Fiscal Year 2022 Annual Report to

The Secretary of Commerce and Trade

The Chair of the House Appropriations Committee

The Chair of the Senate Finance and Appropriations Committee

The Director of the Department of Planning and Budget

The Virginia Innovation Partnership Authority (VIPA)

THE COMMONWEALTH CYBER INITIATIVE: FISCAL YEAR 2022 REPORT

Commonwealth Cyber Initiative

September 26, 2022

Message from the Executive Director

As new programs in cybersecurity pop up around the country and the world, the Commonwealth Cyber Initiative (CCI) remains unique in our focus on economic diversification and development through interconnected mission lines of workforce development, innovation, and research. Virginia had the foresight of creating CCI in 2018 and remains a leader in major cybersecurity initiatives.

The results are clear: Virginia universities and colleges are collaborating as never before and are now competitive for multi-million dollar research contracts focusing on securing our infrastructure and communications networks. CCI's workforce development programs, such as those focusing on internships and apprenticeships, attract hundreds of applications from an extremely diverse cohort. And our innovation initiatives include incubating new cyber startups, empowering existing ones, and forming the next generation of entrepreneurs.

In this past fiscal year, our researchers brought in an astounding $38 million in new research grants and contracts. This strong return on investment is just the beginning: a study by RTI International estimated that in its first two years CCI was responsible for creating more than a thousand jobs and contributing more than $200 million to Virginia's Gross Domestic Product (GDP).

This report summarizes our major activities in Fiscal Year 2022 (FY22) and outlines our plans for the next year. We had an amazing year and have all indications that our results will continue to improve. Our focus, the intersection of cybersecurity, autonomy, and intelligence, is more relevant than ever, and we are achieving our vision of positioning Virginia as a global leader in cybersecurity.

I would like to take the opportunity to thank the many researchers, staff, industry, and government partners who have made these results possible and I look forward to another banner year!

Luiz DaSilva, Ph.D.; Fellow, IEEE

Executive Director, Commonwealth Cyber Initiative

Bradley Professor of Cybersecurity, Virginia Tech

Executive Summary

The Commonwealth Cyber Initiative (CCI) was established under the enabling authority of the Appropriation Act - Item 252.B7, Special Session I, 2018. Its objective is "to serve as an engine for research, innovation, and commercialization of cybersecurity technologies, and address the Commonwealth's need for growth of advanced and professional degrees within the cyber workforce" (Virginia State Budget, 2018).

Our ambitious vision is to establish Virginia as a global leader in cybersecurity, and by doing so, help diversify the economy of the commonwealth, attracting private investment and jobs.

Fiscal Year 2022 (FY22) was our most productive year yet: research funding from sources outside the commonwealth continued to grow, and we have substantially expanded our workforce development and innovation programs. Virginia is unique in the country in establishing this large-scale collaboration among 41 institutions of higher education, and the investment continues to pay off in jobs (and, crucially, a skilled workforce that can fill those jobs!), spin-outs and startups, and the reputation of our academic institutions.

This report highlights some of the major accomplishments from the past fiscal year, which are indicative of what the CCI network is achieving for the commonwealth.

New Research Grants. CCI researchers brought in $38 million in new research grants and contracts to Virginia in FY22. This astounding success comes from our depth and breadth of expertise in cybersecurity and is enabled by the unique research facilities that CCI has established. We are now competitive for large-scale funding in key areas such as securing the next generation of communication networks, sometimes referred to as Next G. CCI researchers are uniquely positioned to contribute to national priorities such as Open Radio Access Network (O-RAN), a topic for which the recent CHIPS and Science Act has authorized an investment of $1.5 billion. Many of our research projects have a strong hands-on, testbed component, providing students (pictured) with valuable practical skills in the design and deployment of secure systems.

Intra-Network Collaboration. The secret sauce to what CCI is achieving is the collaboration that flourishes among our universities and colleges. A recent report from RTI International points out: "The research profile of Virginia universities has grown at a rate outpacing national averages, but they are still small as individual institutions. CCI can serve as a valuable convener to help universities collaborate to elevate their research profile." We are doing exactly that. As an example, we recently received a planning grant from the National Science Foundation (NSF) to build the first industry-university center in Next G: four CCI universities, Old Dominion University (ODU), George Mason University (Mason), Virginia Commonwealth University (VCU), and Virginia Tech (VT), were

funded, and our proposal included letters of collaboration from 52 industry partners. To build additional partnerships, our first network-wide CCI Symposium (pictured) took place in April 2022 in Richmond, bringing together 200 faculty members and students.

Research and Innovation Infrastructure. The family of CCI testbeds continues to grow. This year, we inaugurated three new testbeds at VCU. The medical device security testbed is outfitted with real commercial medical devices that are tested for security vulnerabilities and used to develop mitigation solutions. The OpenCyberCity testbed (pictured) is a realistic, small-scale cityscape in which to run experiments related to smart cities and autonomous vehicles. It has a fully operational water treatment plant, miniature Uncrewed Autonomous Vehicles (UAVs), and a range of smart city sensors. And, complementing CCI's xG testbed, VCU now has an isolated environment where we can conduct 5G and Next G experiments without causing or suffering interference. The CCI Northern Virginia (NoVA) Node added two commercial grade testbeds in addition to three open-source testbeds that were instantiated the previous year. The suite of testbeds enables self-contained, mobile architecture independent of commercial providers to support numerous physical system applications ranging from autonomous vehicle and transportation systems to manufacturing and supply chain. CCI's research facilities are used for research, experiential learning, and to inspire entrepreneurship and spin-out companies.

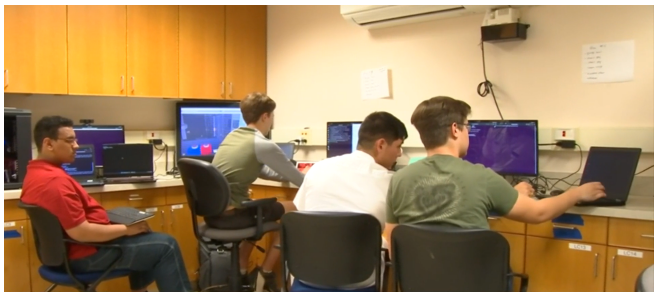
New Research Frontiers. In FY22, we refreshed our major research themes, taking into consideration workforce needs, researcher expertise, and potential for funding, innovation, and partnership with industry. Our new research themes are "Securing the Next Generation of Networks" and "Securing Human-Machine Interactions." The goal of the former is to position CCI to play a leading role in the secure deployment of 5G and in the vision for Next G. It includes research areas such as open interfaces and standards, virtualization and network disaggregation, secure and flexible use of spectrum, integration of cyber physical systems, and quantum communications. In this context, the CCI Southwest Virginia (SWVA) Node seeded the launch of a new Center for Quantum Information Science and Engineering (lead researchers pictured) at VT, which has already been very successful in attracting major research funding and publishing contributions in some of the top journals in the area. The second research theme, Securing Human-Machine Interactions, focuses on the technological challenges in securing an enhanced digital experience. Building on CCI's philosophy of cybersecurity as inherently multi-disciplinary, this theme deals with research areas such as ethical cybersecurity, the metaverse, Artificial Intelligence (AI) assurance, and security and privacy for embedded devices.

Rich Experiential Learning. We are particularly proud of the experiential learning programs that CCI continues to create. This year, the CCI NoVA Node launched a new apprenticeship program. In the first cohort (pictured) we are funding 21 apprentices for seven weeks of full time training and 12 weeks of apprenticeships. Hosts include Arlington County, Peraton, InterSec, DEKRA, and Sedulous, with additional companies being onboarded. Many of the apprentices are transitioning from other careers, and the expectation is that they will receive offers of full-time employment from the hosts. This year we also launched new experiential programs in sectors related to election security, privacy pro-

tection, and digital forensics. Two of these programs are in partnership with the Virginia Board of Elections and the Virginia State Police. Two aspects that are common to all these experiential learning programs deserve to be highlighted: the level of interest from students and professionals, and the diversity of the cohorts. Take the apprenticeship program as an example: we had 400 applicants for 21 positions; among the selected apprentices, 43 percent are female, 19 percent are veterans, and 90 percent identify with underrepresented groups in science and engineering. There are clear lessons: (1) making rich experiential learning opportunities available to all can substantially contribute to diversifying the cyber workforce; and (2) there is tremendous opportunity to scale up all these programs.

Spin-outs and Startups. We are now directly supporting work in dozens of cyber startups in Virginia (the logos on the left represent a sample). These engagements vary from internships paid by CCI to funding for translational research in collaboration with CCI faculty members. This year saw the emergence of two CCI spin-outs: *Symple Solutions* leverages Field Programmable Gate Array (FPGA) technology for verifiability of critical cyber-physical systems; and *Virtual PLC* provides automation of collection and analysis of adversarial data for critical infrastructure customers. Both received seed funding from the CCI Central Virginia Node (CVN) and are part of VCU's Dreams 2 Reality incubator. This year we also launched the CCI Incubator and Accelerator (CCI+A) program. Led by the CCI NoVA Node and co-funded by the CCI Hub, the Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology (CATAPULT) fund provided $50,000 grants to eight new translational research projects led by CCI faculty. These projects are either conducted in partnership with existing startups or aim at creating new spinout companies. Startups participating in the CCI+A program participate in a rigorous program designed to expedite the commercialization, and also receive mentorship from volunteer industry experts, free legal and business consulting, and access to rent-free space in the Digital Innovation Pilot facility at Mason.

Internships, from High School to Grad School. CCI now funds a range of paid internships. Two of these programs are aimed at high-school students, including those who are home-schooled: In SWVA, seven students are paired with Virginia Military Institute (VMI) cadets to work on hardening Internet of Things (IoT) devices such as Google Home and Alexa-enabled devices (pictured). In NoVA, our summer 2021 internship program for high school juniors and seniors received 110 applications for 20 positions, leading us to increase the number of positions to 30 in summer 2022. The CCI Hub funded, for the third year in a row, our Cyberstartups program hosted and run by Mason and leveraging the participation of the entrepreneurs incubating in their Mason Enterprise Centers across the region. The program provides stipends for undergraduate and graduate student internships in Virginia startups focusing on cybersecurity with host companies also providing matching resources. We also continue to fund cybersecurity internships as part of the Commonwealth STEM Industry Internship Program (CSIIP), resulting in 54 placements in 13 companies: 42 percent of these interns are women, 17 percent are military veterans, and 50 percent are persons of color; we find



that 91 percent of interns remain in the cybersecurity field after their internships. Finally, the second CCI Internship Fair took place in October 2021, with 300 students participating in the two-day virtual event, which included industry booths, interviews, and job panels.

The Next Generation of Entrepreneurs. We view forming the next generation of business creators as an important component of our innovation mission. In the first week of January 2022 we welcomed 25 students to our Arlington hub for one week of intensive training in CCI's inaugural Innovation Boot Camp. The event, facilitated by BMNT, exposed students to innovative business practices used in Hacking4X courses across the country to tackle real-world problems from government and industry challenge sponsors. Challenge sponsors included CACI International, the Cybersecurity and Infrastructure Security Agency (CISA), and the Virginia Office of Public Safety and Homeland Security. Additionally, the CCI Coastal Virginia (CoVA) Node led our third cohort of the Innovate Cyber program, opening the program to students from all two- and four-year institutions represented in CCI. A total of 54 students from 14 universities and colleges learned about design thinking and worked in multi-institution teams to devise products to improve cyberhygiene.

CCI funding is distributed to researchers through open calls for proposals issued both by the Hub and the Nodes. Proposals are peer-reviewed and final recommendations made by CCI's Leadership Council. This ensures that the best ideas, aligned with CCI's mission, are selected for funding in an open and transparent manner.

We continue to be advised by a highly distinguished Technical Advisory Board (TAB), with representatives from industry, state and federal government, academia, and the innovation ecosystem. Some major goals for the coming fiscal year include:

- Continuing to develop cross-disciplinary approaches to cybersecurity, focusing on the research theme of securing human-machine interactions and exploring technical, legal, social, and public policy aspects.
- Strengthening and supporting multi-institution teams in Virginia to compete for large-scale research and workforce development grants from the federal government and industry.
- Expanding our innovation programs, connecting our researchers with venture capital, and continuing to align our innovation initiatives with those available through the Virginia Innovation Partnership Corporation (VIPC) and other sources.
- Scaling up our internship and apprenticeship programs.
- Extending our research infrastructure with a new outdoor 5G and Next G testbed using Citizens Broadband Radio Service (CBRS) licensed spectrum.
- Raising our profile and building new partnerships nationally and internationally.

CCI is now three years old. The level of maturity in our workforce development and innovation programs is noticeable, and the collaborations between universities are stronger than ever. The commonwealth's leadership deserves credit for having the foresight of establishing this initiative years ago and for their continued focus on cybersecurity as a critical area for Virginia. Our results to date show how we can be an engine for the commonwealth's economic development.

List of Figures

List of Tables

List of Acronyms

3GPP 3rd Generation Partnership Project

AI Artificial Intelligence

API Application Programming Interface

CATAPULT Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology

CBRS Citizens Broadband Radio Service

CCF Commonwealth Commercialization Fund

CCI Commonwealth Cyber Initiative

CCI+A CCI Incubator and Accelerator

CERS Computer Evidence Recovery Section

CFP Call for Proposals

CISA Cybersecurity and Infrastructure Security Agency

CISA Cybersecurity and Infrastructure Security Agency

CoVA Coastal Virginia

CPS Cyber Physical System

CSIIP Commonwealth STEM Industry Internship Program

CTIA CTIA - The Wireless Association

CTO Chief Technology Officer

CVN Central Virginia Node

CyManII Cybersecurity Manufacturing Innovation Institute

DARPA Defense Advanced Research Projects Agency

DEEPSECURE Development and Experimental Environment for Privacy-preserving and Secure

DHS Department of Homeland Security

DNS Domain Name System

DoD Department of Defense

DoE Department of Energy

FCC Federal Communications Commission

FPGA Field Programmable Gate Array

FY21 Fiscal Year 2021

FY22 Fiscal Year 2022

FY23 Fiscal Year 2023

GDP Gross Domestic Product

Mason George Mason University

GSMA Global System for Mobile Communication Association

HBCU Historically Black Colleges and Universities

HR Human Resources

IDC Inclusion & Diversity Committee

IDS Intrusion Detection System

IoT Internet of Things

IP Intellectual Property

IUCRC Industry-University Cooperative Research Center

LC Leadership Council

MEC Multi-access Edge Computing

ML Machine Learning

MSI Minority Serving Institution

MWC Mobile World Congress

NICE National Initiative for Cybersecurity Education

NoVA Northern Virginia

NOVACC Northern Virginia Community College

NSA Non-Standalone

NSF National Science Foundation

NSU Norfolk State University

ODU Old Dominion University

ONR Office of Naval Research

O-RAN Open Radio Access Network

P2P Peer to Peer

PAL Priority Access License

PI Principal Investigator

RAN Radio Access Network

ROS Robot Operating System

SAS Spectrum Access System

SDR Software Defined Radio

SME Small and Medium Enterprise

STEM Science, Technology, Engineering, and Mathematics

SWVA Southwest Virginia

TAB Technical Advisory Board

TEIM Technology Enabled Internships with Mentoring

TPC Technical Program Committee

UAV Uncrewed Autonomous Vehicle

UVA University of Virginia

V2X Vehicle-to-everything

VCU Virginia Commonwealth University

VIPA Virginia Innovation Partnership Authority

VIPC Virginia Innovation Partnership Corporation

VMI Virginia Military Institute

VPRI Vice President for Research and Innovation

VSGC Virginia Space Grant Consortium

VSP Virginia State Police

VT Virginia Tech

VT-ARC Virginia Tech Applied Research Corporation

VTF Virginia Tech Foundation

VTRC-A Virginia Tech Research Center - Arlington

VTTI Virginia Tech Transportation Institute

WISPER Center for Wireless Innovation towards Secure, Pervasive, Efficient and Resilient Next Generation Networks

W&M William & Mary

xG Next Generation Networks

Contents

https://www.overleaf.com/project/629f6db60ccb541ed76eb079

Chapter 1

The Commonwealth Cyber Initiative

This chapter outlines CCI's vision and mission lines, describes the organization of the network and our advisory group, and outlines the structure for the remainder of the report.

1.1 Vision and Mission

CCI Vision

To establish Virginia as a **global center of excellence** in cybersecurity research and serve as a **catalyst for the commonwealth's economic diversification** and long-term leadership in this sector.

CCI's mission encompasses **research**, **workforce development**, and **innovation** at the intersection between **cybersecurity, autonomy, and intelligence**.

This report describes our progress in each of the mission lines in FY22, in pursuit of the vision of global leadership in cybersecurity for the Commonwealth of Virginia.

1.2 The CCI Network

CCI was established under the enabling authority of the Appropriation Act - Item 252.B7, Special Session I, 2018. Its objective is "to serve as an engine for research, innovation, and commercialization of cybersecurity technologies, and address the Commonwealth's need for growth of advanced and professional degrees within the cyber workforce" (Virginia State Budget, 2018).

1.2.1 An Evolving Network

In FY22, Patrick & Henry Community College joined CCI as part of the SWVA Node, growing our network to **41** institutions of higher education across Virginia, depicted in Figure 1.1.

