division. Internship opportunities are listed online and they include:

- DoD College Acquisition Internship Program (DCAIP)
- DON Pathways Student Trainee
- Office of Naval Research (ONR) — Naval Research Enterprise Internship Program (NREIP)
- STEM Student Employment Program (SSEP)

In addition, the Navy has a direct hire authority for any person entering with the cybersecurity field, meaning that the organization can take resumes directly through their website unsolicited.

With respect to scholarship opportunities, two programs offer funding in exchange for government service:

- CyberCOPRS Scholarship for Service (SFS)[7]
- NSA Funded DOD Cybersecurity Scholarship Program (CySP)[8]

Both offer excellent opportunities for students to have the cost of their education covered and a job upon graduation, in exchange for government civil service for a few years. Academic institutions such as CSUCI must register with the respective programs as well curriculum meeting the requirements to qualify as a candidate for the program.

[7] https://www.sfs.opm.gov

[8] https://public.cyber.mil/cysp

4.2 Recommendations for PHD

- Foster research collaboration with CSUCI. This will have many benefits; CSUCI can leverage its expertise to help PHD solve technical problems, but more importantly, it is the strongest students who work on research problems with faculty, and it will be beneficial for PHD if those students become aware of the interesting projects at PHD.
- Hold quarterly recruitment question and answer sessions for students to speak with civil servant cyberworkforce professionals. This can provide valuable insight to how industry differs from the academic environment and help engage and correct any misconceptions students may have.
- Help CSUCI maintain a database of CSUCI alumni who are working at PHD. Indeed, a census of such employees would be beneficial as these are the natural ambassadors to bring other students to PHD, and also build bridges between PHD and CSUCI.

4.3 Recommendations for CSUCI

Upon initial investigation of opportunities between the organizations to mature their relationship and pipeline, the following are of key importance:

- Investigate SFS partnership requirements against CSUCI curriculum. Students obtaining full undergraduate or graduate level scholarships, in addition to job placement prior to graduation is a benefit for both CSUCI and the government. CSUCI may already meet these requirements and only need to enroll. If not, it would provide insight to additional curriculum or changes to existing curriculum which would be needed to satisfy entrance criteria of the program.
- Investigate CySP partnership requirements against CSUCI curriculum. Students obtaining full undergraduate or graduate level scholarships, in addition to job placement prior to graduation is a benefit for both CSUCI and the government. CSUCI may already meet these requirements and only need to enroll. If not, it would provide insight to additional curriculum or changes to existing curriculum which would be needed to satisfy entrance criteria of the program.

- PHD Workforce Development Division and Competency management leads evaluate the publically accessible (i.e. not requied to be a student) class curriculum available at CSUCI as a potential competetive source of training to meet training qualification standards. Being a local university may provide cost saving advantages while offering state of the art cybersecurity and information technology knowlege and skillsets. Additionally, as noted throughout the paper, PHD personnel have taken a wide array of classes at CSUCI, and they have also taught classes at CSUCI. This should be tracked and improved; Soltys is willing to undertake it.

Glossary

CCNA Cisco Certified Network Associate. 14

CCNP Cisco Certified Network Professional. 12

CCWDES California Cybersecurity Workforce Development and Education Strategy (2020–2030). 3

CEH Certified Ethical Hacker. 12

CISA Certified Information Security Auditor. 12

CISM Certified InfoSec Manager. 12

CISSP Certified InfoSec Security Professional. 12

CLI Command Line Interface. 13

CS Computer Science. 4

CSUCI California State University Channel Islands. 3

CWW CyberWatch West. 10

DCAIP DoD College Acquisition Internship Program. 16

DCWF DoD Cyber Workforce Framework. 6

DoD Department of Defense. 5

DoDD Department of Defense Directive. 6

ICS Industrial Control Systems. 5

IoT Internet of Things. 10

ISEA In Service Engineering Agent. 5

IT Information Technology. 5

JCTCS Joint Cyberspace Training and Certification Standards. 6

NCS Navy Control System. 5

NCWF National Cybersecurity Workforce Framework. 6

NICE National Initiative for Cybersecurity Education. 6

NREIP Naval Research Enterprise Internship Program. 16

ONR Office of Naval Research. 3, 16

OT Operational Technology. 5

PLC Program Logic Controller. 5

RHCSA Red Hat Certified System Administrator. 13

RMF Risk Management Framework. 8

SecDevOps Security Development & Operations. 8

SELinux Security Enhanced Linux. 14

SoCal HTTF SoCal High Technology Task Force. 10

SSEP STEM Student Employment Program. 16

SYSCOM System Command. 4

USN United States Navy. 4

References

[1] S. Morgan, “Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021,” *Cybercrime Magazine*, October 2019. [Online]. Available: https://cybersecurityventures.com/jobs/

[2] K. E. Clement, “California cybersecurity workforce development and education strategy (2020-2030),” California Cybersecurity Task Force, Tech. Rep., June 2020.

[3] R. Rush, “Educational partnership agreement between naval surface warfare center, port hueneme division and california state university channel isalnds,” December 2014, richard Rush was the president of CSUCI at the time.

[4] M. Soltys, “Cybersecurity in the AWS Cloud,” California State University Channel Islands, Tech. Rep., 2020. [Online]. Available: https://arxiv.org/abs/2003.12905

[5] B. Busteed, “Why college will soon be about credegrees and co-ops,” *Forbes*, March 2019. [Online]. Available: https://www.forbes.com/sites/brandonbusteed/2019/03/11/why-college-will-soon-be-about-credegrees-and-co-ops/#60cdc33e3159

[6] ANSI, “Workcred joins experts to share why college will soon be about ”credegrees”,” ANSI News and Publications, Tech. Rep., April 2020. [Online]. Available: https://www.ansi.org/news_publications/news_story?menuid=7&articleid=3da32b36-d324-49e1-8d4c-2ece12a70358

[7] T. Economist, “Learning and earning,” *The Economist*, 2017.

[8] AWS, “AWS Certified Security – Specialty,” Online. [Online]. Available: https://aws.amazon.com/certification/certified-security-specialty/

[9] C. H. Apigian and S. E. Gambill, “Are we teaching the IS 2009 model curriculum?” *Journal of Information Systems Education*, vol. 21, no. 4, 2010.