Commonwealth Cyber Initiative
COASTAL VIRGINIA

Coastal Virginia Center for Cyber Innovation

Semi-Annual Report
July 2021 to December 2022
January 31, 2022

Brian Payne – Director
R. Michael Robinson – Deputy Director
John Costanzo – Chief Administrative Officer/Program Manager

2123 Monarch Hall
Norfolk, Virginia 23529

For additional information please contact John Costanzo, jcostanz@odu.edu.

Commonwealth Cyber Initiative
COASTAL VIRGINIA

The Commonwealth Cyber Initiative CoVA CCI
Semi-Annual Update
For 1st and 2nd Quarters FY 2022

About COVA CCI

Virginia's Commonwealth Cyber Initiative (CCI) aims to create a Commonwealth-wide ecosystem of innovation excellence in cyber-physical systems (CPS) with an emphasis on trust and security. Certified as one of the four nodes of CCI, the Coastal Virginia Center for Cyber Innovation (COVA) seeks to:

Research | Innovation | Commercialization

Coastal Virginia Center for Cyber Innovation

Vision: Secure the nation's critical infrastructure and strengthen Virginia's economy through the commercialization of findings from cutting-edge cybersecurity research focused on the **maritime, defense, and transportation industries**.

Mission: COVA CCI is southeastern Virginia's engine for research, innovation, and commercialization of next-generation cybersecurity technologies particularly in the areas of **Cyber Physical Systems Security (CPSS), 5G, and Artificial Intelligence (AI)**

- **Maritime**
- **Defense**
- **Transportation**

- conduct fundamental research in cyber physical systems security (CPSS), artificial intelligence, and 5G contributing to the CCI mission of establishing Virginia as a global leader in secure CPS and in the digital economy,
- foster and accelerate commercialization of CPSS innovation in order to grow and diversify the Virginia cyber economy, and
- expand and diversify the cybersecurity talent pipeline through investments in research capabilities and commercialization efforts, and
- build a collaborative network within the region of educational institutions, business, and local, state, and federal agencies, and with the other CCI nodes

Under these overarching goals, the COVA CCI is developing and launching a diversity of programs, ranging from cybersecurity research and commercialization to the creation of the Cyber Innovation Park.

COVA CCI created a network of over 100 faculty and researchers representing the region's community colleges and universities. These educational partners include Christopher Newport University, Norfolk State University, Old Dominion University, William & Mary, Regent University, ECPI University, Eastern Shore Community College, Paul D. Camp Community College. Tidewater Community College, and Thomas Nelson Community. COVA CCI is also partnering with over 20 industry and government agencies including the CISCO, G2Ops, Huntington Ingalls Shipbuilding, KBRWyle, MITRE, MI Technical Solutions, Peregrine Technical Solutions, Sentara Healthcare, US Navy, and 360IT to name a few.

Commonwealth Cyber Initiative
COASTAL VIRGINIA

Table of Contents

Summary of Accomplishments for Q1 and Q2 FY 2022 (July – December 2021) 4
1. External Research Grants Attracted to Support the Work of CCI 5
2. Research Grants and Programs Awarded from the Funds Contained in HB30 7
3. Results of Entrepreneurship and Workforce Programming.....21
4. Collaborative Partnerships and Projects 24
6. Geographic Distribution of Awards from the Funds Contained in HB30 26
7. Other initiatives. 27
8. COVA CCI Node in the News 30

Summary of Accomplishments for Q1 and Q2 FY 2022 (July – December 2021)

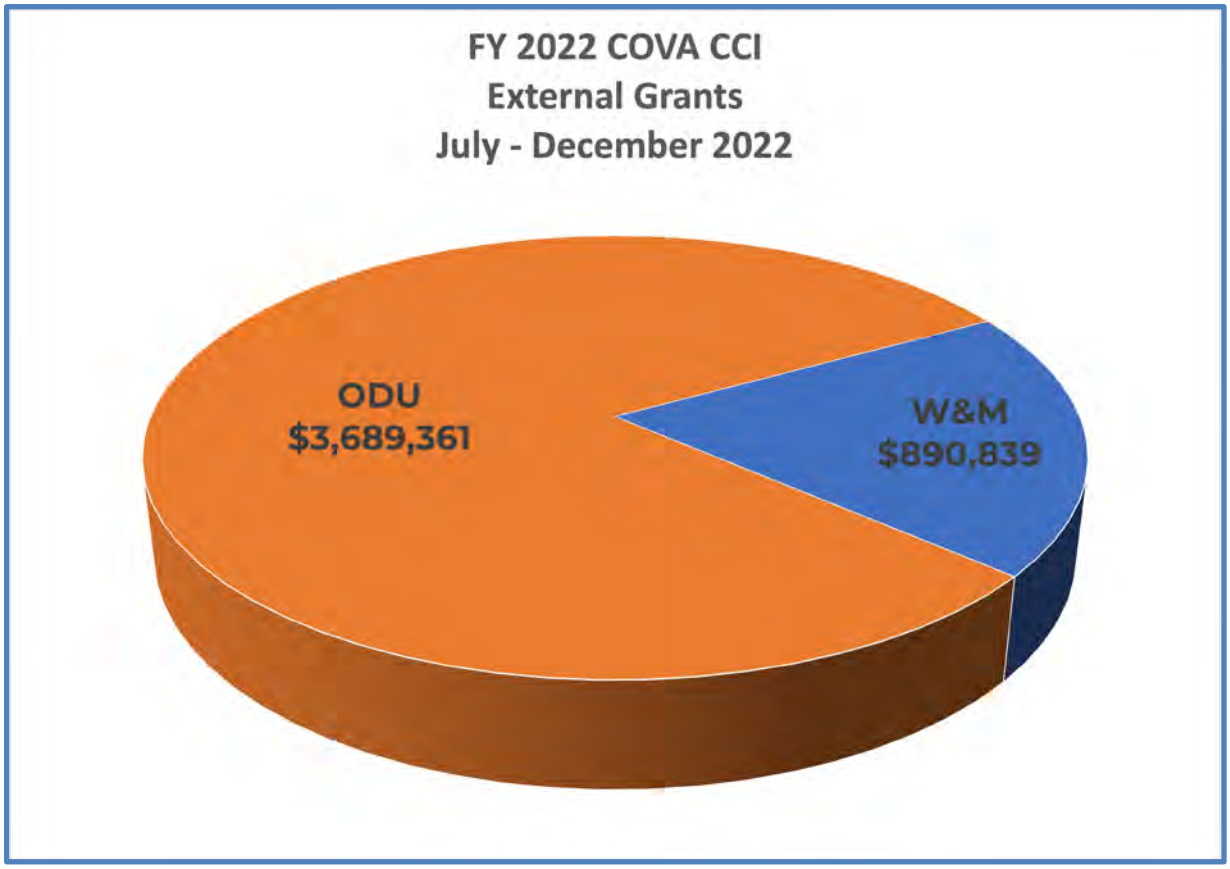
COVA CCI focus during the first half of FY 2022 (July – December 2021) was on continuing the five funded cybersecurity research projects, initiating selected CCI Collaboration Research projects, and supporting sponsored activities.

1. During first two quarters of FY 2022, COVA CCI academic institutions were awarded approximately $4.58 million dollars in cybersecurity grants from government and private industry.
2. Awarded $750,000 in research funds as part of the COVA CCI FY 22 Cybersecurity and Innovation Research RFP with five projects selected to start on July 1, 2021.
3. Continued to support the FY 2021 research projects awarded by CCI.
4. Received funding from CCI during FY 2022 to support four new research projects including two under the NextG RFP, one Cybersecurity Challenge project, and one CCI Cybersecurity Research Collaboration project.
5. Selected sixteen (16) graduate students during fall 2021 to participate in the Cyber Experiential Learning (CyberExL) program. These students supported faculty led research projects, the non-profit Global Fund to End Modern Slavery, Camp Community College, and Peregrine Technical Solutions (local cybersecurity business).
6. Selected thirty (30) students to participate in the Cybersecurity Undergraduate Research Program – fifth teen (15) in Fall 2021 and fifth teen (15) in Spring 2022.
7. Selected fifty-four (54) students from fourteen universities and colleges to participate in the Spring 2022 cohort of Innovate Cyber Challenge.
8. Continued to work with the Virginia Space Grant Consortium on the Cybersecurity Internship program to place cybersecurity students from across the region into internship opportunities. To date twenty-one (21) students from 6 universities/colleges have been placed with eleven (11) companies.
9. Developed a regional network of over 100 researchers, faculty, and business partners working for eight colleges/universities and 20+ businesses
10. Completed the construction of the Cyber Innovation Park in August 2021. Located on the main campus of Old Dominion University this center is now home to COVA CCI and the ODU School of Cybersecurity.
11. Completed the installation of the Shared Collaborative Research Computing Environment (COVA SHARE) and currently are supporting five projects under this environment.