The leadership structure of CCI comprises a hub and four regional nodes. VT serves as the anchoring institution for the hub and coordinates the strategy and activities of the network; the hub is hosted in VT's facilities in Arlington. CCI's Central Virginia Node (CVN) is led by VCU, the Coastal Virginia Node (CoVA) is led by ODU, the Northern Virginia (NoVA) Node is led by Mason, and the Sothwest Virginia Node (SWVA) Node led by VT. The CCI Hub is led by an executive director, assisted by the managing director. Each of the four CCI nodes is led by a node director. Together, they form the CCI Leadership Council (LC), which is responsible for setting the strategy and executing the CCI program. An external Technical Advisory Board (TAB), described further Section 1.3, advises CCI on strategy and programs. The Virginia Innovation Partnership Authority (VIPA) provides oversight for CCI, as one of the commonwealth's centers of excellence. The governance structure is depicted in Figure 1.2.

The CCI executive director chairs the Leadership Council (LC) and is responsible for articulating the research agenda and the innovation and workforce development strategy for the network. The CCI Hub

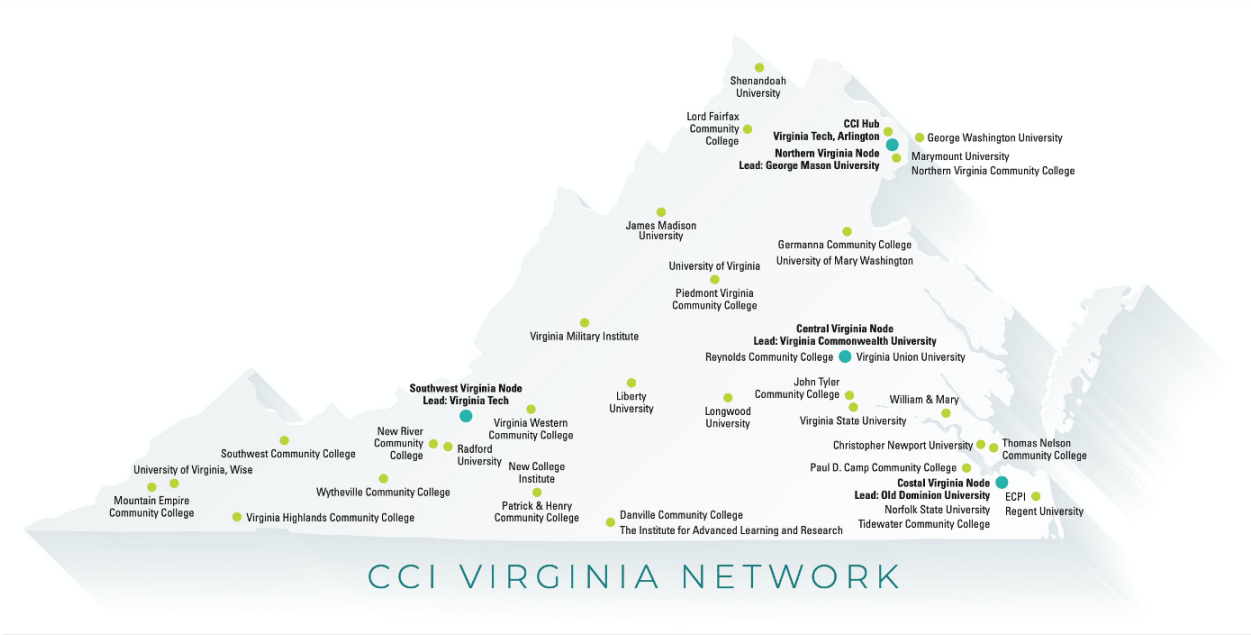


Figure 1.1: The CCI network comprises 41 institutions of higher education across Virginia. Patrick & Henry Community College is the latest member to join.

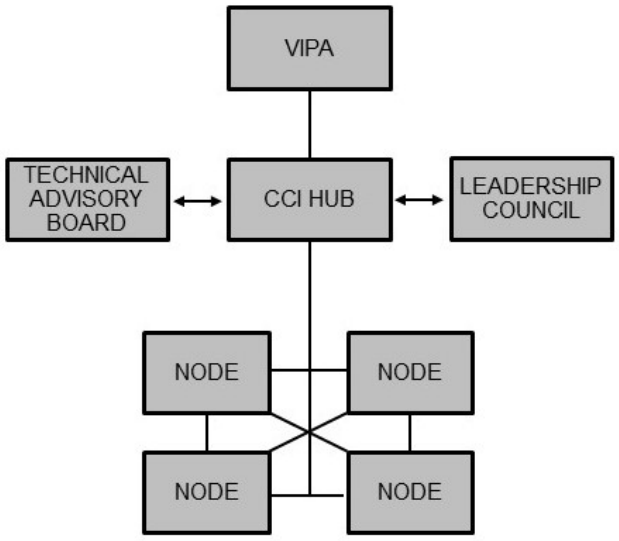


Figure 1.2: CCI governance structure.

designs, coordinates, and funds network-wide programs and deploys key research infrastructure available to all CCI researchers. The hub also houses faculty and graduate students with established expertise in key research areas in cybersecurity, autonomous systems, and intelligence. A communications team in the hub is responsible for external dissemination of CCI activities and successes. Finally, the hub convenes teams throughout the network to put together large, multi-million dollar research proposals for external funding. The CCI Regional Nodes are responsible for developing capacity in research, innovation, and workforce

development in their respective geographic regions, establishing leadership in key focus areas. They also recruit eminent faculty and promising junior faculty for their member institutions and fund programs in the node, as well as collaborations across multiple nodes. The main roles of the hub and the nodes are summarized in Figure 1.3.

HUB	NODES
○ Chairing the Leadership Council and mapping out the CCI research agenda, innovation and workforce development strategy ○ Developing and coordinating network-wide CCI programs ○ Investing in shared research infrastructure ○ Establishing and supporting expertise in the hub in key research areas ○ Providing funding for some network-wide programs ○ Communicating CCI activities and successes ○ Supporting major, high-risk center-level proposal efforts	○ Developing regional capacity in research, innovation and commercialization, and workforce development ○ Establishing each node's identity and leadership in key focus area(s) ○ Building up research capacity through recruitment of eminent faculty and/or promising junior research faculty ○ Funding programs in the node and collaborations across multiple nodes

Figure 1.3: Roles of the CCI Hub and Nodes.

The CCI executive director, managing director, and the four node directors form the CCI Leadership Council (LC), depicted in Figure 1.4. Dr. Luiz DaSilva serves as CCI executive director and holds the position of Bradley Professor of Cybersecurity at VT. Mr. John Delaney, former Chief of Staff for the US Army Cyber Command, is CCI's managing director. Dr. Liza Wilson Durant serves as NoVA node director; she is also a professor and Associate Provost for Strategic Initiatives and Community Engagement at Mason. Dr. Brian Payne serves as CoVA node director; he is also vice provost for Academic Affairs at ODU. Dr. Erdem Topsakal serves as CVN director; he is also a professor and Interim Senior Associate Dean at VCU. Dr. Gretchen Matthews serves as SWVA node director; she is also a professor in the Department of Mathematics at VT. The LC meets virtually every other week and in person for a full-day meeting once per quarter. The in-person meetings rotate between nodes, allowing the LC to meet researchers and visit infrastructure in each of the nodes.

1.2.2 CCI Hub Organization

The CCI Hub is led by the executive director, in close collaboration with the managing director. Prof. Jeff Reed, Willis G. Worcester Professor in the Bradley Professor of Electrical and Computer Engineering at VT, serves as CCI's Chief Technology Officer (CTO), providing advice and leadership of the research focus areas of the initiative. The managing director leads the administrative team for the CCI Hub, including a portfolio director leading the innovation and workforce development missions, a communications and marketing director, a program coordinator in charge of pre-award funded research, and a Human Resources (HR) generalist. The director of CCI's xG testbed, as well as hub research faculty, report to the executive director. The organizational structure of the CCI Hub is shown in Figure 1.5.

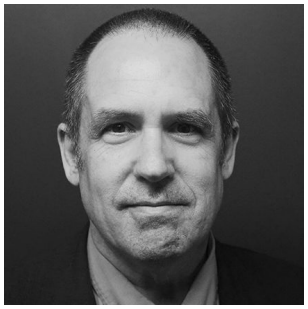
The CCI Hub occupies dedicated space in Virginia Tech's Arlington Research Center for CCI personnel, laboratories, and an xG testbed. We significantly expanded the xG testbed in FY22, with the installation of 72 radios, shown in Figure 1.6. This is the largest testbed of its kind, with the latest generation of software-defined radios and an end-to-end open implementation of 5G, with capabilities to test new technologies expected beyond 5G.

1.2.3 CCI Node Organization

Each of the CCI nodes is led by a node director, as depicted in Figure 1.4. The regional nodes have an extremely lean administrative structure, with each node director assisted by a program manager.

(a) Dr. Luiz DaSilva, Executive Director.

(b) Dr. Gretchen Matthews, SWVA Node Director.



(c) Dr. Brian Payne, CoVA Node Director.

(d) Dr. Erdem Topsakal, CVN Director.

(e) Dr. Liza Wilson Durant, NoVA Node Director.

(f) Mr. John Delaney, Managing Director.

Figure 1.4: CCI Leadership Council.

Commonwealth Cyber Initiative

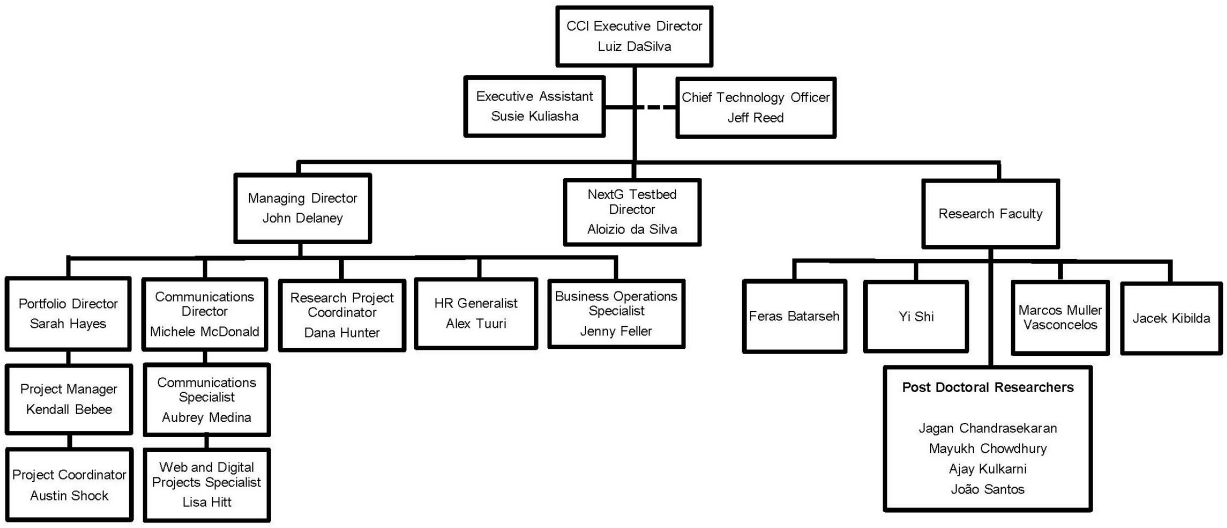


Figure 1.5: CCI organization chart.

In FY22, ODU inaugurated new facilities that house their School of Cybersecurity as well as the CCI CoVA Node. The facilities include classrooms, collaborative spaces and state-of-the-art labs, depicted in Figure 1.7.

(a) Setting up the xG testbed.

(b) xG testbed, with 72 latest generation software defined radios.

Figure 1.6: Setting up the expanded xG testbed in the CCI Hub.

Figure 1.7: New facilities at ODU house the CCI CoVA Node and the School of Cybersecurity.

We also inaugurated three new testbeds at VCU, developed under the leadership of the CVN Director, Erdem Topsakal. The new testbeds include:

- The NextG Testbed, which provides radio silence allowing for 5G experiments in an isolated environment.
- The Medical Device Security Testbed, which allows testing of commercial medical devices to locate and provide suggestions for the mitigation of vulnerabilities.
- The OpenCyberCity Testbed, which provides a realistic, small-scale cityscape in which to run experiments related to smart cities and autonomous vehicles.

A 1:12 scale model, the OpenCyberCity (Figure 1.8) is a smart city testbed where students can learn about several aspects of modern smart cities. The testbed consists of data collection and processing units, database management, distributed performance management algorithms, and real-time data visualization. The OpenCyberCity Testbed connects to the Medical Device Security Testbed through a firewall. Wearable devices, beds, and other gear equipped with sensors could help more people age in place. The NextG Testbed is the place to evaluate the networked underpinnings of many of the advanced applications in smart cities and medical devices. Researchers are working on characterizing the emitted signals of medical devices under attack, which will help create detection systems to secure medical devices in networked healthcare environments.

The CCI Northern Virginia Node added two commercial grade testbeds in addition to three open-source testbeds that were instantiated the previous year. The suite of testbeds enables self-contained, mobile architecture independent of commercial providers to support numerous physical system applications ranging from autonomous vehicle and transportation systems to manufacturing and supply chain. Collectively, these testbeds enable collaboration across regions and institutions and expand our capacity to compete for large scale R&D efforts.

Figure 1.8: OpenCyberCity testbed in the CCI Node at VCU.

1.3 The CCI Technical Advisory Board

The Technical Advisory Board (TAB) is a key component of our governance structure, shown in Figure 1.2, providing advice and guidance on strategic direction for CCI. CCI's TAB has been in place since Fall of 2020.

The composition of the TAB is as follows:

- One Vice President for Research and Innovation (VPRI) from one of the institutions of higher education in CCI;
- One member appointed by the VIPA board or the VIPC;
- Two representatives from industry;
- One representative from the start-up and innovation ecosystem;
- Two leading academic researchers from outside Virginia; and
- One representative from government.

We are fortunate to have an extremely distinguished inaugural TAB. Its members are (Figure 1.9):

- Prof. Elisa Bertino, Samuel D. Conte Professor, Purdue University;
- Mr. David Ihrie, Chief Technology Officer, CIT;
- Prof. Melur (Ram) Ramasubramanian, Vice President for Research, University of Virginia (UVA);
- Prof. Sennur Ulukus, Anthony Ephremides Professor, University of Maryland College Park;
- Ms. Tracy Gregorio, Chief Executive Officer, G2Ops;
- Mr. Jim Mollenkopf, Vice President, Qualcomm;
- Mr. Zachary Tudor, Associate Lab Director, Idaho National Laboratory; and
- Mr. Dan Woolley, Strategic Partnerships Director, The MITRE Corporation.

(a) Prof. Elisa Bertino.

(b) Mr. David Ihrie.

(c) Prof. Melur (Ram) Ramasubramanian.

(d) Prof. Sennur Ulukus.

(e) Ms. Tracy Gregorio.

(f) Mr. Jim Mollenkopf.

(g) Mr. Zachary Tudor.

(h) Mr. Dan Woolley.

Figure 1.9: CCI Technical Advisory Board (TAB).

The full TAB meets once a year. FY22's meeting, held on June 21, 2021, focused on a refresh of CCI's main research themes. The TAB also formed a sub-committee to select the winner of the CCI Impact Award 2022. The award recognizes an individual, team, group, or organization who, through their CCI activities, has conducted breakthrough cybersecurity research or innovation or developed a creative means to improve cybersecurity workforce opportunities for our industry partners and students. This year's award was presented to Duminda Wijesekera, a CCI Fellow from Mason.

All meetings of the TAB in the past two years have been conducted in virtual mode. In Fiscal Year 2023 (FY23), we are planning to meet in hybrid mode, with TAB members able to tour some of the CCI research facilities.

1.4 The CCI Inclusion and Diversity Committee

To increase the participation of under-represented groups in the cyber workforce is one of the strategic goals of CCI:

Strategic Goal

CCI will contribute to increasing the diversity of the cybersecurity workforce, so that the composition of that workforce approximates the gender, racial, and ethnicity distribution of the nation's population. It will also foster a culture of inclusion in the work environment, where everyone is treated fairly and respectfully, regardless of age, gender, ethnicity, religion, disability, or sexual orientation.

To fulfill this strategic goal, CCI has established an Inclusion & Diversity Committee (IDC) with the role of advising the LC on matters of inclusion and diversity. The committee itself has diverse representation from CCI-affiliated institutions throughout the commonwealth. The role of the committee is to advise CCI's LC on matters of inclusion and diversity, including:

- The establishment of programs that aim at increasing participation of underrepresented groups in the cyber workforce;
- Diversity goals and considerations in all programs funded by CCI;
- Organization of seminars, workshops, and training events that highlight diversity issues of particular relevance to CCI research, such as gender and racial bias in AI systems, and consideration of persons with disabilities in the design of autonomous systems;

- Outreach activities geared towards underrepresented groups in Science, Technology, Engineering, and Mathematics (STEM).