Update on the Seven Requirements

1. External Research Grants Attracted to Support the Work of CCI

During the first half of FY 2022, July – December 2021, $4.58 million in research grants were awarded to COVA CCI researchers. Each of these grants has a PI or Co-PI affiliated with or received funding directly from COVA CCI and/or CCI for their research.



FY 2022 COVA CCI External Research Grants – William & Mary					
Sponsor	Project Title	Period of Performance	Awarded Organization	PI/Co-PIs	Funding Amount
NSF	Toward safe, private, and secure home automation: from formal modeling to user evaluation	1/1/22–12/31/24	W&M	Adwait Nadkarni Denys Poshyvanyk	$799,839
New Venture Fund	W&M Cybersecurity Awareness Initiative for Public Interest Technology University	1/1/22-5/30/23	W&M	Dorothea LaChon Abraham Iria Giuffrida	$90,000
W&M Alan B. Miler Entrepreneur-ship Center	Tribe Venture Cohort; William & Mary Student Venture Incubator Program	10/1/21– 5/30/22	W&M	Woosub Jung	$1,000
Total William & Mary					$890,839

Commonwealth Cyber Initiative
COASTAL VIRGINIA

FY 2022 COVA CCI External Research Grants – Old Dominion University					
Sponsor	Project Title	Period of Performance	Awarded Organization	PI/Co-PIs	Funding Amount
HRBRC	Extended Reality enabled 5G tele mentoring	10/1/21–6/30/22	ODU/VMASC	Sachin Shetty	$115,000
Deloitte	Top Down 5G Network Security Design	5/1/21–12/31/21	ODU/VMASC	Sachin Shetty	$50,000
FTI	Cyber Risk and Resilience Analytics	7/1/21–9/22/21	ODU/VMASC	Sachin Shetty	$70,000
NSF	Analytically based frameworks for AI model verification and improvement in cyber-physical systems	10/1/21–9/30/22	ODU/VMASC	Sachin Shetty	$60,000
Deloitte	Top Down 5G Network Security Design	5/1/21–12/31/21	ODU/VMASC	Sachin Shetty	$50,000
DoD	Center of Excellence in Machine Learning	10/1/21–9/30/22	ODU/VMASC	Sachin Shetty	$350,000
NSF	Collaborative Research: CCRI: New: Medium: A Development and Experimental Environment for Privacy-preserving and Secure (DEEPSECURE) Machine Learning	10/01/21-9/30/24	ODU	Hongyi Wu Chunsheng Xin	$780,000
NSA	Backdoor Detection, Mitigation, and Prevention in Deep Neural Networks	9/08/21-12/31/23	ODU	Hongyi Wu, Chunsheng Xin Jiang Li	$500,000
InterDigital	Blockchain-based AI/ML Management to EnableSmart Next G Wireless Networks	10/1/21-10/1/22	ODU	Rui Ning Hongyi Wu Chunsheng Xin	$100,000
GoVA	Cybersecurity Job Creation System (CJCS)	10/1/21-10/1/23	ODU	Hongyi Wu	$1,450,000
NSA	2021 DOD CySP Grant Program: Training Cyber Talents for DoD Workforce	8/01/21-12/31/22	ODU	Chunsheng Xin Hongyi Wu	$316,000
NSA	ODU GenCyber Teacher Camp: Cybersecurity+AI: a GenCyber Camp in the Age of AI to Train K-12 Teachers for Classroom Teaching of Cybersecurity	8/2/21-12/31/23	ODU	Chunsheng Xin Hongyi Wu Danella Zhao Karen Sanzo	$145,000
NSA	JROTC Students and Teachers Interactive Learning	8/2021-12/2023	ODU	Danella Zhao Chunsheng Xin Hongyi Wu Tammi Dice	$175,000
NSA	VA-CNIP: A Coalition for the Virginia Cyber Navigator Internship Program	9/01/21-8/30/24	ODU	Hongyi Wu	$210,000
IMLS	A Graduate Certificate in Web Archiving	8/01/21-07/31/22	ODU	Michael Nelson Michele Weigle Sue Kimmel Jessica Ritchie Hongyi Wu	$98,361
Total Old Dominion University					$3,689,361

2. Research Grants and Programs Awarded from the Funds Contained in HB30

COVA CCI is providing funding under the research category for several initiatives.

Research Programs	Funding
FY 22 COVA CCI Cybersecurity Research and Innovation Funding Program	$750,000
Computer Lab Upgrades Program	$361,820
Cybersecurity Curriculum Development Program	$20,000
Cybersecurity Dissertation Fellowship Program	$100,000
Cybersecurity Undergraduate Research Program	$90,000
FY 21 CCI Funded Research Programs	$1,927,195
FY 22 CCI Funded Research Programs	$187,500
Research Scientists	$348,000

a) **FY 2022 COVA CCI Cybersecurity Research and Innovation Funding program**. COVA CCI is providing funding through the COVA CCI Cybersecurity Research and Innovation Funding program. This program supports diverse and inclusive CPSS research efforts, with a focus on the intersection of artificial intelligence (AI), cybersecurity, and CPS technologies applied to maritime, transportation, and defense sectors. Five projects were approved in June 2022 for a total of $750,000. These projects will be completed in June 2023. See the article "ODU-Led Cybersecurity Projects Grant Funded for more information."

Project Title	PI	Co-PI	Amount
Toward Trustworthiness in Autonomous Vehicles	Evgenia Smirni (WM)	H. Alemzadeh (UVA)	$150,000
A Real-Time Dependency Network Approach to Quantifying Risks and Ripple Effects from Cyberattacks in Shipbuilding and Repair Supply Networks	Rafael Diaz (ODU)	H. Shen (UVA)	$150,000
Comprehensive Assessment and Diagnostics for Federated AI Algorithms in Cyber Physical Systems	Rui Ning (ODU)	J. Le (ODU) C. Xin (ODU) X Deng (VT) Y. Hong (VT) L Freeman (VT)	$150,000 (ODU-$100000) (VT-$50000)
CIVIIC: Cybercrime in Virginia: Impacts on Industry and Citizens	Randy Gainey (ODU)	T. Vandecar-Burdin (ODU) J. Albanese (VCU) J. Hawdon (VT) K. Parti (VT) T. Dearden (VT)	$149,683 (ODU-$50723) (VT-$39267) (VCU-$59693)
Developing a Smart City Virtual Lab to Support CPS Experiential Learning	Murat Kuzlu (ODU)	S. Abdelwahed (VCU)	$150,000 (ODU-$75000) (VCU-$75000)

(1) Project Title: Towards Trustworthiness in Autonomous Vehicles. Dr. Evgenia Smirni, W&M

Abstract: Autonomous vehicles (AVs) are one of the most complex software-intensive Cyber-Physical Systems (CPS). In addition to the basic car machinery, they are equipped with driving assistance mechanisms that use smart sensors and machine learning (ML) for environment perception, pathfinding, and navigation. Even though tremendous progress has been made in advancing the safety and security of AVs, they are shown to be vulnerable to accidental and malicious faults that negatively affect their perception and control functionality and result in safety incidents. Recent works have highlighted two major challenges in safety validation and assurance of AVs: (i) With the increasing use of specialized hardware accelerators (GPUs) for running ML-based perception algorithms, AV control systems have become susceptible to transient faults (soft errors) that can result in erroneous ML inference and unsafe decision making and control. (ii) Safety assurance for AVs requires testing their resilience by identifying and simulating realistic safety-critical fault and attack scenarios by mining a tremendous fault space. To address these challenges, this project brings together a team of experts in GPU and CPS resilience from two CCI nodes to develop a holistic approach for end-to-end resilience assessment of AVs. We combine strategic fault injection at both hardware accelerator and controller software levels to assess the sensitivity of the ML components and control system to accidental or malicious faults and identify critical components and system states. The results from this project will make a firm step towards achieving trustworthiness in autonomous vehicles.

(2) Project Title: A Real-Time Dependency Network Approach to Quantifying Risks and Ripple Effects from Cyberattacks in Shipbuilding and Repair Supply Networks. Dr. Rafael Diaz, ODU.

Abstract: The evolution of defense shipbuilding supply networks toward digital environments increases operational complexity and requires reliable communication and coordination to regulate information exchange. As workers and suppliers transition to digital platforms, interconnection, information transparency, and decentralized decisions become prevalent. The appearance and extensive use of these digital platforms inexorably increase their exposure to cyberattacks. Unfortunately, the effects of a systematic cyberattack on one or more nodes belonging to the shipbuilding supply network (e.g., Colonial Pipeline) are unknown. This collectively may represent a substantial source of disruption. Cybersecurity protection of these networks requires a systemic approach to evaluate their vulnerability and understand ripple effects. However, current evaluation technologies and techniques are

primarily applied to individual nodes or firms (if they are applied at all) and commonly lack systemic perspectives that consider overlapping risks and tiered hierarchies.

To overcome these limitations, we propose developing a cybersecurity supply network Artificial Intelligence (A.I.) framework that enables characterizing and monitoring shipbuilding supply networks and determining ripple effects from disruptions caused by cyberattacks. By representing and replicating the collective behavior of relevant shipbuilding supply network nodes, shipbuilders can monitor and measure the impact of cybersecurity disruptions and test the reconfiguration options that minimize the detrimental effects on the supply network. This framework extends a novel risk management framework developed by Diaz and Smith (2021) and Smith and Diaz (2021) that considers complex tiered networks and systemic hypervulnerabilities (COVA CCI - 2021ODU-06.005) and is currently tested in the port security cyber-physical setting.

(3) Project Title: Comprehensive Assessment and Diagnostics for Federated AI Algorithms in Cyber Physical Systems. Dr. Rui Ning, ODU.

Abstract: Federated Artificial Intelligence (AI) is becoming a critical part of cyber physical systems (CPS) in modern maritime, defense and transportation industry, with its game-changing capability for handling large volumes of data and making collaborative complex decisions in support of self-control and self-actuation systems. While the Federated AI is actively integrated into CPS applications, its malfunction can cause catastrophic failure or even be life-threatening for security-essential and safety-critical CPS such as in transportation and defense. Worse yet, as the Federated AI system incorporates AI and distributed devices, it inevitably introduces heterogeneity, randomness, contamination. Specifically, local data of different participants can be noisy and imbalanced, resulting in performance degradation. Moreover, it is also vulnerable to data poisoning attacks. The overarching goals of this project include (1) establishing a design of experiments (DoE) framework to enable systematical investigation of the security and robustness of the Federated AI system; (2) investigating, assessing and unveiling characteristics of Federated AI models under different data imperfections; (3) developing effective schemes to comprehensively diagnose given Federated AI models for potential data imperfections; (4) developing experimental environment for secure and robust Federated AI research. The project will also develop training modules of secure and robust Federated AI, aiming to prepare students and practitioners with advanced skills to succeed in a cybersecurity career. Overall, the proposed work will lead to enabling technologies for secure and robust Federated AI systems, accelerating their development, and broadening their adoption in various application domains, especially the transportation, defense, and maritime sectors.

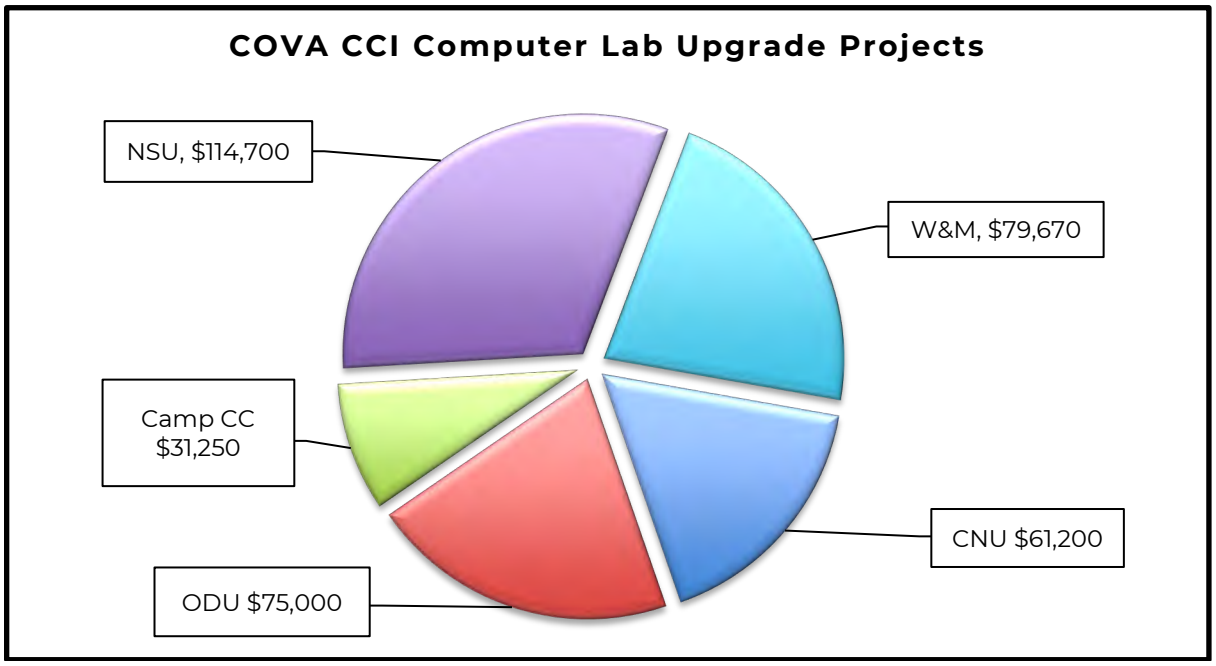
(4) Project Title: CIVIIC: Cybercrime in Virginia: Impacts on Industry and Citizens. Dr. Randy Gainey, ODU.

Abstract: Victimization from cybercrime is a major concern in Virginia, the US, and the world. It is estimated that in 2020, cybercrime resulted in Americans losing an estimated $4.2 billion (FBI 2021). Yet, precise measurement and understanding of the nature of the problem, methods, types, and targets is lacking. While the FBI maintains the Internet Crime Report (IC3), these data are limited to only those crimes reported by victims, which is only a small fraction of the cybercrimes that occur. While a few national citizen and business surveys have been conducted on specific types of cybercrime, the samples have been small, and there is reason to believe their findings may not represent the experience in the Commonwealth. Virginia presents a unique intersection of cyber physical systems with its large workforce in the maritime, defense, and transportation sectors, combined with an educated and mobile workforce making it a uniquely targeted area compared to many other states. This project will create, deploy, analyze, and report on a statewide cybercrime survey of both citizens and businesses. A study and analysis specifically focused on Virginia will enable the delineation of the highest priority threats, identify cybercrime methods used, and provide an assessment of geographic, demographic and industry variation in victimization across the state. The project will provide baseline knowledge and data for future policy, research, and interventions to reduce exposure to cyber victimization in the Commonwealth.

(5) Project Title: Developing a Smart City Virtual Lab to Support CPS Experiential Learning. Dr. Murat Kuzlu, ODU.

Abstract: In this project, our team will develop a virtual smart city lab environment, called VirtualLab@OpenCity, which engages researchers, students, and companies with smart city challenges, such as automation, data analysis, service reliability and sustainability. VirtualLab@OpenCity will provide an experimental environment using a standardized service that supports remote connectivity, data collection, visualization, analysis, resource management and control. VirtualLab@OpenCity aims to build Virginia's cyber-physical systems (CPS) workforce with hands-on experience on new technologies that ultimately lead to innovative smart city solutions. This project will contribute to positioning Virginia as a global leader in secure and trustworthy cyber-physical systems by (a) providing students, researchers, and developers a virtual ecosystem of advanced CPS technologies, (b) providing guidance and support to employ advanced technologies and innovative management systems for ongoing and future smart city plans and (c) foster fruitful collaboration between academia and industry to build a Commonwealth-wide smart city innovation workforce.

b) **Computer Lab Upgrades.** COVA CCI funded five projects, totaling $361,820, supporting partner institution Computer Lab Upgrades with the intent of building new or providing upgrades to academic and/or research computer labs used by students and/or faculty to enhance their academic and research capabilities.