The inaugural IDC is chaired by Dr. Aurelia Williams, professor and director of the Cybersecurity Complex at Norfolk State University (NSU). Additional members are:

- Ms. Jeniffer Allen, CCI program coordinator, CVN;
- Dr. Nathan Carter, chief diversity, equity, and inclusion officer, Northern Virginia Community College (NOVACC);
- Dr. Tracy Lewis, associate professor, Department of Information Technology, Radford University;
- Ms. Michele McDonald, CCI director of communications and marketing;
- Dr. Joseph Simpson, collegiate assistant professor of management and director of the Integrated Security Education and Research Center, VT;
- Dr. Daniela Zhao, associate professor, Department of Computer Science, ODU.

In its first year, the CCI Inclusion and Diversity Committee created the "first stop" in a webinar series dedicated to informing, addressing, and increasing diversity in the cybersecurity field. The first webinar, held in October 2021, featured an inspiring keynote by renowned scholar and National Academy of Education President Gloria Ladson-Billings. The keynote was followed by a panel discussion offering how-to tips to increase diversity within the cybersecurity field.

The committee also hosted Wayne A. Scales, J. Byron Maupin Professor of Engineering at Virginia Tech, at the inaugural CCI Symposium. Scales presented how Virginia Tech researchers are partnering with Historically Black Colleges and Universitiess (HBCUs) and Minority Serving Institutions (MSIs). Scales discussed how CCI researchers can apply some of the same approaches to add diversity and value to their work by collaborating with HBCUs and MSIs.

In addition, the committee developed a demographic survey to help the CCI network track how well we're doing with our outreach efforts.

1.5 CCI Communications

1.5.1 CCI Social Media Strategy, Website, and Metrics

CCI's engaged audience is hungry for more information about what we're accomplishing across Virginia in workforce development, innovation, and research.

We're meeting the challenge with informative social media posts, monthly newsletters, lively graphics, news stories, videos, photos, direct emails, and an ever-expanding website to support our robust selection of programs and events.

This fiscal year, CCI continued building upon a strong start that began in Fiscal Year 2021 (FY21) with the creation of social media accounts and a new website. Figure 1.10 shows the evolution of our social media followers for LinkedIn, Twitter, YouTube and Instagram, accounts over the past fiscal year.

As more events moved from online to in-person, we created a photo library with images of CCI researchers and students in the field, meeting in small groups, collaborating, and generally furthering our mission. We started a Flickr account to share photos with the CCI network. We're particularly delighted to have four videos from Spring 2022 that feature our mission and researchers.

LinkedIn, with its focus on business, is our top social media account. It's where we celebrate the accomplishments of our researchers, students, and partners, along with sharing news. We had 1,027 followers at the end of FY22, a 168 percent increase from FY21. Our Twitter account grew to 384 followers, a 64.8 percent increase from the prior year. The social media metrics for our Twitter and LinkedIn accounts in FY22 are shown in Figures 1.11 and 1.12, respectively.

FY22 is our first full year having a website presence. As shown in Figure 1.13, FY22 website users grew 13.8 percent from the prior year to 29,002 users for the year (accounting for three fewer months of website

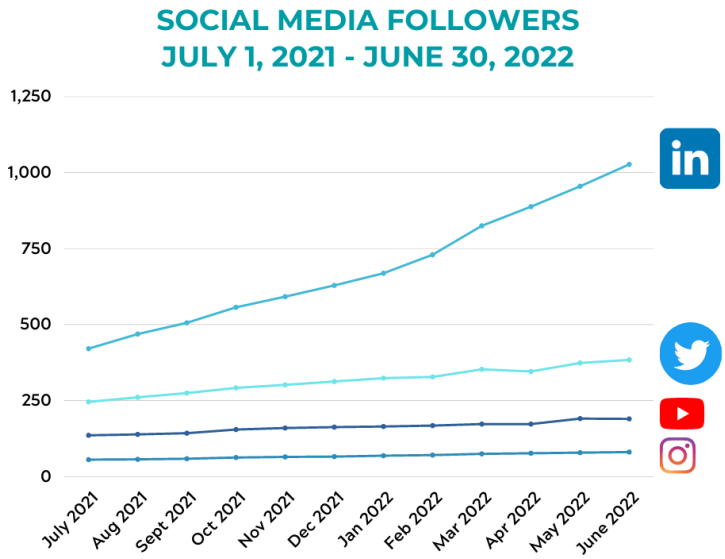


Figure 1.10: Social media followers for CCI's LinkedIn, Twitter, YouTube, and Instagram accounts, from July 2021 to June 2022.

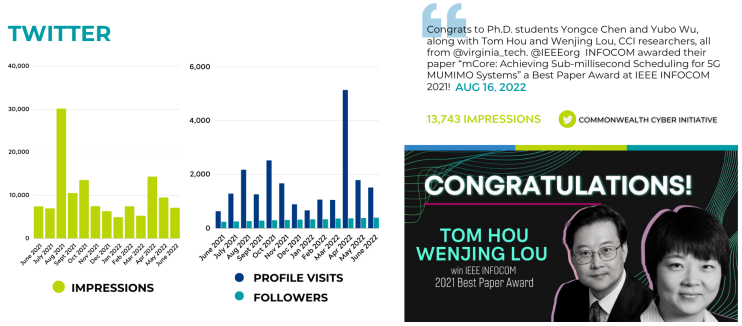


Figure 1.11: CCI Twitter impressions, profile visits, and followers from July 2021 to June 2022. The post with the highest number of impressions is also shown.

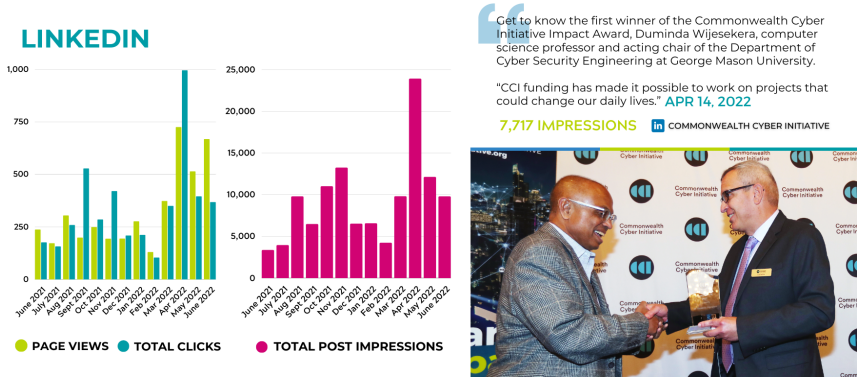


Figure 1.12: Evolution of LinkedIn page views, clicks, and impressions from July 2021 to June 2022. The post with the highest number of impressions is also shown.

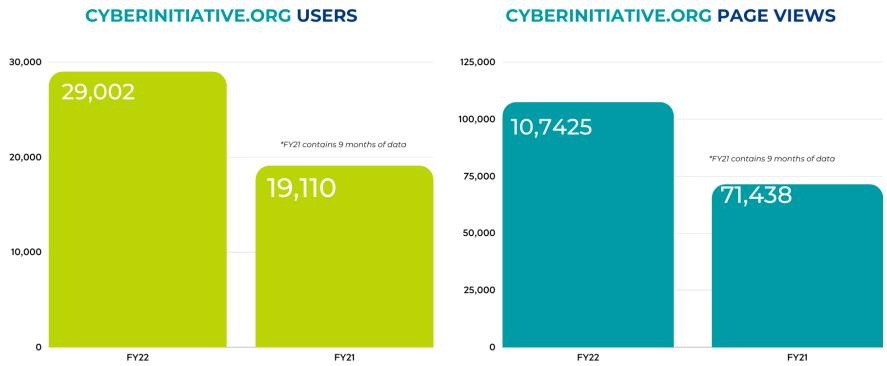


Figure 1.13: Evolution of website usage, focusing on users and page views from July 2021 to June 2022.

analytics in FY21). The number of FY22 page views increased 12.8 percent from the prior year to 107,425. CCI's research sections consistently are the main draw.

Inviting images such as graphics, photos, and videos, combined with succinct text and a user-friendly design, help website visitors quickly find what they need, ranging from events such as the annual CCI Symposium to calls for proposals and funded awards.

While CCI consists of a hub and four independent nodes, people see us as one cohesive organization. Telling a consistent story across the state is a major driver of our communication mission. The main website serves as the focal point to showcase calls for proposals, funded projects, news and other information from all nodes and the hub. The arrival of a new web and digital project specialist in June 2022 enables us to expand the website to show the depth and breadth of CCI's statewide activities and contributions.

This fiscal year, we developed a series of one-page overviews and a more in-depth CCI annual update brochure (Figure 1.14) to inform potential partners about the initiative through an accessible format. The monthly newsletter has grown to 2,500 subscribers from 300 in October 2020 and has strong open rates, another example of our engaged audience. It's an effective way to alert our network about upcoming projects, research calls for proposals, news, events, and standout work from our researchers and partners.

Our communications team has created a compelling narrative across multiple platforms to reach a diverse audience and connect all regions of the commonwealth. A refreshed logo and color palette brought needed vibrancy and flexibility to our communications outreach. We created a new branded presentation template to help our researchers present their CCI-funded work to everyone from small groups to large conferences.

We're looking forward to the 2023 fiscal year. We have great stories to tell!

1.5.2 Appearances in the Media in FY22

Many of the programs and major achievements from CCI researchers and staff have appeared in the print and online media. The following is a list of media hits from July 2021 to June 2022, in reverse chronological order.

- **Virginia Tech**, June 24, 2022: "Professor receives IARPA grant to improve secure communications".
- **Virginia Tech**, June 23, 2022: "Video: VTTI partners with Commonwealth Cyber Initiative to host technology showcase".
- **VMI**, June 13, 2022: "Teens Solve Fictional Murder Mystery at VMI".
- **Virginia Tech**, June 10, 2022: "Laura Freeman named deputy director of the Virginia Tech National Security Institute".
- **Onward New River Valley**, June 3, 2022: "VT Explores the Relationship Between Quantum Networks & Cybersecurity".

Figure 1.14: CCI's first brochure.

- **CCI**, June 3, 2022: "Radford/UVA-Wise team takes first in CCI Student Entrepreneurial Ideation Challenge".
- **Technology.org**, June 2, 2022: "Researchers explore how quantum networks could transform cybersecurity".
- **George Mason University**, June 1, 2022: "Mason students build drones as part of Commonwealth Cyber Initiative".
- **Virginia Tech**, June 1, 2022: "Commonwealth Cyber Initiative researchers at Virginia Tech explore how quantum networks could transform cybersecurity".
- **Virginia Commonwealth University**, May 13, 2022: "New testbeds at VCU College of Engineering boost the Commonwealth Cyber Initiative's capabilities in securing NextG, medical devices and smart cities".
- **Virginia Tech**, June 21, 2022: "Agricultural Cyber Field Day showcases collaboration and innovation".
- **Government Technology**, May 4, 2022: "Virginia Researchers Study Gaps in Cyber Crime Reporting".

- **WSLS News**, April 25, 2022: "High School students learning cyber security training through paid internship with VMI".
- **CCI**, April 12, 2022: "George Mason University Professor Duminda Wijesekera wins CCI Impact Award".
- **Virginia Tech**, April 8, 2022: "Shaping the future of Virginia Tech's 5G power grid".
- **Signal**, April 4, 2022: "Driving the Future of 5G Development and Innovation".
- **Virginia Tech**, March 28, 2022: "Cybersecurity showcase conveys impact and reach of student research".
- **CCI**, March 16, 2022: "CCI researchers do more than run experiments—they're DIY experts".
- **Virginia Tech**, March 14, 2022: "Quantum center unites Virginia Tech's broad expertise in a vital field".
- **Virginia Tech**, March 4, 2022: "Building safer communities: Virginia Tech criminologists awarded grant to study the impact of cybercrime on Virginians".
- **Virginia Tech**, February 21, 2022: "The Commonwealth Cyber Initiative gains speed with new partnership".
- **Virginia Tech**, February 8, 2022: "Virginia Tech places five faculty on Highly Cited Researchers 2021 list".
- **Virginia Tech**, February 1, 2022: "Are contact tracing apps tracking me? Not at all, say Virginia Tech researchers".
- **George Mason University**, January 26, 2021: "Commonwealth Cyber Initiative (CCI) researchers address multidisciplinary challenges".
- **Virginia Tech**, January 20, 2022: "Virginia Tech receives $2.8 million grant from the Department of Defense; Stephanie Travis named director of Senior Military College Cyber Institute".
- **WFRX Fox**, January 19, 2022: "Roanoke-Blacksburg Regional Airport preparing for potential 5G towers to come to the area".
- **CCI**, December 13, 2021: "CCI's CyberExL Program Is Giving Graduate Students Hands-On Experience".
- **Virginia Commonwealth University**, November 30, 2021: "Computer science professor named president-elect of IEEE society".
- **Old Dominion University**, November 21, 2021: "Wu Receives VASCAN Founders Award for Cybersecurity Contributions".
- **University of Virginia**, November 21, 2021: "UVA Joins Forces with the Virginia Department of Elections in Statewide Effort to Prepare Future Cybersecurity Leaders for Protecting Critical Infrastructure".
- **Virginia Tech**, November 18, 2021: "Research drives cybersecurity innovation, inspiration in Southwest Virginia".
- **CCI**, November 16, 2021: "Finland's Economic Affairs Minister Visits Virginia Tech to Discuss Future Collaborations with CCI".
- **Virginia Tech**, November 16, 2021: "Senior White House National Security Council officials to discuss need to defend critical U.S. infrastructure on Nov. 19".

- **Virginia Tech**, October 29, 2021: "Matt Hicks receives NSF CAREER award to develop tools for enhanced hardware security".
- **CCI**, October 18, 2021: "CCI Researchers Meet to Discuss How Cybersecurity Can Combat Misinformation and Disinformation".
- **George Mason University**, October 6, 2021: "At the Cross-Roads of Health Policy and Information Technology - Cybersecurity and Healthcare Data: What Executives and Policy Makers Need to Know Event Held in Arlington".
- **George Mason University**, October 4, 2021: "Cyber security engineering major competes at Deloitte CCI Cyber Camp".
- **Fox 5, Washington DC**, September 30, 2021: "Cybersecurity Awareness Month: Conti ransomware and other security warnings".
- **Virginia Economic Review**, Third Quarter 2021: "Sharing Resources to Improve Cyberspace: A Conversation with Luiz DaSilva".
- **Virginia Economic Review**, Third Quarter 2021: "A New Approach to Cyber Collaboration".
- **Virginia Economic Review Podcast**, September 22, 2021: " Sharing Resources to Improve Cyberspace: A Conversation with Luiz DaSilva".
- **CCI**, September 21, 2021: "Exploring the Artistic Side of Cybersecurity".
- **George Mason University**, September 15, 2021: "Mason partners with COMSovereign and Widelity to advance 5G innovation".
- **Government Technology**, September 14, 2021: "Editorial Board Endorses VA's Commonwealth Cyber Initiative".
- **The Virginian-Pilot**, September 8, 2021: "Editorial: Defending against cyberattack".
- **Old Dominion University**, August 27, 2021: "ODU Awarded NSF and NSA Cybersecurity Grants".
- **University of Virginia**, August 18, 2021: "Systems Engineering Undergraduate Wins Cybersecurity Competition".
- **CCI**, August 16, 2021: "Announcing Deloitte CCI Cyber Camp Winners".
- **Old Dominion University**, August 13, 2021: "Professors Study Cybersecurity's Role in Curbing the Spread of Misinformation".
- **Virginia Tech**, August 3, 2021: "Commonwealth Cyber Initiative funds seven projects to curb the spread of misinformation campaigns".
- **CCI**, July 12, 2021: "Meet CCI's First Batch of Summer Interns".

1.6 Report Structure

This report describes the CCI's progress and achievements in FY22. Chapter 1 outlines our vision and mission, describes the organization of the CCI Hub and Nodes, and summarizes our media strategy. Progress on the three mission lines of research, workforce development, and innovation is described in Chapters 2, 3, and 4, respectively. Chapter 5.1 is devoted to CCI's collaborative partnerships and projects. Chapter 6 contains the financial reports from the hub and nodes for FY22. Finally, Chapter 7 describes our main activities and programs planned for FY23.

The seven reporting requirements specified in Item 135, Chapter 1289, HB30, are:

- External grants attracted to support the work of CCI;

Reporting requirement	Section(s)
External grants attracted to support the work of CCI	2.1
Research grants awarded from the funds contained in HB30	2.2
Research faculty recruited	2.3
Results of entrepreneurship and workforce programming	3.1, 4.1
Collaborative partnerships and projects	5.1
Correlated economic outcomes	5.2
Geographic distribution of the awards from the funds contained in HB30	6.3

Table 1.1: Mapping of reporting requirements to sections of this report.

- Research grants awarded from the funds contained in HB30;
- Research faculty recruited;
- Results of entrepreneurship and workforce programming;
- Collaborative partnerships and projects;
- Correlated economic outcomes; and
- Geographic distribution of the awards from the funds contained in HB30.

The mapping of these reporting requirements to sections of this report is shown in Table 1.1.

Chapter 2

CCI Research

This chapter summarizes the main achievements in FY22 for the CCI research mission line.