Project Title	Institution	Amount
Enhancing Secured Cybersecurity Infrastructure for Cybersecurity Students in an Interdisciplinary Department	Christopher Newport University	$61,200
Laboratory for Developing Highly Secure IoT-based Applications for Real-time Data Acquisition and Analysis	Old Dominion University	$75,000
The Cybersecurity Lab Enhancement Project	Camp Community College	$31,250
Enhancing CASE-V Testbed with a Ceph-Based Software-Defined Storage Infrastructure	Norfolk State University	$114,700
Developing Infrastructure for Advancing Research and Teaching in Security and Reliability	William & Mary	$79,670

c) **Cybersecurity Curriculum Development.** COVA CCI is funding Cybersecurity Curriculum Development projects that are focused on identifying gaps in existing curricula and the development of strategies to fill these gaps. Two projects were funded in FY 2022 for a total of $20,000. Information and links to previously completed curricula are found on the COVA CCI Talent Development/Curriculum Development website.

COVA CCI curriculum development projects		
Project Title	Institutions	Amount

Cyber Commissioning Training to meet CPS Building Requirements	Old Dominion University	$10,000
Web Science and Web Security	Old Dominion University	$10,000

(1) **Cyber Commissioning Training to meet CPS Building Requirements Project Abstract.** Historically, cyber-physical systems (CPS), otherwise known as industrial control systems (ICS) or supervisory control and data acquisition (SCADA) devices, all of which include electrical, HVAC and water systems, were not connected to the internet. More recently renamed as operational technology (OT) or the internet of things (IoT) devices, these systems tend to be more focused on availability and often did not have to abide by cybersecurity regulations. This changed in 2015 when the Department of Defense (DoD) adopted the Risk Management Framework (RMF) National Institute of Science and Technology (NIST) Special Publication (SP) 800-82 Rev. 2, Guide to Industrial Systems (ICS) Cyber Security, to conduct cybersecurity on these systems. Then in 2018, DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, also required the use of NIST SP 800-171, plus in June 2019, it was announced that the new DoD methodology to conduct these 7012 activities is the Cybersecurity Maturity Model Certification (CMMC), which while tailored more for IT vice OT systems, will be enforced in 2020 / 2021 to include ICS/SCADA/OT and IoT systems, and will be more rigorous in enforcing the cybersecurity gap for CPS. Finally, there has been a recent push by the DoD, to lock down all new buildings from a cyber security aspect, so taken together, you see a huge focus in this area, yet there is little to no training being done. This proposal is to develop an unclassified course icw the Virginia Cyber Range to support these requirements.

(2) **Web Science and Web Security Project Abstract.** Old Dominion University's Web Science and Digital Libraries (WS-DL) Research Group is internationally recognized for both its research and curricula. WS-DL's courses (offered in the computer science department) web science, data science, digital libraries, web archiving, information visualization, human-computer interaction, natural language processing, data mining, machine learning, information retrieval, and web programming. More recently, WS-DL's research and course offerings have moved toward the intersection of the web and security. In the process of developing and delivering our courses, it has become clear that we need to offer a 400/500 level course focused on *web client security*. We are unaware of any such course currently offered in the state of Virginia with a focus on web client security. Given the central role that the web plays in our daily commerce, education, and entertainment, we should be doing a better job producing BS and MS students with expertise in securing web applications. While web security is a significant portion of cybersecurity, it is often overlooked or taken for

granted. And web security requires thorough knowledge of the web itself. In the context of this proposal, we will develop, enhance, and share a four-course sequence that focuses on web programming, web server development, web science, and most importantly, web security. These courses are currently in various stages of readiness for sharing but have all been taught successfully in the CS department of ODU in the recent past. This will be a preeminent four course advanced undergraduate/beginning graduate sequence in all matters of the web.

d) **COVA CCI Cybersecurity Dissertation Fellowship program** supported four cybersecurity Ph.D. students, three (3) from William & Mary and one (1) from Old Dominion University. These students are using the funds to further develop their Ph.D. dissertations and research.

Name	Institution	PhD program	Dissertation/Project Title
Woosub Jung	W&M	Computer Science	Using power side channel auditing and deep learning to secure Internet of Things (IoT) devices
Sunil Manandhar	W&M	Computer Science	Improving Privacy, Security, and Safety in Emerging Platforms
Amit Seal Ami	W&M	Computer Science	Practical and Secure Software Assurance in IoT
Miguel Toro-Jarrin	ODU	Engineering Management & System Engineering	Predictors of Secure Email use Behaviors in Organizations in the USA

e) **Cybersecurity Undergraduate Research Program**. COVA CCI supported the Cybersecurity Undergraduate Research Program in Fall 2021 and selected students for the Spring 2022 program. This program leverages the strength of research-extensive institutions to support active research participation by undergraduate students in the area of cybersecurity. Students will have opportunities to explore a variety of cutting-edge research topics, including but not limited to: Blockchain Security, Cyber Law & Policies, Human Behavior Security, Online Scams, Mobile Protection, Secure Digital Printing, Secure Internet of Things, Secure Machine Learning, Social Engineering, and Wireless Security. To learn more about

this fall's program see this article. The student research is found on the COVA CCI/Innovation/Undergraduate Research website.

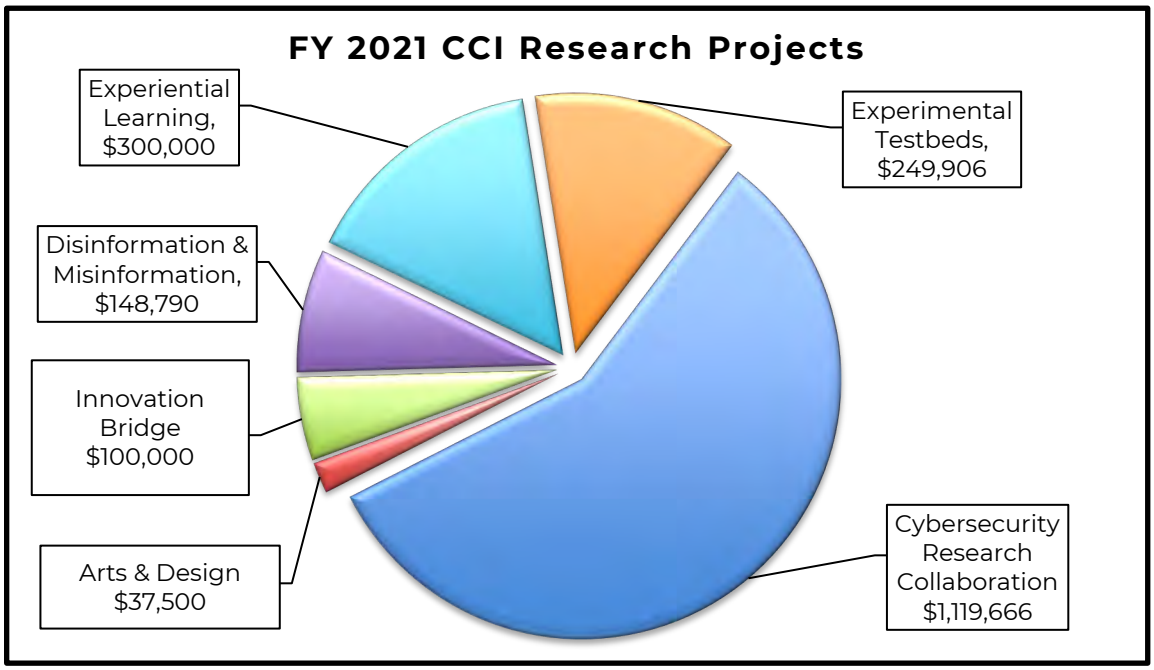
ODU Cybersecurity Student on the value of this program.
"This program pushed me to do independent research and create a final research product, which is a great thing to list on the resume and provides the chance to learn one aspect of cybersecurity more in-depth. I found this Program to be a great complement to my coursework in cybersecurity at ODU, and I value the connections to other educational institutions (e.g., William & Mary) that the Program provided. My research project could very well end up factoring into my future career directions in cybersecurity and law."

COVA CCI Cybersecurity Undergraduate Research Program		
Project Title	Institutions	Amount
Fall 2021 Cohort 15 students	Old Dominion University William & Mary	$45,000
Spring 2022 Cohort 15 Students	Camp Community College Christopher Newport University Norfolk State University Thomas Nelson Community College Tidewater Community College Old Dominion University William & Mary	$45,000

Fall 2021 Cybersecurity Undergraduate Research Program Students.
Pictured top row (left to right) – Matthew Nguyen (ODU), Raymond Geistel (ODU), Joanna DiScipio (W&M), Marlowe Cosby (ODU), and Conner Wu (W&M). Picture bottom row (left to right) – Mary Riley (ODU), Sierra Burnett (ODU), Torre Williams (ODU), Zobair Wali (ODU), David Cooke (ODU), and Seth Smith (ODU). Not pictured – Chad Holm (ODU), Killian Robinson (ODU), Kevin Rossi (ODU), and Noam Stanislawski (W&M).

f) **FY 2021 CCI Funded Research Programs.** COVA CCI was awarded multiple projects in the amount of $1,927,195, in response to requests for proposal sponsored by CCI in FY 2021. These projects continued their research during FY 2022. See the CCI website for details on these projects.

CCI Research Projects	Awards	Total Funding awarded to COVA CCI
Collaborative Research Funds (FY 21/22)	7	$1,119,666
Building Bridges: Arts and Design	2	$37,500
Experiential Learning	2	$300,000
Experiential Research in CCI Testbeds	3	$249,906
Role of Cybersecurity in the Spread of Disinformation and Misinformation	3	$147,790
Cybersecurity Innovation Bridge Funds	3	$71,333
Totals	**17**	**$1,927,195**



(1) **Cybersecurity Collaboration Research project**. In January 2021, COVA CCI awarded seven (7) projects totaling approximately $1.1 million dollars, as part of the CCI led Cybersecurity Collaboration Research project. These projects continued during the first half of FY 22 (July – December) and are beginning to finalize their research. See this article for more details - [cci-funds-22-cybersecurity-grants]. The funded projects are listed below.

COVA CCI led Cybersecurity Collaboration Research projects

Title	PI / Univ	Co-PI / Univ	Funding
Secure and Privacy Preserving 5G Network for Connected Vehicles	Sachin Shetty (ODU)	Tan Le (ODU) Jeff Reed (VT) Cong Shen (UVA) Duminda Wegesekera (GMU) Kai Zend (GMU)	$200,000 ODU – $57,523 VT – $35,976 UVA – $35,500 GMU – $71,001
Backdoor Detection and	Hongyi Wu	Chunsheng Xin	$184,816

Mitigation in Deep Neural Networks	(ODU)	(ODU) Jiang Li (ODU) Rui Ning (ODU) Jin-Hee Cho (VT) Leigh Armistead (Peregrine)	ODU – $136,532 VT – $48,284
DeepPOSE: Securing Transportation Systems from GPS Spoofing Attack	Chunsheng Xin (ODU)	Danella Zhao (ODU) Yanxiao Zhao (VCU) Kevin Kefauver (GCAPS)	$200,000 ODU – $101,175 VCU – $50,000 VT – 48,825
A Systematic Evaluation of Smart City Security and Privacy	Adwait Nadkarni (WM)	Yuan Tain (UVA)	$194,850 WM - $95,460 UVA – $99,390
Virginia State Investments in Port of Virginia: A simulation-based framework for identifying, assessing, and mitigating systemic cybersecurity at the operational technology layer.	Rafael Diaz (ODU)	H. Shen (UVA)	$200,000 ODU –$77,761 UVA –$122,239
Sensor Degradation Detection Algorithm for Automated Driving Systems,	Michelle Chaka (VT)	Chunsheng Xin (ODU)	ODU - $75,000
Developing an Open Architecture Testbed and Learning-based Management for Smart Cities (OpenCity)	Sherif Adbelwahed (VCU)	Murat Kuzlu (ODU)	ODU - $65,000

(2) **CCI Arts and Design Collaboration Project.** The Arts and Design Collaboration challenges the community of researchers in the Arts and Design to reimagine and depict the results of cybersecurity research (and in particular research that occurs in CCI) either for scientific purposes, or for creative arts practice purposes. In response to this RFP, COVA CCI was awarded two projects and they completed their efforts during the 1st and 2nd quarters of FY 2022.

Title	PI / Univ	Co-PI / Univ	Funding
Develop a Gamified Mobile Application for Cybersecurity Education and Assessment via a User Centered Design Process	Kevin Moberly (ODU)	Ryan Patton (VCU) Deri Draper (ODU) Jeff Pittges (Radford) Bobby Keener (CivilianCyber)	ODU - $25,000
Moving Choreography to a New Universe: an AI-Driven Privacy Automation Approach	Kate Sicchio (VCU)	Sachin Shetty (ODU) Yan Lu (ODU)	ODU - $12,500

(3) **CCI Experiential Learning Project.** COVA CCI received two projects in response to the 2021 CCI Experiential Learning CFP and they completed their efforts during the 1st and 2nd quarters of FY 2022.

Title	PI / Univ	Co-PI / Univ	Funding
Cybersecurity Monitoring and Assurance Training Program for Safe and Secure Port Operations	Sachin Shetty (ODU)	Saltuk Karahan (ODU) Sarada Prasad (ODU) Jim Haug (Longwood) Darrell Carpenter, (Longwood) Jennifer Maeng (UVA) Thomas Polmateer (UVA) Lessie Oliver-Clark (VSU) Wei-Bang Chen (VSU) Wookjin Choi (VSU) Rich Ceci (VIT)	$150,000
Cyber Risk Management and Analytics: An Interdisciplinary Approach in Experiential Learning	Chon Abraham (W&M)		$150,000

(4) **CCI Experimental Research in CCI Testbeds.** COVA CCI received three projects in response to the 2021 CCI Experimental Research in CCI Testbeds CFP. These projects are ongoing and are expected to complete their work by June 2022.

Title	PI / Univ	Co-PI / Univ	Funding
Experimental Research: Investigating Robustness and Uncertainty of AI Algorithms in Cyber Physical Systems	Rui Ning (ODU)	Jiang Li (ODU) Xinwei Deng (VT) Laura Freeman (VT) Yili Hong (VT)	$49,906
Beamforming Optimization for 5G and Beyond	Chunsheng Xin (ODU)	Hongyi Wu (ODU)	$50,000
Building a THz Testbed to Expand CCI 5G Testbed for 6G Research	Hongyi Wu (ODU)	Chunsheng Xin (ODU)	$150,000

(5) **Role of Cybersecurity in Spread of Disinformation and Misinformation.** COVA CCI received two projects in response to this RFP as lead PIs and one as a Co-PI with George Mason. These projects are ongoing and are expected to complete their work by June 2022. See these two articles, CCI Researchers Meet to Discuss How Cybersecurity Can Combat Misinformation and Disinformation and Professors Study Cybersecurity's Role in Curbing the Spread of Disinformation to learn more about this program.