2.1 External Grants to Support the Work of CCI

CCI's vision is one of Virginia as a global center of excellence in research at the intersection of cybersecurity, autonomous systems, and intelligence. The economic impact that CCI can bring is predicated on being recognized by industry, government agencies, and the broader research community as being leaders in this research domain. To achieve this mission, CCI is investing in unique research infrastructure and in research programs that build capacity and seed new areas of excellence. This has already resulted in unprecedented success in obtaining extramural funding to support CCI research. This section summarizes the outcomes of CCI's research mission.

2.1.1 Extramural Funding in FY22

In FY22, the CCI network received 77 external grants totaling $38,112,377 to support the CCI mission lines of research, workforce development and innovation. 48 grants (62%) were from federal and state agencies and 29 grants (38%) were from industry. Summary information is shown in Figure 2.1 and details are found in Appendix 1.

Node	Number of Grants	Grant Total
CCI Hub	3	$1,008,096
Central Virginia	15	$10,354,574
Coastal Virginia	17	$5,310,200
Northern Virginia	12	$7,839,343
Southwest Virginia	30	$13,600,164
Total	**77**	**$38,112,377**

Federal Grants	State/Industry Grants
48	**29**
$32,126,329	**$5,986,048**

Figure 2.1: External funding obtained by the CCI network in FY22.

2.1.2 Spotlight: Center for Wireless Innovation towards Secure, Pervasive, Efficient and Resilient Next Generation Networks (WISPER)

A CCI team lead by CCI Fellow and ODU professor Hongyi Wu successfully obtained NSF funding for the planning grant for a new Industry-University Cooperative Research Center (IUCRC) focusing on NextG technologies. The team includes Principal Investigator (PI) from four CCI universities: ODU, VCU, VT, and Mason.

This planning grant is of strategic importance for CCI and the commonwealth. If successful, this will be the first NSF-funded center bringing together industry and academic researchers on the topic of NextG networks. It will bring global visibility to CCI researchers and strengthen our network of industry partners. The successful planning grant proposal contained more than 50 letters of support from industry partners interested in participating in the center.

The proposed Center for Wireless Innovation towards Secure, Pervasive, Efficient and Resilient Next Generation Networks (WISPER) will coordinate academia, industry, and government to pioneer transformative next generation (NextG) wireless technologies for key industry verticals. Our missions include: (1) growing the U.S. innovation capacity in the next generation wireless networks; (2) catalyzing breakthrough precompetitive research for enabling NextG wireless communications; (3) contributing to the emerging North American vision for the next generation of wireless networks; (4) providing guidance to standardization bodies and cooperation partners; and (5) producing a workforce prepared to tackle complex next generation wireless challenges.

WISPER will focus on developing transformative wireless innovations. Areas of research include but are not limited to: (1) exploration of new spectrum bands for NextG wireless networks through a holistic lens by considering performance, efficiency, resilience, and security and privacy; (2) deep integration of artificial intelligence in wireless networks; (3) softwarization and virtualization of NextG network functionalities; (4) development of advanced solutions based on quantum and blockchain technologies to support NextG wireless communications; (5) demonstration of NextG wireless networks in diversified industrial applications; and (6) development of an industry-guided workforce development program in the context of next- generation wireless networks.

The proposed WISPER Center will contribute significantly to the country's future communication infrastructure, with broader impacts on diversity and inclusion, workforce development, and technology transfer. A Diversity & Inclusion Committee will be formed to review the current diversity and inclusion profile and develop specific measures and plans for inspiring the participation of underrepresented groups. WISPER will prepare students to become proficient in NextG techniques, leading to transformative changes in the state of wireless workforce preparedness. WISPER will enable seamless integration of the center's new discoveries into NextG wireless systems, accelerating technology transfer, enhancing the competence of the industrial members, and contributing to the Nation's leadership in NextG technologies.

2.2 Research Grants Awarded from the Funds in HB30

In FY22, CCI awarded grants to the participating institutions, aligned with our goals in research, workforce development, and innovation. These funds were awarded on a competitive basis, with researchers responding to calls for proposals issued by CCI. Proposals were reviewed by experts in the area of each call, and the LC made final funding decisions based on recommendations from reviewers. This section describes the grants awarded in this Fiscal Year from CCI funds.

2.2.1 Securing NextG

Objective of the Call

The overall goal of this program is to establish CCI as a leader in NextG security. While no formal definition of NextG currently exists, what we mean by the term is the generation of networks and technologies that is expected to eventually, in the next decade, complement and/or replace 5G. The NextG Alliance is a North American consortium formed to further develop the vision of NextG.

Objectives of this call include:

- To produce seminal contributions to secure NextG networks.
- To establish a CCI vision on NextG network security.
- To position CCI researchers to be competitive for government and industry funding of NextG research.
- To contribute to workforce development for NextG.

In addition to the usual research outputs, we anticipate this program to produce a CCI-led publication (e.g., an edited book) and a set of lecture notes. Each funded proposal will focus on a particular aspect of NextG security.

This call utilizes CCI Hub funds and is open to PIs in any of the public institutions that are part of CCI.

Selection Criteria

Each proposal was reviewed by at least three subject matter experts and evaluated according to the following criteria:

- Strong intellectual merit related to CCI's focus area (the intersection of cybersecurity, autonomy, and intelligence);
- Relevance to the focus of the call: cybersecurity and NextG;
- Significant initial results in the selected topic in NextG security;
- Strong broader impacts related to CCI's mission;
- Potential to generate additional funding and revenue; and
- Broadening participation by researchers in the CCI network in CCI-funded initiatives.

Research Grants Awarded

The number and value of grants associated with each CCI node are tabulated in Figure 2.2. Individual grants are listed in the Appendix 2.

Node	Number of Grants	Grant Total
Central Virginia	2	$200,000
Coastal Virginia	1	$100,000
Northern Virginia	3	$300,000
Southwest Virginia	2	$199,567
CCI Hub	1	$100,000
Total	**9**	**$899,567**

Figure 2.2: Securing NextG Research Program.

2.2.2 SWVA Research Engagement Program

Objective of the Call

CCI Southwest Virginia has a particular emphasis on cybersecurity related to fast, secure, and customizable communications systems and technologies, including 5G, Artificial Intelligence (AI), Machine Learning (ML), defense-in-depth cybersecurity solutions, emerging technologies (such as NextG and quantum algorithms) and cryptographic protocols, applications in transportation, energy, space, autonomous systems, manufacturing, and agriculture, as well as issues surrounding human factors, privacy, ethics, and global security in society.

This program utilizes SWVA Node funds and is open to PIs from public institutions of higher education from CCI Southwest Virginia (SWVA). This call was restricted to faculty members who have not previously served as PI on an award from CCI.

Selection Criteria

Proposals were reviewed by subject matter experts and evaluated according to the following criteria:

- Intellectual merit (40%): clearly defined problem/unmet need and how proposed work will address it.
- Broader impact (20%): potential to benefit society and contribute to the achievement of specific, desired societal outcomes, as it aligns with CCI's mission..
- Value of the funding (20%): concrete plans to use the results from this research to secure external funding or Intellectual Property (IP).
- Alignment and qualifications (20%): relevance to CCI mission and suitability of team background to proposed work.

Research Grants Awarded

The peer review process resulted in seven research grants awarded, as summarized in Figure 2.3.

University	Number of Grants	Grant Total
Virginia Tech	6	$72,276
Virginia Military Institute	1	$13,898
Total	**7**	**$86,174**

Figure 2.3: SWVA Research Engagement Program.

2.2.3 CCI Fellows Program 2022

This program, launched in FY22, has the objective of supporting large-scale proposals for extramural funding involving three or more CCI institutions. Increasing the competitiveness of our researchers to obtain funding for center-scale projects is one of our strategic goals.

Objective of the Call

This call will fund CCI researchers to lead center-scale proposals. PIs funded under this call will be designated CCI Fellows. Proposals must involve at least three CCI institutions of higher education (from any Node). A CCI institution of higher education must play a coordination role in the project. The budget associated with CCI institutions in the center-scale proposal must be at least $3 million.

Proposals must be in response to a published call or a direct solicitation from a funding agency or company.

This program is funded with CCI Hub funds, and receives proposals on a rolling basis. The program was announced in early 2022, with the first awards expected to happen in FY23.

Selection Criteria

Proposals will be evaluated by the CCI leadership according to the following criteria: strong intellectual merit relevant to CCI's mission and to the topic of this call, strong broader impacts related to CCI's mission, competitiveness of the team for center-scale funding, and potential to generate additional funding and revenue.

2.2.4 CCI Fellows

The original CCI Fellows Program completed its second and last year in FY22. Back in 2020, CCI selected nine fellows (see Figure 2.4) from universities in the CCI network to represent CCI and conduct cybersecurity related research, develop experiential learning projects and develop and/or participate in workforce development programs. The primary objective of the CCI Fellows Program is for the fellows to contribute to CCI's

research mission while fostering collaboration and engagement across the commonwealth's cybersecurity ecosystem.

Fellow	University
Dr. Duminda Wijeskera	George Mason University
Dr. Kai Zeng	George Mason University
Dr. Hong-yi Wu	Old Dominion University
Dr. Sachin Shetty	Old Dominion University
Dr. Yeng-Hung Hu	Norfolk State University
Dr. Milos Manic	Virginia Commonwealth University
Dr. Jack Davidson	University of Virginia
Dr. Jeff Pittges	Radford University
Dr. Kevin Heaslip	Virginia Tech

Figure 2.4: CCI Fellows FY22.

The CCI Fellows conducted research supporting each of CCI's three mission lines of research, workforce development and innovation/commercialization. The following are highlights of some of the research projects and their impacts.

Dr. Sachin Shetty, Old Dominion University. Dr. Shetty is conducting research on blockchain- and 5G-empowered asset management resulted in commercialization of a blockchain-based IoT solution and efforts are under way to set up a startup company. The ubiquitous adoption of networked devices and IoT across sectors, such as healthcare, manufacturing, automotive, etc., has led to operational, financial, and risk management impacts about security threats, lack of security measures in current IoT devices, and a lack of standards and regulations. Currently, enterprise operations across these sectors are plagued by service interruptions, lack of Quality of Service guarantees, and unreliable analytics supporting business processes. Although several solutions exist to protect networked devices, they do not provide resilient and trusted networked asset management solution. The goal of the fellowship project is to develop a 5G empowered platform to realize a trusted platform to leverage the low power and high latency capabilities required to track IoT devices in congested and contested communication environments.

Dr. Jeff Pittges, Radford University. Dr. Pittges is leading an experiential learning project. The goal of the project is to prepare students for industry employment through internships, co-ops, and other experiential learning opportunities. The project will develop infrastructure to recruit students into STEM fields, prepare them for experiential learning, support them during their learning experience, develop an employer network, and identify best practices for successful experiences.

Dr. Duminda Wijesekera, George Mason University. Dr. Wijesekera further developed the Living Innovation laboratory at Mason with complete experimental apparatus. This included obtaining and purchasing equipment and developing research leveraging these resources. These include a Linux CNC machine that carves 3D high carbon metal objects from AutoCad documents, a satellite-based RTX GPS correction services, and a Dual GPS server system for 3 cars already in use. Additionally, he has established 10 Dell servers and one GPS server for deep learning, visualization and to expand the driving simulation system to exceed 3 seats. Dr. Wijesekera was also able to secure a donation of a US-made stand-alone 5G system valued at $400,000.00 and anticipates further enhancing laboratory capabilities in FY23.

For NextG research, Dr. Wijesekera developed an architecture to provide connected and disconnected services (in a bubble) using post-quantum cryptography and implicit certificate services based on secure containers using hardware TPM modules while also developing multiple Kubernetes-based NextG systems to identify inter-system signaling vulnerabilities.

In terms of Cyber Physical Systems (CPSs), Dr. Wijesekera developed a Linux CNC vulnerability detection capability using reverse engineering, published vulnerabilities and code analysis. He also modeled the entire Linux CNC system formally using AADL and proved that the system carves AutoCad designs with some conditions even in the presence of faults and attacks and developed and implemented auto-generated

attack-fault-mitigation Trees for CPSs, extending his work of the past few years.

Looking at smart transportation, in particular intelligent intersections research, Dr. Wijesekera has invested in his students, training and empowering them to develop a NextG multi-access edge service that unifies fixed, actuated and synchronized traffic signals. Under his guidance, the CCI research team is currently moving from theory and simulation that enforces traditional signal constraints (such as all-red phases). Their product learns traffic patterns from BSM messages and transmits signal as MAP-SPaT (messages that embed signal phase and timing per lane into an accurate map of the intersection) messages using a controller that learns, updates traffic queues, enforces constraints and emits signals.

Additionally, Dr. Wijesekera has mentored his students in the area of NextG sensor fusion for connected automated vehicles, where they are using differential GPS-based multi-sensor systems to fuse information on two cars (with different viewpoints) using a geometric viewpoint transformation. They leverage LiDAR points clouds for primary fusion and wrap color and infrared camera images around them.

Finally, Dr. Wijesekera is providing additional undergraduate research opportunities on the Smart Building Initiative. His students have modeled Mason's Horizon Hall using AutoCad and are working on using infrared-based occupancy counters to determine the building usage scenarios. The objective is to use an in-building Multi-access Edge Computing (MEC) to control HVAC systems and physical access.

Dr. Hongyi Wu, Old Dominion University. Dr. Wu leads the research and innovation project titled A Development and Experimental Environment for Privacy-preserving and Secure (DEEPSECURE) machine learning research. While ML is embraced as an important tool for various science, engineering, medical, finance, and homeland security applications, it is becoming an increasingly attractive target for cybercriminals. DEEPSECURE is a first-of-its-kind development and experimental platform to support secure and privacy-preserving ML research. With its novel modular design integrated with fully customizable function blocks and sample modules, DEEPSECURE is a game-changing tool to effectively support research in this emerging field by enabling fast design, prototyping, evaluation, and re-innovation of trustworthy ML applications. It enables a variety of compelling new research projects that focus on ML security and privacy, leading to breakthroughs to protect ML systems and accelerating their development and widening their adoption. It will contribute significantly to the protection of the future cyber and physical world and safeguard human society. DEEPSECURE receives strong community support from over 20 key stakeholders across the country, including many CCI partners. It includes significant efforts for fostering and sustaining an ML security and privacy research community. The project includes specific measures and plans for inspiring the participation of underrepresented groups and infusing diversity and inclusion in all aspects of the project.

Dr. Frank Hu, Norfolk State University. Dr. Hu's research is developing deep learning and other machine learning techniques for classifying advanced malware. This project has: 1) provided a deep learning-based solution to advanced persistent threats detection and prevention; and 2) developed a rigorous malware-facing course curriculum coupled with experiential learning activities to prepare underrepresented minority students for the nation's cybersecurity workforce at a more competitive level.

Dr. Kevin Heaslip, Virginia Tech. Dr. Heaslip continued to advise Arlington County on privacy considerations for its Smart City Program and collaborated with other researchers linking artificial intelligence and CPS security.

Dr. Milos Manic, Virginia Commonwealth University. Dr. Manic continues to work closely with Battelle Energy Alliance to study cyber threat detection for wind and solar energy producers and a variety of other cybersecurity and AI research projects.

Dr. Jack Davidson, University of Virginia. Dr. Davidson is conducting research on FuzzROS: Structure-Aware Coverage-Guided Fuzzing for Robot Operating System (ROS) applications and a workforce development program sponsored by the Non-Standalone (NSA) and Department of Homeland Security (DHS) to identify students interested in cybersecurity to take additional cybersecurity courses and ultimately pursue a cybersecurity career. Additionally, the program is developing a "Host a UVA Cybersecurity Student at Work for a Day" program. The program will pay student travel expenses to spend a day with a cybersecurity professional at their place of work.

2.2.5 Other Grants Awarded by the Hub

CCI has affiliated faculty attached to academic departments at Virginia Tech and conducting CCI-funded research in the CCI Hub. These faculty members are listed in Figure 2.5.

Faculty	Department	Grant Amount
Dr. Wenjing Lou	Computer Science	$25,000
Dr. Haining Wang	Electrical and Computer Engineering	$173,000
Dr. Laura Freeman	Statistics	$70,894

Figure 2.5: CCI Hub Faculty FY22.

Dr. Wenjing Lou. With CCI's support, Wenjing Lou led a team of one postdoc and eight graduate students in the past year, working on several important cybersecurity research topics.

Blockchain security: Blockchain as a distributed networked system is multi-layered, which has complex security implications that are not yet fully understood or addressed. Existing analyses on blockchain consensus security overlooked an important cross-layer factor – the heterogeneity of the Peer to Peer (P2P) network's connectivity. Dr. Lou's team has been modeling and analyzing various factors, including consensus protocols used, underlying peer-to-peer network connectivity, malicious mining strategies (such as selfish mining), and quantifying their impacts on the fundamental security of the blockchain systems. The team received an NSF SaTC medium project for this line of research. The project title is "A Networking Perspective of Blockchain Security: Modeling, Analysis, and Defense". A Ph.D. student working on Blockchain topics graduated this year and landed a tenure track faculty position due to his excellent work in this area.