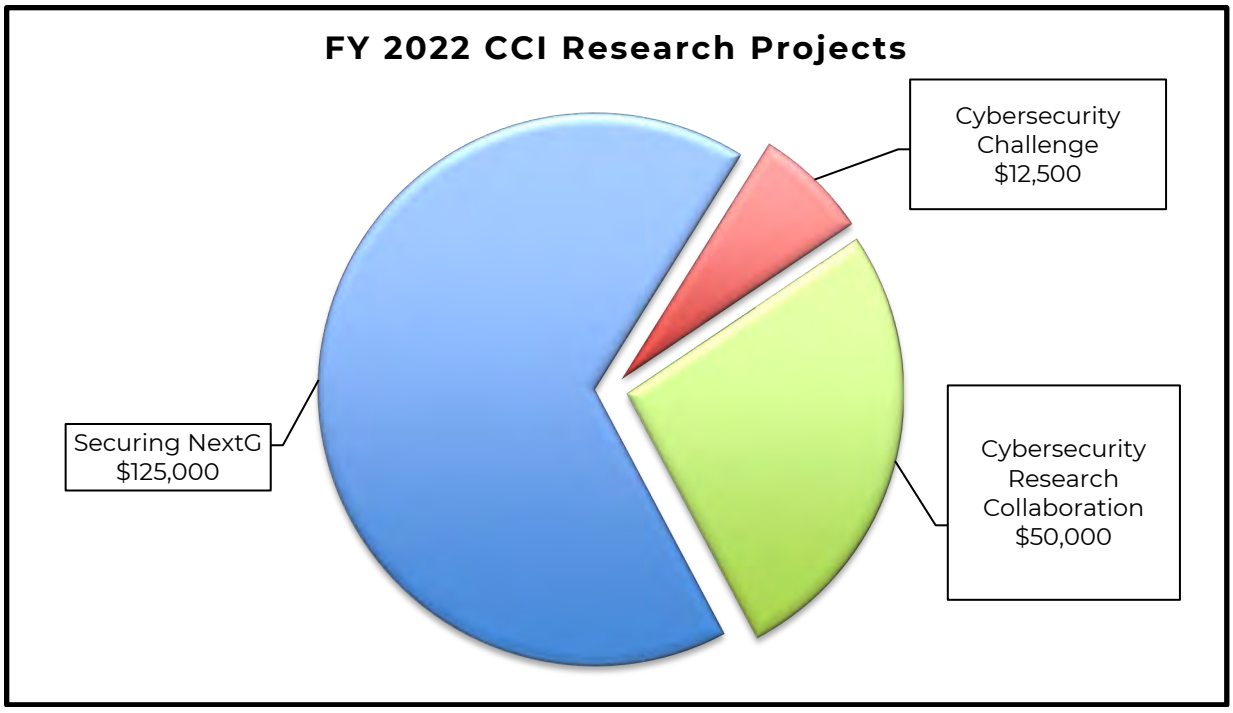
Title	PI / Univ	Co-PI / Univ	Funding
The Acceptance and Effectiveness of Explainable AI-Powered Credibility Labeler for Scientific Misinformation and Disinformation	Jian Wu (ODU)	Jerimiah Still (ODU) Jiang Li (ODU)	$63,790
Question Under Discussion Framework to Analyze Misinformation targeting Security Researchers	Sachin Shetty (ODU)	Teresa Kissel (ODU)	$65,000
Artificial Intelligence Based Analysis of Misinformation and Disinformation Efforts from Mass Media and Social Media in Creating Anti-U.S. Perceptions	Kavak Hamdi (GMU)	Saltuk Karahan (ODU) Hongyi Wu (ODU) Kim Perez (TCC)	$64,996 (ODU - $20,000)

(6) **Cybersecurity Innovation Bridge Fund.** COVA CCI received two awards as lead PIs and one as a Co-PI with VCU. These projects are ongoing and are expected to complete their work by June 2022.

Title	PI / Univ	Co-PI / Univ	Funding
A Minimum Viable Product to Secure IoT Devices through Power Auditing and Privacy Preserved Convolutional Neural Networks	Gang Zhou (WM)	Chunsheng Xin (ODU) Danella Zhao (ODU)	$50,000 (ODU - $21,333)
A Platform for Improving AI Trust in 6G Networks	Murat Kuzlu (ODU)		$50,000
GINDAR - Generative Adversarial Networks (GAN)-based Internet-of-Medical-Things (IoMT) Network Detection and Response	Tamer Nadeem/VCU	Sachin Shetty (ODU)	$50,000 (ODU - $0)

g. **FY 2022 CCI Funded Research Programs.** COVA CCI received multiple projects in the amount of $187,500, in response to various requests for proposal sponsored by CCI in FY 2022.

FY 2022 CCI Research Projects	**Awards**	**Total Funding awarded to COVA CCI**
Securing NextG	2	$125,000
Cybersecurity Challenge	1	$12,500
Cybersecurity Research Collaboration (FY 2022)	1	$50,000
Totals	**4**	**$187,500**



(1) **Securing NextG.** COVA CCI received one (1) award as lead PI and one (1) as a Co-PI with Virginia Tech as the lead. These projects will start work in January 2022 and complete their research in December 2022.

Title	PI / Univ	Co-PI / Univ	Funding
Blockchain-based Deep Learning Management to Enable Smart NextG Wireless Networks	Rui Ning (ODU)	Hongyi Wu (ODU) Hongzhi Guo (NSU)	$100,000
Radio Access Network Slicing Security for NextG Networks	Laura Freeman (VT)	Sachin Shetty (ODU)	$25,000 (ODU) $75,000 (VT)

(2) **Cybersecurity Challenge.** Camp Community College received one award as part of the Cybersecurity Challenge.

Title	PI / Univ	Co-PI / Univ	Funding
The Legacy and Sensitive Device IoT Passive Connection Project	Robert Tureman (Camp C.C.)	NA	$12,500

(3) **Cybersecurity Research Collaboration FY 2022.** Old Dominion University partners as a Co-Pi with Virginia Tech on the research project, "Deep Resilience for Multifaceted Federated Learning in IoT."

Title	PI / Univ	Co-PI / Univ	Funding
Deep Resilience for Multifaceted Federated Learning in IoT	Cho (VT)	Hongyi Wu (ODU)	$50,000 (ODU) $75,000 (VT)

h. **Research Faculty Recruited.** COVA CCI hired six (6) additional research faculty in FY 2022, with four (4) supported directly with CCI funds and two (2) hired as matching department funds. Bios for these research scientists are found on the COVA CCI website/People/Research Scientists. You can also watch a short YouTube video, Meet the COVA CCI Research Scientists, where several of the research scientist provide an introduction.

- Tabrez Ebrahim (William & Mary).
- Kazi Aminul Islam, ODU School of Cybersecurity.
- Tran Phoung, ODU School of Cybersecurity.
- Masud Rana, ODU VMASC.
- In addition, ODU hired two additional scientists as a match – Lori Portman (ODU School of Cybersecurity) and Safdar Bouk (ODU VMASC).

COVA CCI also continued to support four research faculty hired in FY 2020/2021.

- Le Thanh Tan, Old Dominion University.
- Rui Ning, Old Dominion University.
- Daniel Shin, William & Mary.
- Yan Lu, Old Dominion University. Hired as a match.

Le Thanh Tan, Ph.D, Engineering
Institut National de la Recherche Scientifique (2015)
Research Assistant Professor, ODU
tle@odu.edu

Yan Lu, Ph.D
Old Dominion University (2020)
Research Assistant Professor, ODU
y2lu@odu.edu

Rui Ning, Ph.D,
Electrical & Computer Engineering, ODU (2020)
Research Assistant Professor, ODU
rning001@odu.edu

Daniel Shin, Juris Doctor
William & Mary Law School (2019)
Cybersecurity Researcher, W&M
dshin01@wm.edu

3. Results of Entrepreneurship and Workforce Programming Innovation, Workforce Development and Experiential Learning Programs

COVA CCI is supporting several programs in innovation, workforce development, and student experiential learning. These include the INNOVATE Cyber Challenge, graduate student experiential learning program (CyberExL), AccessCyber and Cybersecurity Internship Program.

Program	Funding
Innovate Cyber Challenge	$90,000
CyberExL	$100,000
AccessCyber	$30,000
Cybersecurity Internship Program	$41,565 [1]

[1] Internships were funded in FY 2020/2021 and this reflects total payments from October 2020 through December 2021.

a) **Innovate Cyber Challenge.** COVA CCI expanded the scope of the Innovate Cyber Challenge to include students from all state public 2- and 4-year institutions with the goal of selecting 50 students. The summer and fall were spent on recruiting students for spring 2022 cohort with a total of 54 students from 14 universities/colleges selected to start the program in January 2022.

This program groups the students into teams and each team is assigned a cybersecurity problem/challenge. Over the course of the semester the teams will use design thinking to come up with unique solutions for this problem and present their final product during a Showcase event in April 2022.

Visit the COVA CCI/Innovation/Innovate Cyber Challenge webpage to see previous projects.

b) **Graduate student experiential learning program (CyberExL).**
COVA CCI moved the management of its graduate student experiential learning program to William & Mary where it is managed by Dr. Stephanie Blackmon, William & Mary School of Education. The program was rebranded as CyberExL and the first cohort of graduate students will start working with their respective organizations in January 2022. A total of sixteen students were selected in fall 2021 to support several programs/research projects, including the Global Fund to End Modern Slavery, Peregrine Technical Solutions, COVA CCI AccessCyber, Camp Community College, COVA CCI Innovate Cyber Challenge, and two research projects, Cyber Risk Management and Analytics led by Dr. Chon Abraham, William & Mary, and Crowed sourced Review Manipulation Attacks Online platforms led by Dr. Faryaneh Poursardar, Old Dominion University. Additional information can be found on the COVA CCI/Talent Development/Experiential Learning Program website.

To learn more about the programs and students selected for the Spring 2022 cohort see this article – [CCI's CyberExL Program is giving graduate students hands-on experience.]

c) **AccessCyber.** COVA CCI provided $30,000 in funding to William & Mary to conduct an evaluation of COVA CCI experiential learning programs and curriculum materials. This program is called AccessCyber. The information will be complied into a database which can be used to amplify access to the curriculum and experiential learning opportunities across the COVA region, analyze access to the materials and opportunities to strategically address gaps in outreach, and impact the representative COVA communities by providing greater access to cybersecurity materials and opportunities. The ultimate goal is to develop a work product that can be shared across all CCI regions.

d) **COVA CCI Cybersecurity Internship Program.** COVA CCI is partnering with the Virginia Space Grant Consortium (VSGC) to manage the COVA CCI Cybersecurity Internship Program using their Commonwealth STEM Industry Program (CSIIP). VSGC will leverage CSIIP to build and improve on the relationships with employers across the Commonwealth to develop internship and experiential learning opportunities.

To date twenty-one (21) students from 6 universities/colleges have been placed with eleven (11) companies. See the [COVA CCI/Talent]

Development/Cybersecurity Internships website for additional information and links to the CSIIP website.

Company	# of Interns
ARKS, Inc.	2
AScIS	2
Coronet Tech Enterprises, Inc.	2
DroneUp	1
Grey Gecko	2
IntellecTechs	3
Jenlyn Solutions	3
MI Technical Solutions	2
Peregrine	1
Universal Solutions International, Inc. (USI)	1
York County	2
Grand Total	21

University/College	# of Students
Christopher Newport University	2
Old Dominion University	13
Radford University	2
Thomas Nelson Community College	2
Tidewater Community College	1
William & Mary	1
Grand Total	21

4. Collaborative Partnerships and Projects

COVA CCI is working with academic institutions from across the state on Cybersecurity Research projects previously mentioned in this report. Researchers are also working with business partners on potential federal funding opportunities and current research. Some of these partners include CivilianCyber, MIBE, MITRE, MI Technical Solutions, Port of Virginia, and Peregrine Technical Solutions.

See the COVA CCI/Partners website for a list of current academic and business partners.

5. Correlated Economic Outcomes (Jobs and New Business Formation)

One the goals of CCI and COVA CCI is to grow the cybersecurity workforce in the Commonwealth. COVA CCI is working with university researchers to achieve this goal. Below are two examples how this is being accomplished.

Dr. Hongyi Wu, CCI Fellow and Director of Old Dominion University's School of Cybersecurity, is leading a project focused on growing Virginia's cybersecurity workforce by filling or creating over 1,300 jobs over the next five years. His project, "Cybersecurity Job Creation Systems," is being funded by the Growth and Opportunity Virginia (GoVA) in the amount of $1,45 million. Old Dominion University, working in partnership with George Mason University and the Eastern Shore Community College, along with over 40 additional partners, will recruit students, with an emphasis on veterans, to complete six specially designed courses which will enable

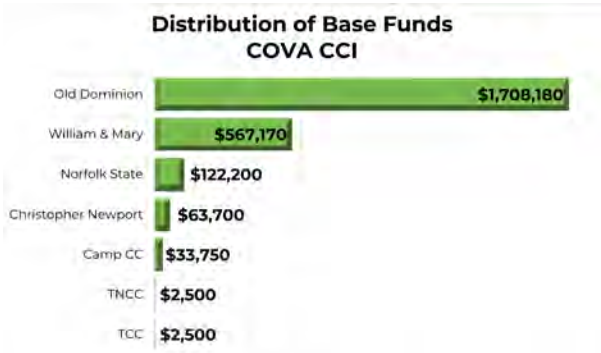
them to earn slakeable credentials to fill the multiple cybersecurity positions across the state. It is projected that over 1,300 students will complete this program during the next five years, generating over $12.6 million in tax revenue. Additionally, industry and academic partners have committed $2.9 million in cash and in-kind support. This project shows the value of combining the efforts of industry and academia to fill a critical workforce gap. Additional information regarding this project is available in this article – ODU Cybersecurity Job Creation System wins Government Innovation Award.

Another project highlighting the value of partnering with industry to expand the cyber workforce and cyber capabilities is the work supported by Dr. Sachin Shetty, CCI Fellow and Executive Director of the Center for Secure & Intelligent Critical Systems, Old Dominion University, in the development and the manning of the Port of Virginia's new Cybersecurity Operations Center. Dr. Shetty and his team from ODU, Longwood University, Virginia State University, and the University of Virginia, were awarded a CCI funded Experiential Learning project, "Cybersecurity Monitoring and Assurance Training Program for Safe and Secure Port Operations," to create a suite of experiential learning modules which the Port of Virginia will use to train cybersecurity interns, establishing a potential workforce pipeline. The first interns will start working with the Port in summer 2022. Additional information on this project is available in this article - ODU Helps to Guide Port of Virginia's New Cybersecurity Lab.

> Mr. Rich Ceci, Senior Vice President of Technology and Projects at the Virginia International Terminals, LLC said; *"Our recent work in the cybersecurity space has allowed us to leverage our relationship and involve very high-caliber academic expertise to meet an urgent need. Together we are building what will become a reference model for the entire U.S. port industry."* (ODU Helps to Guide Port of Virginia's New Cybersecurity Lab.)

6. Geographic Distribution of Awards from the Funds Contained in HB30

Distribution of COVA CCI Allocated Funds across the node region.

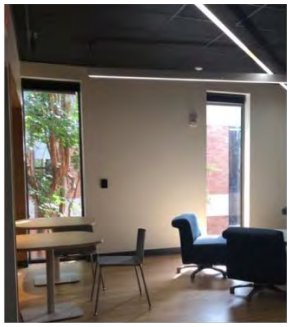


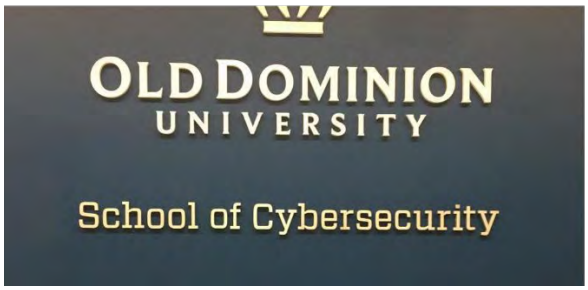
Distribution of Funds Across the Node Region	
Institution	Amount
Camp Community College	$33,750
Christopher Newport University	$63,700
Norfolk State University	$122,200
Old Dominion University *(Note 1)*	$1,708,180
Thomas Nelson Community College	$2,500
Tidewater Community College	$2,500
William & Mary	$567,170
Total Committed Funds	**$2,500,000**
Note 1: Funding under ODU includes funds managed by the ODU Research Foundation, Virginia Space Grant Consortium (VSGC), Research Scientists Salary, and other Operations Costs	
ODU RF Managed Projects	*$600,000*
Computer Lab Upgrades	*$75,000*
Curriculum Development	*$20,000*
VSGC Managed Projects	*$32,500*
Research Scientist Salaries	*$348,000*
PhD Fellow Program	*$25,000*
CoVA Cybersecurity Student Association	*$20,000*
Operations and other funds	*$587,680*
Total ODU Funds	*$1,708,180*

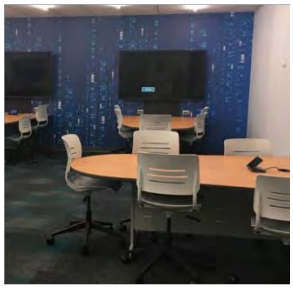
7. Other initiatives.