Blockchain-enabled novel applications: Another line of research we have been actively pursuing is novel security applications enabled by blockchain. In the past year, we have focused on developing a centralized spectrum access system that leverages blockchain and smart contract technologies to address the potential security and performance issues facing dynamic spectrum sharing in the 5G or Next G wireless networks. The current Spectrum Access System (SAS) designated by the Federal Communications Commission (FCC) follows a centralized server-client service model, with each SAS administrator operating their own servers without an efficient, trustworthy, and automated inter-SAS synchronization mechanism. In response, we have proposed a blockchain-based decentralized SAS architecture dubbed BD-SAS to provide SAS service efficiently to spectrum users and enable automated inter-SAS synchronization without assuming trust in individual SAS service providers.

Machine learning-based intrusion detection systems: Machine Learning (ML) technologies have been used extensively to build various applications. Our work focuses on ML-based Intrusion Detection Systems (IDSs) in mission-critical but hostile IoT environments. We previously developed security solutions to defend against some most effective security attacks on ML systems, including a model poisoning attack that attacks an ML system at training time and an adversarial example attack that attacks an ML system at the testing time. In the past year, our focus has been on exploiting contrastive learning to boost IDS performance in IoT networks. We proposed FeCo, a federated-contrastive-learning framework that coordinates in-network IoT devices to jointly learn intrusion detection models. FeCo features a novel representation learning method based on contrastive learning that is able to learn a more accurate model for the benign class, which significantly improves the intrusion detection accuracy compared to previous works.

Dr. Haining Wang. In FY22, Dr. Wang's team conducted four different research projects under the support of Defense Advanced Research Projects Agency (DARPA), NSF, and Office of Naval Research (ONR). More specifically, (1) we investigated various security issues in cloud environments, including VM live migration, adversarial container workloads, and data center thermal vulnerabilities; (2) we studied scalable key management for distributed IoT devices in 5G environments; (3) we explored new side-channels for defense and offense; and (4) we studied different security issues in naming space, including reliable Domain Name System (DNS) deployment and typosquatting attacks in container registry. We have published five journal papers and nine conference papers in top security venues, such as IEEE TDSC, IEEE S&P, ACM CCS, USENIX Security, ACM SIGMETRICS, and IEEE/IFIP DSN.

Dr. Laura Freeman. Dr. Freeman provides technical leadership and guidance on data science and artificial intelligence in support of the xG Testbed. In particular she focuses on how we can bring the computing a storage capabilities designed for robust, resilient, and assured AI into wireless applications. Efforts in the past year have included transitioning the existing AI Testbed into open source infrastructure that is compatible with the 5G architecture and developing use cases for how AI and 5G technologies integrate

into AI-enabled networked communications.

2.3 Faculty Recruited

2.3.1 Hub Faculty

The CCI Hub hired two new research faculty members and three post-doctoral researchers in FY22. They are:

Dr. Yi Shi is a CCI Research Associate Professor at Virginia Tech. His research focuses on machine learning, algorithm design, and optimization for next generation wireless networks and security. Prior to joining VT, he was a Senior Lead Scientist at Intelligent Automation, a BlueHalo Company. He received his Ph.D. in 2007 from the Department of Electrical and Computer Engineering at VT. He has published over 160 papers on wireless communications, wireless networking, security, machine learning, and optimization. His work won the IEEE HST 2018 Best Paper Award, the ACM WUWNet 2014 Best Student Paper Award, the IEEE INFOCOM 2011 Best Paper Award Runner-Up, and the IEEE INFOCOM 2008 Best Paper Award. Dr. Shi served as a Technical Program Committee (TPC) chair for ACM Workshop on Wireless Security and Machine Learning (WiseML) 2019–2022, the Emerging Technologies track for IEEE MASS 2021, the Machine Learning for Wireless Communications, Networking, and Security Symposium for IEEE GlobalSIP 2019, IEEE Workshop on Cognitive Radio and Electromagnetic Spectrum Security (CRESS) 2014 and 2016, an Editor for IEEE Communications Surveys and Tutorials, and a TPC member for many IEEE and ACM conferences. For his professional activities, he was recognized as a Distinguished TPC Member for IEEE INFOCOM in 2021 and an Exemplary Editor for IEEE Communications Surveys and Tutorials in 2014. He is a Senior Member of IEEE.

Dr. Jacek Kibilda is the 5G and AI Research Assistant Professor with the Commonwealth Cyber Initiative and a Research Assistant Professor with the Bradley Department of Electrical and Computer Engineering at Virginia Tech. He holds a Ph.D. from Trinity College Dublin, Ireland, and is the recipient of the TechImpact Fulbright Fellowship. Dr. Kibilda has vast experience managing national and European research consortia in his previous roles as Research Fellow at Trinity College Dublin and Senior Research Scientist at the Wroclaw Research Center EIT+. As the recipient of a Science Foundation Ireland Challenge Research Fellowship, he was involved in developing and managing Science Foundation Ireland challenge-funding programs. He has authored two book chapters and over 30 peer-reviewed publications on modeling and technology design for mobile networks. He is currently focusing on research into modeling and technology design for next-generation mobile networks. Dr. Kibilda received the 2018 CONNECT's Education and Public Engagement award for his work on a research immersion program for high-school students and broader impact activities. He wrote opinion pieces on the developments in 5G for the Irish Times and performed what is probably the world's first stand-up on modern telecommunications. He is a Senior Member of the IEEE and a Contributing Member of the Next G Alliance.

Dr. Jaganmohan Chandrasekaran is a CCI postdoctoral associate at Virginia Tech. After obtaining his undergraduate degree (B.Tech) in Information Technology from Anna University, India, he worked as an analyst programmer for a US-based insurance company from 2009 to 2012. In 2013, he joined The University of Texas at Arlington for graduate studies in Computer Science. At the University of Texas at Arlington, he first earned his Master's degree in 2015 and later a Ph.D. in 2021. He is a recipient of a STEM fellowship from 2015 to 2021 and a Dissertation Fellowship recipient in 2021. Dr. Chandrasekaran's research is at the intersection of software engineering and AI, focusing on addressing the software engineering challenges in the AI system development lifecycle. His current research aims to develop AI assurance approaches for a reliable and trustworthy AI system. His work has been published at peer-reviewed international conferences.

Dr. Ajay Kulkarni is a CCI postdoctoral associate at Virginia Tech. After obtaining his undergraduate degree (B.E.) in Computer Engineering and a graduate degree in Modeling and Simulation (M.Tech.) from the University of Pune, India, he moved to the United States for further education. In 2016, Dr. Kulkarni joined George Mason University's Computational and Data Sciences department for his graduate studies. In 2018, he earned his second Master's degree (M.S.) in Computational Science and, later, in 2022, a Ph.D. in Computational Sciences and Informatics. During his graduate studies, he received the Recognition of Teaching Excellence award six times (2018-2021) from the College of Science and a Dissertation Completion

Grant in 2022. Dr. Kulkarni's research focuses on AI that aims to develop explainable, trustworthy, and reliable AI applications. His work has been published in peer-reviewed journals and international conferences.

Dr. Mayukh Roy Chowdhury received his Ph.D. in Electrical Engineering from the Indian Institute of Technology (IIT) Delhi, New Delhi, India in 2022. His thesis is titled Resource Efficient Strategies for Massive Machine Type Communication (mMTC) in 5G. He worked in the multi-institute indigenous 5G testbed project funded by the Department of Telecommunications, Government of India. Prior to that he received the M.Tech degree in Communication Systems Engineering from Indian Institute of Technology (IIT) Patna, India, in 2016 and the B. Tech. degree in Electronics and Communication Engineering from West Bengal University of Technology, Kolkata, India, in 2012. He has worked in the 6G Lab, Samsung Research and Development Institute, Bangalore (SRI-B), India and TCS Innovation Labs, Bangalore, India as a research intern. He has been working as a CCI postdoctoral research associate at Virginia Tech since April 2022. His research interests include AI driven radio resource management for cellular networks, applied machine learning in 5G and next generation wireless networks, reinforcement learning, AI on edge for smart IoT systems, MEC for 5G, random access for massive machine type communication in 5G, and resource efficiency in communication networks.

2.3.2 Node Faculty

2.3.3 Northern Virginia Node

The Northern Virginia Node did not recruit new faculty members in FY22 but plans to hire additional faculty in FY23.

2.3.4 Coastal Virginia Node

Dr. Kazi Aminul Islam is a research assistant professor/research scientist at the school of cybersecurity at ODU. He recently completed his Ph.D. degree in the Electrical and Computer Engineering department at ODU. Previously, he received his Bachelor of Science degree in Electrical and Electronic Engineering from Khulna University of Engineering and Technology, Bangladesh, and an MS degree in Electrical Engineering from Lamar University, USA.

Dr. Tran Phoung is currently a Research Assistant Professor at the School of Cybersecurity, ODU. Before that, she was a Research Fellow at IC2, School of Computing and Information Technology, University of Wollongong, and a Contributed Fellow at CSIRO – Data61. From Spring 2017 to Summer 2018, Dr. Phoung was a postdoctoral researcher at ODU. She has published in the top tier of cryptography/security conferences and journals, including ACM CCS, ESORICS, IEEE INFOCOM, ACM ASIACCS, IEEE TIFS, and IEEE TII.

Dr. Masud Rana joined as a research faculty member in the CoVA Node in FY22.

Dr. Lori Pitman holds a PhD in International Studies from ODU, a Master's in Humanities from the same institution, and a Master of Laws degree from Sofia University, Bulgaria. As a subject matter expert, Dr. Pitman worked on different projects on disinformation, sponsored by NATO and by the U.S. Department of State. She was also a guest-speaker at various international events organized by the Tactics Institute for Security & Counter Terrorism (UK), the Legal Innovation Lab Wales (UK), NATO-ACT and NATO Innovation Hub.

Dr. Pitman has published multiple peer-reviewed articles and book chapters with a focus on international security and cybersecurity. Her publications appear in International Journal of Cyber Criminology, International Journal of Intelligence & Cybercrime, International Journal of Criminal Justice Sciences, Journal of Criminal Justice Studies, Politikon: The IAPSS Journal of Political Science, and the Encyclopedia of Global Security Studies. She is also a co-editor of the NATO-issued volume Advances in Defence Analysis, Concept Development and Experimentation: Innovation for the Future.

Dr. Safdar Bouk received the B.S. degree in computer systems from the Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2001, and the M.S. and Ph.D. degrees in engineering from the Department of Information and Computer Science, Keio University, Yokohama, Japan, in 2007 and 2010, respectively. He was a recipient of the Japanese Government (Monbukagakusho) scholarship. Dr. Bouk served as lecturer with the Department of Computer Engineering, QUEST, Pakistan, from 2002 to

2005, and Assistant Professor with the Department of Electrical Engineering at CIIT, Islamabad from 2010 to 2016. He was a postdoctoral fellow at Kyungpook National University, Daegu, Korea. In Daegu, South Korea, he also served as Research Professor with the department of Information and Communication Engineering, DGIST from 2017 to 2021. His research interests include reliable and low latency wireless networks, future internet architectures, and resilient CPSs.

2.3.5 Southwest Virginia Node

Dr. Atul Mantri joined as an Assistant Professor, Department of Computer Science, VT. Dr. Mantri was recruited from the University of Maryland's Joint Center for Quantum Information and Computer Science (QuICS), where he was a postdoctoral associate. After completing his Ph.D. at Singapore University of Technology and Design (SUTD) and Center for Quantum Technologies, Dr. Mantri spent time as a Research Associate at the University of Edinburgh. His research focus is secure delegated quantum computing with interests in the roles of interaction, randomness, security, and quantum correlations in various quantum cryptographic tasks pertaining to the client-server setting. His broader work is in quantum computation and quantum information.

Dr. Jason LeGrow joined as an Assistant Professor, Department of Mathematics, VT. Dr. LeGrow was recruited from the University of Auckland and received his Ph.D. from the University of Waterloo. His research interests include post-quantum cryptography; cryptanalysis and optimization of Commutative Supersingular Isogeny Diffie-Hellman (CSIDH), an isogeny-based key establishment protocol; isogeny-based protocols for blockchain applications; and modern topics in cryptographic secret sharing.

2.3.6 Central Virginia Node

The Central Virginia Node did not recruit new faculty members in FY22.

2.4 Research Infrastructure

CCI has made a major investment in creating a geographically distributed testbed for research and innovation in 5G and Next Generation networks. We call it the *CCI xG testbed*. This platform is allowing CCI researchers, in partnership with government and industry, to experiment, validate, and test new technologies and approaches to accelerate fundamental research and innovation on cybersecurity in the context of the next generation of mobile and fixed networks.

Value Proposition

The xG Testbed contains assets for research and innovation in 5G and NextG, embedding Artificial Intelligence (AI) in the operation of the network, supporting research in network security, O-RAN security, and AI assurance, among other topics. Figure 2.6 shows the logo developed for the testbed.

Figure 2.6: CCI xG Testbed logo.

The value proposition for the xG Testbed can be summarized as follows:

- First end-to-end ORAN-compliant 5G/6G network with fully integrated AI infrastructure. Fully built with open source AI and network components.
- Includes massive computing and storage capabilities focusing on AI Assurance for cybersecurity.
- This multi-site testbed allows experimentation with non-locality in complex networks.
- Able to deploy at scale AI solutions in distributed networks.
- Supports hands-on multi-disciplinary training of cyber professionals well versed in AI and communications.

Design Principles

Our goal is to support innovation that is aligned with the standardization of 5G being led by the 3rd Generation Partnership Project (3GPP) as well as to contribute to the emerging vision for the next generation of networks, which we refer to as *Next G*. To this end, we adopt the following principles in the design of our testbed:

- Openness: reliance on open systems, whenever possible, for access to communications and network functions and programmability;
- Accessibility: access to the testbed by researchers throughout the CCI network of institutions;
- Programmability: configurable and programmable hardware and source, end-to-end, from the user equipment to the core network;
- Flexibility: flexible network management and orchestration compliant with an end-to-end 5G architecture composed of a mix and match of open-source and commercial hardware and software, with a cybersecurity focus, enabling indoor and outdoor deployment;
- Componentization: fully componentized implementation with open Application Programming Interfaces (APIs); containerized, cloud-ready implementations;
- Interoperability: integration ensuring the integrity of the end-to-end solution; interoperability among network components and existing testbeds, securing and hardening the network infrastructure;
- Support of verticals: alignment with key verticals to be supported by 5G and Next G networks, and co-location with research infrastructure supporting those verticals.

The testbed has components located in the CCI Hub and each of the nodes. These components are aligned with verticals that are of particular focus in each node: national security, autonomous vehicles, transportation networks, manufacturing and supply chain in the NoVA Node; IoT, smart communities, and medical devices in CVN; ports and warehouses in the CoVA Node; autonomous and unmanned vehicles, additive manufacturing, and the energy grid in the SWVA Node. The testbed component in the CCI Hub provides a full-stack 5G core and radio access network, including commercial-grade and experimental Software Defined Radio (SDR) equipment and open source software; it is accessible remotely by all CCI researchers.

Chapter 3

CCI Workforce Development

This chapter summarizes the main achievements in FY22 for the CCI workforce development mission line.

3.1 Results of Entrepreneurship and Workforce Programming

CCI has invested in the creation of new experiential learning opportunities to Virginia students, and in pairing students with cyber startups, medium and large businesses, and government agencies for training and career development opportunities. This section highlights the CCI programs that focus on workforce development.

3.2 Experiential Learning Program in FY22

In its third iteration, the 2022 Experiential Learning call for proposals elicited 21 submissions, with nine successful proposals totalling $899,153 awarded in grants. CCI researchers were eligible to respond to this call, and proposals were selected based on recommendations by a peer review group. The percentage of the funding for projects in each CCI Node is shown in Figure 3.1.

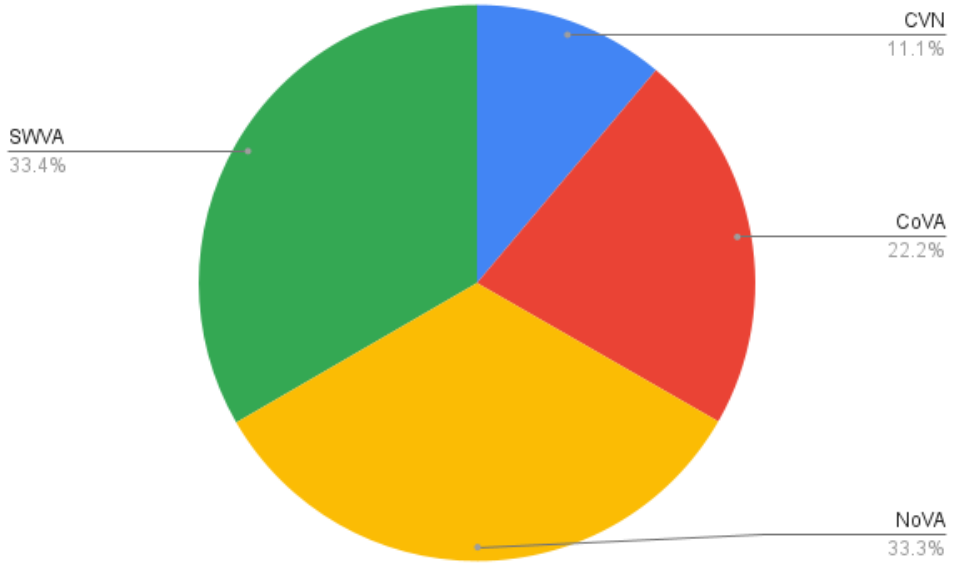


Figure 3.1: Funding percentage by Node for the FY22 Experiential Learning program.