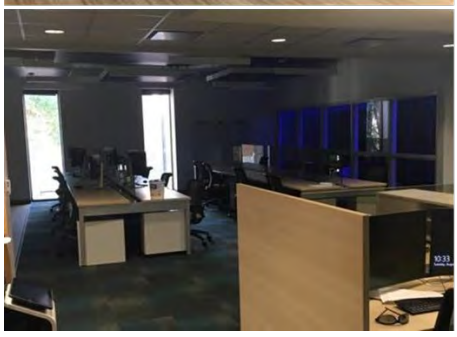
a) Cyber Innovation Park

Cyber Innovation Park opened in August 2021 as the new home to COVA CCI and ODU's School of Cybersecurity. It includes about 10,000 square foot space in Monarch Hall, for housing a data center, multiple research labs, teaching labs and classrooms, meeting space, faculty, offices, and a student cyber incubator. You can take a virtual tour of this space on the COVA CCI YouTube Channel.









b) COVA Shared Research Environment

COVA CCI invested $708,000 in FY 2020/2021 to create a shared collaborative research computing environment, known as COVA Share, to support the growing cybersecurity programs, academic and research collaboration opportunities, and industry partnerships. Guided by the researchers in the Coastal Virginia Center for Cyber Innovation, the computing center and network investment support the COVA Node and enable communication to the Hub and other Nodes. The environment lays a foundation to support 5G testbed data collection, secure , and transfer between connected Node members and to the CCI Hub for analysis and other collaboration. It provides access to a flexibly designed computing environment via connectivity improvements between ODU and William & Mary, and between ODU and Norfolk State University for potential collaborative efforts involving secure transfer of data between schools or secure remote access to physical or virtual hosts.

There are currently four (4) active projects on the COVA SHARE – Research Environment.

- Backdoor Detection and Mitigation in Deep Neural Networks
  - PI: Dr. Hongyi Wu, Old Dominion University
  - Machine learning using GPU capability
- Explore Privacy Preservation in Deep Image Retrieving Systems
  - PI: Dr. Qun Li, William & Mary
  - AI algorithm development with neural networks
- UNC Add Health Data Analysis
  - PI: Dr. Brandi Woodell, Old Dominion University
  - Analysis of Add Health Data using Stata
- Computer Science 734/834
  - PI: Dr. Jian Wu, Old Dominion University
  - Host 24 environments for students to develop web search engine

There are two (2) active projects on the COVA SHARE – Academic Environment.

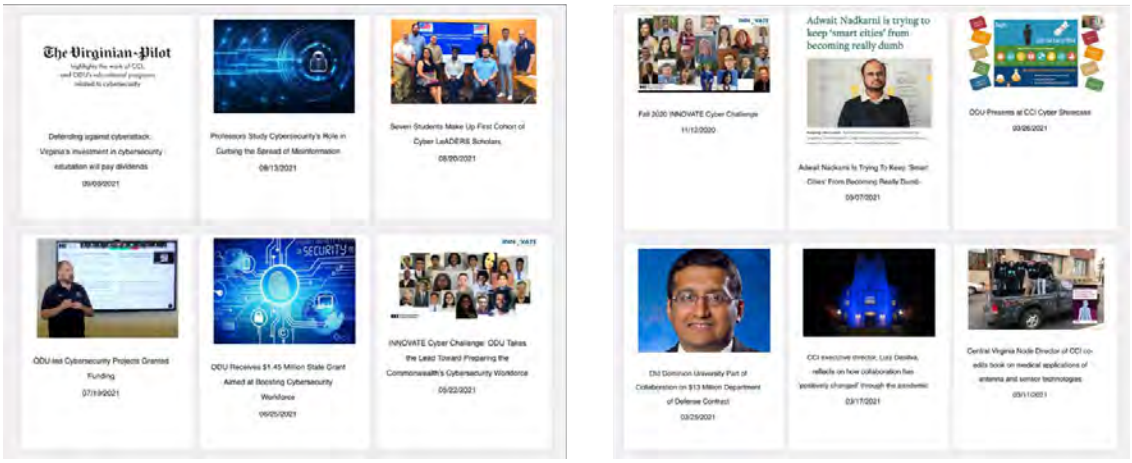
Dr. Jian Wu, Old Dominion University, used the COVA SHARE Academic Environment for two courses. The CS734/834 (Introduction to Information Retrieval) was offered in Fall 2021. The major activities included web crawling, deploying web-based user interfaces, and mining data using machine learning and information retrieval methods. Each of the nine groups was given a virtual machine with 2 cores, 16GB RAM, 40GB storage, Ubuntu, and a GUI interface. In the Spring 2022 semester, Dr. Wu is teaching CS450/550 (Database Concepts) with more than 40 students. It is expected that there will be 14-20 groups. Each student is given access to a

database that is not visible to the others. Students in a group share a database for the group project. In general, this infrastructure provided local access to a collaborative space for group projects. The maintenance team provided timely and quality service. Dr. Wu would like to use the infrastructure for more future courses, such as CS418/518 (Web Programming) and his CCI research project on misinformation and disinformation. Dr. Wu also hopes GPUs will be added into the infrastructure to facilitate integrating deep learning into courses, such as CS734/834 and a future course on Fundamentals of Deep Learning.

Professor Robert Tureman, Camp Community College, is working with the COVA SHARE support team to enable his community colleges students to gain access to virtual Linux, Kali, and Windows systems. One challenge the students have is access to Linux or Windows based networks. This environment allows the students to use virtual machines and simulations to improve their cyber, networking and program skills in a structured lab. Professor Tureman received additional COVA CCI funds under the Computer Lab Upgrade program to assist in building a scaled version of the COVA SHARE environment on the Camp Community College campus. This lab will include workstations and networking to promote student learning through simulation of networking issues and programming problems which require implementing cybersecurity tools.

Visit the COVA CCI/Research/COVA SHARE website for additional information on COVA SHARE and watch a short overview YouTube video – What is COVA Share? – to learn more about this resource.

8. COVA CCI Node in the News



COVA CCI has been activity promoting the success of its various activities through local news sources. Below is a list of relevant news stories from the past 6 months. You can view these articles and others on the COVA CCI website – News.

ODU News (January 21, 2022)
Cybersecurity Undergrads Benefit from ODU-Led Program

ODU News (January 10, 2022)
ODU Researchers Among Top 2% of Scientists in the World

ODU News (January 7, 2022)
ODU Cybersecurity Job Creation System Wins Government Innovation Award

ODU News (December 22, 2021)
ODU Helps to Guide Port of Virginia's New Cybersecurity Lab

ODU News (December 21, 2021)
Old Dominion University Earns Prestigious Research 1 Designation from Carnegie Classification of Institutions of Higher Education

CCI News (December 13, 2021)
CCI's CyberExL Program Is Giving Graduate Students Hands-On Experience

ODU News (November 21, 2021)
Wu Received VASCAN Founders Award for Cybersecurity Contributions

ODU News (November 11, 2021)
ODU Cybersecurity Student Wins National Capture the Flag Competition

CIRI (Critical Infrastructure Resilience Institute) News (November 8, 2021)
CIRI-developed CRISM tool selected for Homeland Startup Studio 2021 Program.

ODU News (November 4, 2021)
ODU, HRMC Announce Maritime Innovation Initiatives

The Virginian Pilot (September 8, 2021)
Defending against cyberattack: Virginia's investment in cybersecurity education will pay dividends

ODU News (August 8, 2021)
Professors Study Cybersecurity's Role in Curbing the Spread of Misinformation

ODU News (August 13, 2021)
Professors Study Cybersecurity's Role in Curbing the Spread of Disinformation

ODU News (August 27, 2021)
ODU Awarded NSF and NSA Cybersecurity Grants

ODU News (July 7, 2021)
ODU-led Cybersecurity Projects Granted Funding

ODU News (June 25, 2021)
ODU Receives $1.45 Million State Grant Aimed at Boosting Cybersecurity Workforce

10. For additional information contact John Costanzo, Chief Administrative Officer, COVA CCI, jcostanz@odu.edu, or visit the COVA CCI website (https://covacci.org) and the Commonwealth Cyber Initiative website (https://cyberinitiative.org/).