The projects funded by this program are summarized below.

- **Digital Forensics Experiential Learning Program with Virginia State Police**: Irfan Ahmed; VCU; $100,000. This program will create CCI4n6, an industry-focused experiential learning program in digital forensics in direct partnership with the Computer Evidence Recovery Section (CERS) at Virginia State Police (VSP). PI Ahmed has worked closely with digital evidence examiner Bruce Patterson and first sergeant Robert Keeton at the CERS in Richmond, VA, to design an experiential learning CCI4n6 program, which is practical for VSP to implement and beneficial for the students for workforce development.

- **Cyber Startups: CCI 2022 Scalable Pilot Programs for Experiential Learning**: Gisele Stoltz; Mason; $99,799. Recognizing that startups and small businesses are an important and growing part of the Virginia cybersecurity ecosystem, this project aims to achieve the following two objectives: to provide students in cybersecurity degree programs who are from diverse backgrounds with relevant, hands-on experiential learning opportunities; and to provide cybersecurity startups and Small and Medium Enterprises (SMEs) with the talent they need to scale their businesses. This project seeks to diversify the talent pipeline to cybersecurity jobs and build a resilient and diverse cybersecurity innovation ecosystem that will help Northern Virginia thrive post-pandemic.

- **Disinformation as Data Poisoning**: Dan Runfola; William & Mary (W&M); $99,374. The William and Mary geoLab has hosted two annual fellowship projects with CCI to date, engaging 99 students in projects exploring the intersection of deep learning, data poisoning and satellite imagery. These projects have been largely implemented in collaboration with the defense and intelligence industry partners, and have led directly to internship and job opportunities. Working with these – and new – partners, we are now launching a third round of this project focusing on disinformation as data poisoning. In this project, 25 additional students will work closely with defense and intelligence partners to test and prototype techniques to identify and automatically mitigate data poisoning in social media streams. This work will build on the fundamental hypothesis that techniques which are effective in detecting data poisoning in imagery models (i.e., corrupting pixels in an image to distort deep learning models outputs) could also be substantially helpful in detecting data poisoning in models integrating social media (i.e., disinformation which is 'poisoning' the corpus of tweets collected). Our projects to date have been both cost-effective and scalable, and have enabled us to build substantial local infrastructure to support increasingly lower-cost student engagement with project partners and advisors.

- **Solving the Cyber Workforce and Skills Challenges through Experiential Learning**: Brian Ngac; Mason; $100,000. Through 1) recruiting students interested in the cyber security field and industry participants with motivation in mentorship; 2) working with industry participants to design challenging and engaging cyber projects; 3) guiding the students through project execution in an agile environment; and 4) having the students present their work and lessons learned to the CCI community and beyond, this experiential learning effort can prepare students to be more marketable and effective in the workforce because of the integration of industry participation. Having run experiential learning courses since Spring 2021, our team's methodology has evolved to provide students an effective and enjoyable experience to be remembered and leveraged for early career years. The experience also benefits our industry participants by leveraging our talent pool for recruitment opportunities and by providing a cost-effective method to attempting new / risky projects.

- **Preparing Virginia's Workforce to Secure the Nation's Election Infrastructure**: Massimiliano Albanese; Mason; $99,985. George Mason University recently joined a coalition of seven Virginia universities and colleges partnering with the Virginia Department of Elections to create and manage the Virginia Cyber Navigator Internship Program, with the goal of educating students on how to protect our critical election infrastructure through a combination of in-class learning and experiential learning opportunities. Students who intend to participate in the program are required to take a gateway course on election security. Selected students are offered a 10-week paid internship with the Virginia Department of Elections and will work in teams under the supervision of a faculty mentor. The program has been extremely successful for Mason and has exceed all expectations both in terms of students enrolled in the course and in terms of qualified internship applicants. This CCI-funded project expands the

election security program at Mason by increasing the number of supported interns, expanding the pool of faculty involved as mentors, and creating an annual Election Security Workshop.

- **Expanded Scalable Pilot Program for Experiential Learning in CCI Through the Commonwealth STEM Industry Internship Program**: Mary Sandy; ODU; $100,000. The Virginia Space Grant Consortium (VSGC), a CoVA CCI team member, is using its highly successful Commonwealth STEM Industry Internship Program (CSIIP.org) as a venue for facilitating state-wide experiential learning opportunities for Virginia STEM students pursuing CCI-defined majors in support of CCI's aim to create a commonwealth-wide ecosystem of excellence in Cyber Physical System (CPS) at the intersection of cybersecurity, autonomous systems and data. This partnership is serving as an innovative program allowing for expansion to serve the entire commonwealth and support CCI's goal of closing the workforce gap in cybersecurity in the commonwealth.

- **Use and Abuse of Personal Information**: Alan Michaels; VT; $99,995. The Use and Abuse of Personal Information experiential learning effort engages a diverse multi-disciplinary group of undergraduate students to explore and quantify how personal information propagates across the Internet. The CCI effort builds upon two years of experimentation that demonstrated the ability to generate realistic fake identities, perform one-time online interactions, and subsequently collect and analyze how that information is being both used and abused across email, SMS text, and voicemail modalities. Of particular interest are cross-site sharing behaviors (attributable due to one-time interaction), adherence to published privacy policies, trends across industries, root sources of spam and malicious content, and answering a variety of social science questions. The initial experiment engaged 15 students from 10 different majors at VT. The upcoming experiment incorporates published lessons learned from in three conference papers and an invited Blackhat USA presentation to perform a scaled experiment with on the order of 100,000 fake identities that also integrates automated open source intelligence (OSINT) collection and analysis tools. Further, the CCI investment is aimed at evolving towards an independently sustainable vertically integrated project that can broaden engagement to include faculty and students at other universities, with end goal being a real-time dashboard/open dataset that reflects information use and sharing behaviors.

- **Enhancing Experiential Learning via Technology Enabled Internships with Mentoring (TEIM): Phase 2 Implementation**; Jeff Pittges; Radford; $100,000. This critical gap is being addressed in southwest Virginia via the CCI-aligned Technology Enabled Internships with Mentoring (TEIM) program. TEIM clearly defines a student-driven learning approach that allows professionals to engage in a structured, high-impact manner. The novel, technology supported program emphasizes real-world knowledge attainment, mentoring from cybersecurity professionals, and entrepreneurial ideation via response to a collaborative professional challenge. To scale the value of TEIM, the project team proposes a statewide launch. CCI supported objectives include: 1) complementing high-quality traditional education, 2) enhancing workforce-ready skills via immersive industry experiences and 3) leveraging existing CCI investments to enhance/scale talent development. With dedicated mentoring support from cybersecurity and technology membership organizations and successful past performance in multiple CCI nodes, the project team is well positioned to deliver a successful statewide launch of the TEIM program.

- **Future Cyber Security Educators: Empowering Cadets as Educators**; Mohamed Azeb; VMI; $100,000. Motivated by the successful high-school and home school internship program, a Department of Defense (DoD) workforce development grant at VMI, VMI Cyber Captain program (CCP), and VT educational programs such as the Future Faculty Diversity Program, we see value in training the cyber security leaders and educators of tomorrow. In this project, we build on the aforementioned successes and propose a comprehensive top down cascaded training program, Future Cyber Security Educators (FCSE), with in-depth involvement and stakeholders from academia, government, national defense and private industry.

3.3 Workforce Programs Developed by the CCI Nodes

In addition to the CCI-wide programs described above, in the past year the CCI Nodes also developed and executed many successful workforce programs.

3.3.1 NoVA Node

The NoVA Node carried out six workforce initiatives:

- **High School Cybersecurity Internship Program**: The CCI NoVA Node funded 30 high school students for internships with cybersecurity companies during Summer 2022. The experience includes a 2-week professional skills training program to prepare students for the professional work environment. 181 applications were received for the 30 available placements. Of the selected applicants, 37% identify as women, and 20% are or will be the first in their family to attend college. Underrepresented population groups in science and engineering comprise 40% of this year's cohort. Host companies include: Chainbridge Solutions, Leidos, ManTech, NT Concepts, Obscurity Labs, Oceus Networks, Singlepoint, Widelity, and the United States Government. This program is an expansion of the successful program launched in FY21.

- **University/College Cybersecurity Entrepreneurship Internship Program**: To support both workforce development and early-stage cybersecurity startups that have limited resources, Mason conducted an expansion of its successful Cybersecurity Internship program, partnering with entrepreneurs and their early-stage companies to provide invaluable experiential learning opportunities to students. CCI NoVA Node ran two cohorts of cybersecurity internships with early-stage companies in fall 2021 and spring 2022. In fall 2021, the program received 164 applications for 22 positions; in spring 2022, 114 applications were received for 18 internships with 13 companies. Fifty percent (50%) of the interns were female and 79% identified as minorities. Host companies included: Colvin Run Networks, DataLock Consulting Group, KaDSci, LLC, ITinfra, NN Data, Total Cyber Solutions, Next5, Solvitur Systems, Assursec, LLC, Degree Six, Auspex Labs, Inc., CyRisk, Altamira Technologies, Harmony Tech, Monoc Securities, Gigasheet, Inc, InterSec, Inc, NowSecure. This effort not only expands cybersecurity experiential learning, but augments the workforce to accelerate commercialization of cybersecurity technologies and the creation of new jobs in the sector.

- **Undergraduate Research Program** CCI NoVA Node sponsored 25 undergraduate students conducting cybersecurity research at George Mason University, James Madison University and University of Mary Washington. Example research projects included:

  • Protecting Critical Infrastructure • SCIBORG: Secure Configurations for the IoT Based on Optimization and Reasoning on Graphs • Malware Localization and Confinement in Large Scale IoT Networks • Post-Security Breach Press Release and its Effect on the Company's Stock Price • Securing Emerging Networks of Diverse Devices with Intelligent and Resource-Efficient Mechanisms • Smart Building Control using NextG Mobile Edge Servers (MEC) • SAWBRID: SmArt WhiteBoard Replacement Interactive Device • Security, Privacy, and Trust Enrollment (SPaTE) for mobile Health (mHealth) • Fast, Automatic, and Accurate Code-based Attack Attribution through Deep Learning • An Empirically Surfaced Taxonomy of the Chief Information Security Officer • Impact of Human Behavior on Hybrid Driving Environment

  These experiences are building significant technical expertise and capacity in undergraduates, making them particularly well trained for advanced work in industry and government. Forty-four percent (44%) of this year's Undergraduate Research Assistants cohort identify as women, and 52% identify with underrepresented population groups in science and engineering.

- **Teacher Cybersecurity Professional Development Program**. 23 public school teachers from across the region, including Arlington, Alexandria, Fairfax, Prince William, Stafford counties, participated in a 5-month cohort entailing virtual cybersecurity workshops and other training opportunities over the course of the academic year. The overall goal was to help teachers build confidence in their

knowledge of cybersecurity and support introduction of cybersecurity concepts into the classroom, regardless of grade level or subject matter. Topics addressed in the professional development workshops included:

• Intro to Cybersecurity • Linux 101/ Intro to a Cyber Range • Linux 102 and Fun with Linux • Passwords/ Cracking Passwords • Malicious Links and Untrusted Sources • File Hashing • Backdoor Attacks • Simple Web Application Attacks • Advanced Web Application Attacks

Sessions were facilitated by CCI Nova Node partner Cyber.org. The program culminated in presentations by teachers of lesson plans they have developed for their specific classrooms and disciplines with impact to more than 2700 K-12 students. Participating teachers were also offered an opportunity to participate in the Education Discovery Forum on June 20-22. CCI NoVa Node underwrote the registration fees for participation in this conference.

- **Cybersecurity Apprenticeship Program**. As part of CCI NoVa Node's effort to expand the pipeline of cybersecurity talent beyond degree-seeking individuals, the CCI NoVa Node Cybersecurity Apprenticeship program is providing cybersecurity training and an immersive apprenticeship for people who wish to transition into a career in cybersecurity but do not have prior experience. This program includes a 7-week classroom learning and training experience, beginning July 5, 2022, followed by a 12-week apprenticeship/traineeship with a cybersecurity company. The program received over 400 applications for 21 available positions. 43% of the cohort identify as female, and veterans represent 19%. Underrepresented population groups in science and engineering comprise over 90% of this cohort. Placement in apprenticeships is ongoing and includes to date, apprenticeships with Arlington County, DEKRA, Sedulous, and Peraton.

- **Undergraduate Internship Program** This program enables undergraduates from across the CCI NoVa Node to participate in internships with cybersecurity companies from across the region. There are currently 16 students participating in this program. Industry hosts include NT Concepts, Inc., Cask Government Services, Edgemoor Research Institute, InterSec, Inc., Telos Corporation, Fend, Inc., IvySys Technologies, and KeyCaliber, Inc. Thirty-one percent (31%) of this cohort identify as female.

- **Clearance Readiness Program**: All CCI NoVa Node students who participate in CCI experiential learning programs, regardless of their home institution are asked to participate in the Mason Clearance Readiness program which includes attendance at a series of workshops to help prepare students to obtain a clearance. In addition to an Introduction to Clearances, students participate in additional workshops on strategies to effectively complete the required SF-86, what is evaluated in a background investigation, best practices for success in the clearance process, and participate in employer panel discussions about careers that require a clearance.

3.3.2 COVA CCI

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.

- **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 started 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, W&M, and Crowdsourced Review Manipulation Attacks Online platforms, led by Dr. Faryaneh Poursardar, ODU.

- **AccessCyber.** COVA CCI provided $30,000 in funding to W&M 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 product that can be shared across all CCI regions.

- **COVA CCI Cybersecurity Internship Program**: CoVA CCI COVA CCI is partnering with VSGC to manage the COVA CCI Cybersecurity Internship Program using their Commonwealth STEM Industry Internship 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-eight (28) students from 6 universities/colleges have been placed with twelve (12) companies.

3.3.3 SWVA Node

The SWVA Node funded 16 workforce programs:

- **Artificial Intelligence and Visual Analytics in Cybersecurity Experiential Learning for Workforce Readiness**: ProCyEd (Professional requirements to Cybersecurity Education) aims to address the "readiness gap" between the cybersecurity knowledge, skills and activities used in real-life professional careers, and experiential learning offered in cybersecurity curricula. Data-driven assessment is needed to determine the efficacy of educational modules for workforce readiness and advancement. Combining AI (for example, gaming, machine learning, and computational intelligence) and visual analytics (for example, interactive visualizations and using AI to inform and guide the visual analytics discovery process), ProCyEd can provide a comprehensive platform that helps guide users acquiring the right experiential training and education that qualifies them for a specific career path in cybersecurity. ProCyEd framework and attached tools enable adaptive experiential learning experience that better prepares students for the cybersecurity work field.

- **Cyber security aware IoT Networks: An Internship Program for high school students**: Inspired by the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, and in order to graduate the next cyber leaders with the knowledge, skills, and abilities to effectively perform, both individually and as team members, we believe that cyber education must start early. For that, we built an internship program as a pilot project to connect college students with high schoolers in a hands-on based training program. The tasks required for cybersecurity work, and the readiness to serve cyber missions, depend mainly on the student's ability to understand cyber operations, the value of cyber security aware design and development. These are key for many roles such as Data Scientists, Reverse Engineers, Malware and Exploitation Analysts, Vulnerability Researchers, and Information Operations Integrators into Cyber Operations. In addition to cultivating extensive technical competencies, effective cyber leadership requires the development of knowledge, skills, and abilities that are not typically addressed in regular educational programs. With the help of this grant and in cooperation with the DoD sponsored cyber defense lab, we used trained cadets (captains) as trainers and coworkers to transfer the knowledge and train the participating high school candidates.

- **Research Experiences for Community College and K-12 teachers**: Radford University, in collaboration with Virginia Western Community College, is working with teachers in K-12 and Community Colleges across Virginia to develop research experiences in the areas of security analysis, cryptography and IoT security. K-12 and community college educators will use the experience gained through research participation to develop classroom-appropriate experiential learning exercises in cybersecurity and related topics. K-12 and community college educators will work in the Artis Cybersecurity Research and Education Lab - a facility that includes IoT labs and Security analysis lab - and participate in exploring privacy of IoT devices used in smart home and environments relevant to SWVA region such as manufacturing, agriculture and networking research. Current research in 5G at Radford will

also be part of these experiences. To prepare the educators for research, camps will be conducted in security topics supported by other grants (e.g., NSA Capacity Building grant (2021-22)).

- **CCI SWVA Cyber Internships - GCAPS**: The goal of this project is to provide local cybersecurity students with hands-on experience using cybersecurity concepts as well as providing them with relevant work experience to help them find future opportunities in the cybersecurity workspace. Two projects were created for the students to work on that would be relevant to their cybersecurity backgrounds and help them expand their knowledge in their field. The students were to be split into two groups with each of the groups being assigned one of the projects to take on and complete. One of the groups of students would be working on a project to support Virginia Tech Transportation Institute (VTTI) in their organization of a tech showcase event that would be used to demonstrate different CCI funded projects and technologies that were being developed and encourage researchers from the various CCI nodes to collaborate. Specifically, they would be working on developing a Hack-a-thon capture the flag style competition utilizing the technology that VTTI would be demonstrating in the tech showcase event to create challenges for participants to solve. This project also identifies a framework that can be used to organize future capture the flag competitions. The other group of students would be working on a project to identify and research security vulnerabilities and attacks and some security products and solutions for Vehicle-to-everything (V2X) networks. This project's goal was to determine what security concerns currently exist in the growing V2X space and what the current state-of-the-art is for mitigating those concerns. This project gathers technical information about V2X security that can be used in future projects involving V2X technology.

- **Experiential learning Mini-grants in cyberbiosecurity and data analytics in agricultural and food systems for increasing SmartFarm technology development, applications, and data security**: Data analytics and security are essential topics for students in agriculture and the life sciences; these students must be prepared to analyze and protect life science data in associated industries. While a few undergraduate courses introduce related concepts, greater effort is needed to reach the broader agricultural and life science student population. This initiative provides mini-grants to support experiential learning for developing cyberbiosecurity and data analytics case studies, course modules, or experiential learning opportunities for agricultural and food systems-focused community college, undergraduate, and graduate courses. A request for proposals was distributed in Fall 2021 for experiential learning materials developed by graduate students with mentoring from VT Center for Advanced Innovation in Agriculture (CAIA) affiliate faculty and faculty at other CCI-affiliated institutions. Four proposals were received and three proposals were funded (two from CCI funding; one from CAIA funding). A second RFA was distributed in January 2022 for faculty to address course module development. Seven proposals were received and six proposals were funded. Three projects were directly funded through CCI Southwest and three were funded through CAIA resources. Projects ranged from data analytics for animal agriculture, soil chemistry, and food processing to cyberbiosecurity for agriculture and food science students. Projects involved faculty and students from Virginia Tech, Radford University, Lord Fairfax/Laurel Ridge and Virginia Western community colleges. Learning materials from each project are being developed and will be shared through open educational resource options.

- **Security Clearance Ready Certificate (SCRC) Program**: Security Clearance Ready Certificate (SCRC) is a program that informs undergraduate and graduate students about and prepares them for the security clearance process. The SCRC program is available to all students at CCI SWVA institutions. Students are required to attend four seminars during the academic year to earn the SCRC. There will be many opportunities to participate in seminars via virtual platforms (such as zoom) or in person. This program is designed to demystify the clearance process and streamline pathways between higher education programs and jobs requiring security clearance.

- **Technology Enabled Internships and Mentoring (TEIM)**: The Technology Enabled Internships and Mentoring (TEIM) program was developed to develop the workforce-ready skills of a select group of SW VA students with a desire to pursue a cybersecurity career. The program combines high-quality education with critical thinking/soft skills and applied knowledge; by delivering an immersive industry work experiences with mentoring relationships. The technology-driven work/experiential self-directed

learning curriculum will increase the student's knowledge of key cybersecurity concepts supported interactions with industry professionals during the weekly mentoring sessions. Students will access the learning content via the secure online application, Your Career Counselor (YCC), which has been developed by CivilianCyber to help students advance their knowledge of key cybersecurity concepts (see item 11). Over the course of the eight-week program the students will complete a cybersecurity learning module (comprised of both written, video, and interactive lessons), including: 1) Cybersecurity Awareness and Planning, 2) Data Governance, 3) Resilience, Back Up and Recovery, 4) Network and Data Access, 5) Student Driven Topic, 6) Program Conclusion. Once a module has been completed the student will meet with their mentor to review that week's topic. The mentee will present their learnings and solicit feedback from their mentor. The student will update their learning profile in the YCC platform with the results and complete a short test to ensure that they have correctly understood that module. Each module must be completed before the student can proceed to the next module. The result is a real-world, student owned professional engagement that also provides mentoring and an expansion of their relationship network.

- **CCI SWVA Cyber Internships - VT**: The project consists of hiring Virginia Tech students to work in the central Information Technology (IT) area. The interns will focus on cyber security tasks in the cyber defense, security architecture and risk management areas.

- **Cybersecurity Vertically Integrated Projects (VIPs)**: The "Use & Abuse of Personal Information" project is aimed primarily at the multi-disciplinary evaluation of propagation of personal information across the Internet. The project's general approach is to create false identities, use these identities to sign up for websites, and then evaluate emails, SMS messages, and phone calls received as a result of the signups. Last year's pilot project involved 15 students from 10 different majors, with their results leading to a presentation at Blackhat USA 2021 and 3 follow-on publications (1 at the ACM-sponsored Data Privacy Management workshop of the ESORICS conference and 2 at the IEEE-sponsored Intelligence and Security Informatics conference), all accepted/presented Fall 2021. This AY's project team, involving 13 students from 7 majors, was broken into three sub-teams: one focused on the voicemail/SMS collection engine, a second focused on the email server, and the last focused on building the target organization list and specific research questions. The first sub-team completed a trade study Fall 2021 before selecting and ordering an open source (FreePBX) phone server, which is now mostly configured. The second sub-team has finished configuring the email server and is adding additional functionality aimed at simulating repeated interactions to improve the believability of the false identities. The third sub-team located a database of over three million internet organizations and is curating the database to address specific research questions currently under development. In parallel with these CCI teams, (1) Raytheon IIS has funded three additional sub-teams focused on data analytics and post-processing of the content, helping build a larger ecosystem of PII research and (2) OUSD has funded an ECE senior design team focused on developing an account signup acceleration engine. Work continues over the 2022 summer semester to establish a new database to catalogue the signups, develop methods for user authentication and logging, and merge sub-team code repositories.

- **Wise Minds at Work** : Wise Minds at Work (WMAW) is an intensive in-the-field learning experience that brings together students in cross-disciplinary teams to address cybersecurity challenges of for-profit businesses and other organizations. Technology majors will anchor these teams. Teams may also include students majoring in criminal justice, psychology, sociology, etc., based upon the needs of the specific industry partner and as dictated by the needs of the project. OBJECTIVES: This program would offer a 360-degree benefit, which would include the possibility of full-time employment for Virginia's college graduates, an opportunity for employers to sample the talent of rural Southwest Virginia, and a stronger relationship between UVA Wise and employers. Additionally, this project would position Southwest Virginia as a permanent technology recruitment pipeline for employers throughout the Commonwealth. RESULTS: Six interns were recruited to work with three technology companies, one in Southwest Virginia and two in Northern Virginia. Although the companies were impressed with the work of the interns, full-time employment was not offered due to the business impact of COVID-19 and market uncertainties. Two of the companies transitioned two interns from Wise Minds to our technology internship program, Wise Works. A fourth company was lined up to participate in the program

but decided late in the process that it didn't have the capacity to mentor and supervise interns during the pandemic.

- **Competition Training to Increase Pathways to Cybersecurity Workforce**: The project has three main objectives including: 1) Training for competitions led by industry experts, 2) Exercise development by faculty and student to provide competition training and 3) Training with other college teams. The first objective was addressed in the fall of 2021. Two industry experts, Keith McMannon (red Canary) and Dr. Arnab Ray (Abbott Labs), provided training on red -teaming and medical device security respectively. In the Spring of 2022, training was done by Liam Epperly on pen-testing. For the Fall 2022 the team is currently working on training sessions in network security, linux, securing IoT devices and red-teaming. Dr. Art Carter and Dr. Jeff Pittges are in discussions with with Sedulous on providing internships and other experiential learning related to cybersecurity (ttps://sedulous.com) Dr. Uppuluri and Dr. Pittges met with SkyePoint Decisions to provide guest lectures and possibly a workshop and other engagements. Skyepoint may also train students on mock interviews (https://skyepoint.com/about-skyepoint/leadership-team). The second objective will be accomplished through an RFP issued for proposals to develop exercises. The RFP has been released and proposals will be accepted through Summer 2022. Selected exercises will be hosted either on the Virginia Cyber Range or Radford University Range. Dr. David Raymond at Virginia Cyber Range has agreed to post exercises on the Range as feasible. Training between teams from Virginia Western Community College, Germanna Community College, Lord Fairfax Community College and Radford University will be conducted in Fall 2022 and Spring 2023 to address the third objective of training with other college teams.

- **Cyber Range Accessibility Program**: When we started this project, the Virginia and U.S. Cyber Range Exercise Area, CTF platform, Courseware Repository, and Knowledge Base did not meet modern web accessibility standards. W3C web accessibility standards are provided in the Web Content Accessibility Guidelines (WCAG) 2.1 (https://www.w3.org/TR/WCAG21/). The DOJ has cited WCAG 2.1 as an acceptable metric for web content accessibility under the ADA. In order to make our resources broadly accessible to underserved individuals, as well as to reduce exposure to legal complaints under the ADA, the cyber range proposed to contract with a third party expert to conduct a full assessment of our resources using a Voluntary Product Accessibility Template (VPAT) and to work with our team to remediate accessibility shortfalls. This will also greatly improve our ability to commercialize the cyber range as many potential U.S. Cyber Range customers insist on a VPAT addressing WCAG 2.1 guidelines and will not use our resources without this. The cyber range contracted with Level Access, a well-known accessibility support company, who did a thorough analysis of our software and services to identify shortfalls. The cyber range development team spent 8 weeks working with Level Access to correct deficiencies, and had an initial VPAT issued on July 7th, 2021. The team will continue to work with Level Access in the coming years to refine and maintain our significantly enhanced level of web accessibility. This project also included funding in support of expanded courseware in the cyber range catalog and student wage salary in support of capture-the-flag challenges for Virginia and U.S. Cyber Range competitions. In the fall of 2022, Level Access will evaluate and test the redesign of the U.S. Cyber Range website to optimize compliance with WCAG 2.1 guidelines.

- **Cybersecurity Careers Video Series**: To fill current open cybersecurity positions and to meet the expected growth in cybersecurity positions, the Virginia Cyber Range plans to develop a cybersecurity careers video series highlighting diversity in cybersecurity to increase interest in cybersecurity as a career. The Cyber Range will interview current cybersecurity students in high schools in Virginia who are interested in pursuing a career in cybersecurity as well as former students pursuing postsecondary education in pursuit of a cybersecurity career. Our goal is to develop a series of 1-minute videos to promote careers in cybersecurity careers including among underrepresented groups. In addition to these students, we will seek to interview individuals currently in the cybersecurity workforce demonstrating diversity in race, gender, disability, age, veterans' status, etc. We will align their work roles with the NICE Cybersecurity Workforce Framework work roles. The videos will also highlight non-technical cybersecurity roles in marketing, business, and leadership. The Virginia Cyber Range will contract with a professional video production company to ensure a professional video is produced.

- **Summer Faculty Boot Camp for Developing Virginia Tech Partnerships in Quantum Information Science and Engineering (QISE) with Historically Black Colleges and Universities (HBCUs)**: Quantum Information Science and Engineering (QISE) is a rapidly growing research and educational agenda at Virginia Tech (VT). The Colleges of Science and Engineering, the Innovation Campus, as well as the Commonwealth Cyber Initiative (CCI) are experiencing growth in QISE. The federal government (e.g. NSF, DoD, DoE) and industry (e.g. IBM) expect Historically Black Colleges and Universities (HBCUs) to play an important role in developing the future QISE workforce. However, at most HBCUs, QISE expertise, research, education, and infrastructure is at a nascent state. This project seeks to develop sustainable and equitable partnerships in QISE with HBCUs that are mutually beneficial to VT and HBCU partner institutions. The project will ultimately lead to expanded opportunities for research funding, curriculum development, diversifying the VT graduate student body and ultimately diversifying the QISE workforce.

- **Project Charter Quantum Science and Engineering**: Quantum Information Science and Engineering (QISE) is expected to revolutionize society in the coming decades. Virginia Tech has recently recognized QISE as an OVPRI Frontier Research area and set up an ICTAS-level research center. There must be a well-trained QISE workforce in the Commonwealth. This project is a collaboration between Virginia Tech Engineering Online and the Department of Electrical Engineering to meet four related objectives: 1) To develop an online virtual lab (piloted in-person spring 2022; initial online course development complete June 1 2022), 2) To develop modular open educational resources in quantum science and engineering with a focus on security applications. (modules to be determined by partners in August 2022), 3)To develop a strategic partnership with HBCUs, which the federal government, corporate and philanthropic groups acknowledge is critical for the diverse future QISE workforce, beginning with a collaboration with Prairie View A & M and including Virginia State and additional HBCUs in the Commonwealth, utilizing the platform of the Inclusive Engineering Consortium IEC (iec.org). (partnership with VSU, PVAMU initiated with Feb. 2022 visit and series of development meetings; 4 students recruited for summer 2022), 4) To support proposals for additional external funding, e.g. NSF RISE proposal to be submitted by PVAM and VT to develop infrastructure at PVAM to support he course at other HBCUs longer term. (NSF QISE Workforce grant track 2 submitted with partners, June 2022).

- **HackHouse: Open access IoT Lab in a box**: "Radford University is collaborating with Virginia Tech to develop an Internet of Things Lab (IoT lab) that can be used to develop hands on lab exercises to teach security and privacy issues on IoT devices. Why is this useful? As IoT devices become ubiquitous, cybersecurity is no longer confined to traditional computing devices such as laptops and desktops. So, most cybersecurity graduates (Associates, Bachelors and Masters) will work in securing IoT devices. This project will help develop a basic lab that promotes a few security experiments. Specifically, the project aims to: (a) Develop and setup the hardware lab such that network traffic monitoring and capturing tools can be deployed at different points on the IoT network (b) Develop tools to co-relate captured traffic Results so far: A basic IoT lab has been setup at Radford. The lab supports monitoring of traffic between IoT devices, between the IoT devices and the WiFi router and the traffic from the WiFi router to the Internet. We have deployed and configured a tool called MITMproxy to monitor encrypted web based traffic. Currently we are working on setting up MITMproxy in a transparent mode – so that the IoT devices need not be made aware of the monitoring tools. A work in progress poster on this lab was presented at the Colloquium on Information Systems Security Education 2021.

3.3.4 Central Virginia Node

Virginia launched the Commonwealth Cyber Initiative (https://cyberinitiative.org/) (CCI) with the mission to serve as an engine for research, workforce development, and innovation at the intersection between cybersecurity, autonomous systems, and intelligence. The CCI network consists of a Hub, led by Virginia Tech and located in Northern Virginia, and regional nodes across the state. UVA is partnered with Virginia Commonwealth University (VCU) to form the Central Virginia Node (CVN).

As part of the CCI network, and as specified by a Memorandum of Understanding (MOU) with VCU, UVA Engineering has received $125,000 to support workforce development/innovation projects. A faculty steering committee has been convened to guide CCI-related investments, include use of these funds. The committee consists of: Jon Goodall (Chair), Jack Davidson, Barry Johnson, Cong Shen, Jack Stankovic, and Yixin Sun. The committee reviewed proposals for workforce development/innovation projects, and recommended funding for two projects, described below. All projects have a period of performance of 7/1/2022-6/30/2023. The recommendations were approved by UVA Engineering's Associate Dean for Research, Fred Epstein.

- Jack Davidson (CS), in partnership with Julia Lapan and her team in the Center for Engineering Career Development: "Host a UVA Cybersecurity Student at Work for a Day", $40,000. This project will support student travel to spend a day with a cybersecurity professional at their place of work. The program will primarily target companies (and agencies) within the Northeast Region (Maryland, Virginia, and North Carolina). However, we would also consider placing students at locations outside the region if the company is a member of our cybersecurity advisory board. We currently have 19 companies supporting our various cybersecurity programs, including the Virginia Cyber Navigator Internship program funded by the NSA. A small committee of cybersecurity faculty and Center for Engineering Career Development staff will select and match the students to participating companies. We would strive to recruit and select a diverse group of students. On returning from the day with their host, students would submit a trip report about their experience. The "host a student day" provides UVA undergraduate students a unique, early experiential learning activity in cybersecurity. Additionally, the program will help our students build their professional network, which is critical for successful job searches and career goals.

- Dan Quinn (MAE—ECE) and Homa Alemzadeh (ECE): "Link Lab Professional Development", $25,000. This project will create a Link Lab centered program that focuses on skills in communication, leadership, ethics, and entrepreneurship to support research and workforce development in the areas of cybersecurity, autonomous systems, data intelligence, and cyber-physical systems. The new program will include an expanded set of Professional Development Seminars, a Student Retreat, and an Industry Networking Event. We will also use financial incentives to catalyze student-led interdisciplinary research collaborations. In addition to all Link Lab students, the program offerings will be open to students of UVA faculty working on CCI-related topics and projects. The schedule of professional development seminars will also be shared with UVA faculty involved with cybersecurity research and education in UVA Engineering to encourage their students to attend. And finally, invitations for select activities will be extended to all CCI-funded projects for students to participate virtually or in-person as possible.

3.4 CCI Internship Fair

On October 5, 2021 CCI provided a series of panels featuring government, industry, and academic leaders highlighting their open opportunities, sharing how to apply, internship expectations, and answering questions live. Panelists included representatives from the U.S. Dept. of Homeland Security, Cybersecurity and Enterprise Architecture Division (CEAD); U.S. Dept. of Healthy and Human Services; Appteon; Palo Alto Networks; Microsoft; Civilian Cyber; and Deloitte.

On October 6, students had the opportunity to visit organizations' and institutions' virtual booths. Students created a profile, uploaded their resumes, and connected with recruiters and program leaders through 1:1 live messages and videos from the convenience of their own homes. Employers were be able to meet with students from across the commonwealth and a variety of cyber and cyber adjacent fields all in two days without the added expense and logistics of travelling.

Following the success of the 2021 internship fair, CCI will again host a virtual internship fair on September 22 and 23, 2022. With students returning to school at the end of August, registration for the 2022 internship fair will open in August 2022.

3.5 CyberFusion

The Commonwealth Cyber Fusion, hosted by VMI, Senator Mark R. Warner, the Virginia Cyber Range, and CCI took place on the VMI campus on February 25-26, 2022. CyberFusion combines a collegiate cyber competition with learning and career opportunities featuring a career fair, career panel, and the Virginia Cup Capture the Flag Competition. The event hosted two competitions, one for 4-year and one for 2-year colleges. 106 students competed over the weekend, in 19 teams, 6 community college teams and with 29 students observing. The team from Laurel Ridge Community College (formerly Lord Fairfax Community College) and the team from George Mason University won their respective divisions. The competition was completely free for student teams and their coaches due to corporate sponsorship and CCI. This enabled all interested teams to compete, regardless of fundraising ability.

3.6 CCI Cyber Camp

The 2022 CCI Cyber Camp was held at the Virginia Tech Research Center - Arlington (VTRC-A) from June 6-9. This year's program featured unique aspects to CCI and provided students with an opportunity that they could only achieve through CCI. Students worked directly on the CCI XG Lab, and the AI lab. The agenda included workshops in both labs, a data anlaytics workshop, mock interviews with recruiters from CACI International, a career panel, and a resume and cover letter writing workshop. This was a two-phased event, starting with an online, capture-the-flag competition with the top 20 students attending the in-person portion. Students came from the following universities, colleges, and community colleges:

- Christopher Newport University
- College of William and Mary
- George Mason University
- Laurel Ridge Community College (formerly Lord Fairfax Community College)
- Old Dominion University
- Radford University
- University of Mary Washington
- Virginia Tech

Chapter 4

CCI Innovation

This chapter summarizes the main achievements in FY22 for the CCI innovation mission line, in particular results of innovation and commercialization programming.

4.1 Hub-led Programs

4.1.1 The CCI Innovation Bootcamp

In January 2022 CCI hosted the inaugural Innovation Bootcamp at the Virginia Tech Research Center in Arlington, VA. Facilitated by BMNT Inc., students were exposed to innovative business practices, used in Hacking4X courses across the country, to converge on real-world problems sourced from government and industry challenge sponsors. Challenge sponsors included CACI International, the Cybersecurity and Infrastructure Agency CISA, and the Virginia Office of Public Safety and Homeland Security.

Students met with challenge sponsors to learn about pain points and issues, and then over the course of three days, evolved one prioritized problem, learned foundational innovation methodologies needed to progress to prototype phase, and then developed a prototype and pitched the new capability to their stakeholders.

The application process required students to submit a 60second video pitch describing why they wanted to participate in the bootcamp. Of over 50 students that applied, 30 students were invited to attend. Students came from the College of William and Mary, George Mason University, Laurel Ridge Community College (formerly Lord Fairfax Community College), Old Dominion University, Virginia Commonwealth University, Virginia Military Institute, and Virginia Tech.

This was a very popular event and CCI has begun planning for next year's bootcamp.

4.1.2 Virginia Cybersecurity Challenge

5G connectivity ushered in a new era of possibilities for cybersecurity. Recognizing this, the Commonwealth Cyber Initiative (CCI) and US Ignite partnered to host the Virginia Cybersecurity Challenge, a four-phase competition with the goal of sparking the development of cybersecurity prototypes that leverage unique elements of emerging 5G technologies to provide secure operations or communications in ways not possible with previous generation networks. Ultimately, it is expected that the competition will lead to the creation of new cyber jobs within the Commonwealth. After completing the first two phases of the competition, we are excited to share more about the four finalist teams plus the prizes each earned as a result of their concepts and prototypes!

- **Reducing the risk of Intentional Electromagnetic Interference using Multifunctional Phase Change Composites**; VCU; Awarded $60,000. To address the danger of electromagnetic sabotage, which involves the deliberate use of electronic equipment performance, this team is developing a multifunctional coating that can concurrently provide high-frequency electromagnetic radiation shielding and passive thermal management for microwave devices. The coating is generated through a composite

system that consists of a phase-change matrix improved through the inclusion of magnetic filler particles with high microwave absorption efficiency. The innovative solution conforms to the size, weight, power, and cost demands of 5G devices.

- **Data-driven Cyber-Attack Control in Communication between Autonomous Vehicles and infrastructure for 5G-assisted Transportation Cyber-Physical Systems**; UVA; Awarded $60,000. This team developed and implemented software prototypes to detect false information in the vehicle-to-infrastructure communication in Transportation Cyber-Physical Systems (TCPS). In this phase, the team investigated the efficacy and accuracy of real-time false information detection in the V2I communication by leveraging smartphones to simulate vehicles and AWS as the 5G infrastructure. The team will also develop software for the V2I false information detection in the 5G-assisted TCPS.

- **NetSense: A Web-based Software-as-a-Service Modeling Environment to Study and Analyze Wireless 5G Networks as Complex Systems**; VMI; Awarded $25,000. In this project, the team presented a web-based modeling and analytical environment for running network dynamics and predicting the spread of malicious behaviors and computer viruses on 5G networks. The project uses a novice approach to view the 5G network as a complex system of interacting components. By recasting real 5G networks in an abstract simulated graph, the team can run intensive data analytics and simulations, and propose intervention strategies to avoid cascading failures. A useful forthcoming feature entails a dashboard to query and visualize networks, subnetworks, and their properties to address this issue.

- **Proactive Trustworthy - Self Sovereign Identity Management (PT-SSIM) solution for 5G IoT-based D2D authentication**; VMI, ODU; Awarded $15,000. Recognizing the need to enable privacy-friendly, computationally efficient, and reliable device-to-device (D2D) authentication, this team's project introduces a zero-knowledge proof mechanism with intrinsic resilient storage and management that enables automated trustworthy authentications. This 'Proactive Trustworthy Self-Sovereign Identity Management' (PT-SSIM) system manages a blockchain-based smart contract platform to facilitate an operation that can support a large number of concurrent identity verification transactions. PT-SSIM is built to enable user-controlled identity verification with no credential disclosure.

In the first week of October, these teams will demonstrate an operational product based on their prototype and a functional application to a panel of judges for evaluation, and submit a proposal for commercialization.

The final phase of the Virginia Cybersecurity Competition focuses on taking the solutions created by the teams to market and generating cyber jobs within the Commonwealth. Commercialization activities will be set by US Ignite, CCI, and other partners. Such activities include facilitating networking sessions with high-tech partners, enrollment in relevant accelerators and incubators, and guided business plan development.

The above blog post can be found at https://www.us-ignite.org/get-to-know-the-four-virginia-cybersecurity-challenge-finalists/

4.2 Node-led Programs

In addition to the CCI network-wide programs the Hub administered, the CCI Nodes also funded several innovation programs.

4.2.1 Northern Virginia Node

- **Innovation Commercialization Assistance Program.** ICAP serves early-stage companies, and follow-on impact or capital is often earned or awarded months to years following program completion – ranging from 12, 24, or even 36 months later. All ICAP companies are connected to an ICAP Mentor as soon as they apply to the program. This allows companies the potential to have multiple meetings prior to the beginning the Introductory Course. As a result, each company becomes better prepared to maximize the benefits of the course. During the course, companies develop (or refine) their business thesis, define an initial customer segment and value proposition, review the buying ecosystem, and

conduct 20 or more customer discovery interviews. Each team that completes the introductory course receives a follow-up action item list/roadmap to discuss next steps and plans for future advising. Each team continues to work with their ICAP Mentor for as long as needed for their specific venture.The CCI NoVa Node ICAP initiative continues to mentor companies that began the program in FY21 as well as new companies who have joined one of three virtual ICAP Introductory Course cohorts that have been launched since July 2021. In FY22, seven (7) new cybersecurity companies completed the ICAP course, with additional entities identified and scheduled to join the July 2022 cohort. Additionally, ICAP is partnering with Women's Society of Cyberjutsu (WSU) to host a sub-cohort focused solely on female-led cyber venture. The cyber entrepreneurial ecosystem is nascent and developing and, as such, direct outreach to individual partners has proven to be the most effective way to recruit teams for ICAP cohorts. A limited number of organizations are working together to support cyber-related entrepreneurship, which has become a key focus area for ICAP. As such, the ICAP team has identified strategic opportunities to interface with companies who might benefit from ICAP and pursued them as such. A number of initiatives for FY23 – including personnel support for the CCI+A cyber accelerator and its own invite-only mini-summit – are currently being planned. The CCI NoVa Node Investment has enabled ICAP to obtain significant additional funding to expand the number of companies it can support, and its impact across the Commonwealth. These grants include $200,000 from CIT, $525,000 from VA Bio Connect, and $882,000 from GO Virginia.

- **Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology (CATAPULT)**. In 2022, the CCI launched a Cyber Acceleration, Translation, and Advanced Prototyping for University Linked Technology (CATAPULT) Fund to advance collaborative translational research projects amongst CCI partners, with the goal of speeding the transition of academic research outcomes to the marketplace. The CATAPULT Fund is supporting 8 awards of $50,000 each. An investment of $200,000 by the CCI NoVa Node was matched with funding by the CCI Hub. The CATAPULT Fund is an important tool in the CCI's Innovation toolbox, providing funding critical to advance the maturity of cyber discoveries during the critical "Valley of Death" phase of commercialization, as defined by the National Science Foundation. During this phase, innovators are preparing for SBIR or CRCF grants to assist in product development and market testing, but are not quite prepared for outside investment. The CATAPULT Fund is helping innovation teams pay for critical resources, personnel, time to test products, and get market initial market feedback integral to obtaining Seed or Angel funding.

- **CCI+A**. The CATAPULT grants will also trigger recipients' participation in the Commonwealth Cyber Incubator + Accelerator (CCI+A) – launched in early 2022 in the new Digital Innovation Pilot facility on George Mason University's Mason Square campus. CCI+A offers: (1) a bootcamp-style program to rapidly move new technologies forward; (2) support for customer discovery efforts; (3) opportunities for cyber startups to engage with potential industry and government partners, as well as broader DMV- and Commonwealth-based customers; (4) opportunities for customer engagement; (5) opportunities to bring university innovation to industry and government for feedback and collaboration; (6) industry and government collaboration opportunities for cyber faculty on technical work and product testing; (7) opportunities for training students for work in cyber startups; (8) engagement with meaningful student projects; (9) cyber-focused hack-a-thons; (10) cybersecurity-focused workshops, meetings, and collider events with government agencies and industry; and (11) opportunities to engage with seed and venture capital, including the opportunity for exposure to investors and for potential prize money at Mason's annual Accelerate innovation competition. The call for proposals for the CATAPULT fund was released on Feb 14, 2022, with proposals due April 29, 2022. Eight new companies and faculty partners were notified of their successful selection for CATAPULT funding in June 2022. Four of the of the newly developed companies were founded by faculty from Mason, two by faculty from ODU, 1 by a faculty member from William and Mary 1 by a faculty member from James Madison.

4.2.2 Coastal Virginia Node

INNOVATE Cyber.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. They all completed their work in April 2022.

4.2.3 Southwest Virginia Node

- **SWVA Region Innovation Call for Proposals (CFP): Ideation to Commercialization**

  Objective of the Call: The product development process includes idea generation, screening, concept development, product development, and commercialization. The objective of this CFP is to further innovation and product development by funding a project to the subsequent stage(s) in the process. For example, the team may propose funds for market research (concept development), if that is the next stage of the product development, for prototype creation (product development), or for other mechanisms to advance commercialization.

  This program utilizes SWVA Node funds and is open to PIs from public institutions of higher education from CCI Southwest Virginia (SWVA).

  Selection Criteria: Proposals were reviewed by subject matter experts and evaluated according to the following criteria:

  - Commercialization potential (20%): clearly defined problem/unmet need; how the proposed technology will address this problem/need; technical feasibility; data or prototype availability; and strength, experience, and engagement of team.
  - Market potential (20%): market size or opportunity; strength of competition and competitive products; ability of proposed solution to capture market share; and ability to secure long-term competitive advantage including IP protection.
  - Development plan and budget (20%): clear and appropriate budget that aligns with technology development plan; plan can be achieved in allotted time frame with requested funding; milestones have defined end points and deliverables; scientific/development methods are valid.
  - Value of the funding (20%): commercialization funds will move technology to clearly defined next stage or inflection point; value of potential technology development exceeds the risk-adjusted cost of funding; achievement of milestones will de-risk technology and/or validate market opportunity; and funds will have proportional impact on moving technology forward with CCI goals.
  - Alignment and qualifications (20%): relevance to CCI focus areas; and suitability of team background to proposed work.

  Innovation Grants Awarded

  The number and value of grants associated with the program are tabulated in Figure 4.1. Individual grants are listed in the Appendix 2.

University	Number of Grants	Grant Total
Virginia Tech	2	$60,000
Radford University	1	$30,000
Total	**3**	**$90,000**

Figure 4.1: SWVA Ideation to Commercialization.

Automated Functional Scenario Creation. This project intends to advance and formalize the automated creation process of simulated driving events, and corresponding parameters, based on naturalistic driving data (NDD). In turn, these advancements will lead to increased commercialization

potential for these technologies, particularly via support of their use in scenario libraries within the automotive sector. The use of scenario-based test cases and scenario selection is an economical alternative to statistical distance-based validation of technology, which requires the onerous, and sometimes impossible, task of driving billions of miles with vehicles equipped with Advanced Driver-Assistance Systems (ADAS) and Automated Driving Systems (ADS) on live public roads. Previous efforts have used real-world crash and near-crash events in simulation environments to develop, evaluate, and specify requirements during ADAS and ADS technology development. However, applying this methodology across large-scale NDD could take years, making the results irrelevant by the time that work is completed. The project will focus on the use of automated methods and processes to minimize human annotation in the creation of these events. The resulting collection of scenarios will enable further development and research into autonomous vehicles and related cybersecurity issues. The scenario collection developed under this investigation will also serve as a catalyst for future cyberthreat projects that utilize simulation, thereby growing the capabilities of the CCI nodes.

- **Cyber RADaR: Cybersecurity Rapid Asymmetric Discovery and Reporting via AI-driven Social Media Crowdsourcing**. Cyber RADaR automates the use of social media to address zero-day cyber threats via development of the Cybersecurity Rapid Asymmetric Discovery and Reporting (Cyber RADaR) managed security service (MSS). Cyber RADaR will use Artificial Intelligence (AI) and Machine Learning (ML) concepts to automate real-time global crowdsourcing and analysis of social media content to proactively deliver an organization-specific "Insights Dashboard" for asymmetric cybersecurity threats and their remediation. Benefits to automating this approach to zero-day threats via the Cyber RADaR product include: 1) Automated collection of diverse thinking and innovative problem-solving data, 2)Quicker understanding of individual zero-day cyber threats and paths to remediation, 3) Problem-centric feedback independent of personal or provider issues/agendas, and 4) An overall situational awareness for both individual and collective cyber threats.

- **Market Research for No-train AI in Enterprise Defense-in-depth Applications**. Stealthy or zero-day attacks such as advanced persistent threats (APT), ransomware (e.g., 2021 Colonial Pipeline hack), supply-chain attacks (e.g., 2020 SolarWinds hack), and insider threats are extremely challenging to detect, because there are no clearly defined attack patterns. Rigid rule-based detection would not be effective. Typical general-purpose machine learning AI approaches would not work for cybersecurity detection either, because they require complex manual tuning and customization to build models – a serious roadblock to deployment. The key feature of our no-train AI technology is automation – automatically compute and detect without supervision. Our solution does not require pre-defined rules and policies or manual supervision. It handles and adjusts to uncertainties in discovering anomalous patterns. The core of this system is the ability to efficiently sift through a huge amount of multi-attribute data and logs and recognize outlier events by modeling and capturing uncertainties associated with human or system behaviors. This new capability is particularly relevant for detecting stealthy or zero-day attacks, including insider threats. To further develop this technology, we first conduct an in-depth survey by interviewing cybersecurity professionals locally and globally and comparing existing commercial solutions (under proper IRB approval). Our user study is centered on several key aspects, e.g., on operational needs, compatibility requirements, detection risks, and real-world human-in-the-loop deployment challenges. We also perform experimental measurement studies to systematically assess and compare the detection capabilities of various cybersecurity solutions (including our no-train AI approach) against stealthy threats and large datasets. If successful, our work will substantially strengthen the defenders' posture in the ever-changing cybersecurity landscape.

Other Southwest Virginia Node Innovation Programs

- **Center for Advanced Innovation in Agriculture (CAIA) University-Industry Symposium on Agricultural Innovation, Artificial Intelligence, and Opportunities (AIAIO)**. Technology application and adoption in food and agriculture requires effective translation of data through integration of data science, software tools, and systems models to create information of relevance for decisions, demonstration of efficiencies, consideration of security, and economic value and return. Conversations

between university researchers and industry sectors increases awareness of need and understanding of challenges. This project creates opportunities for discussions with VT faculty, industry, and other universities by contributing supporting funding (sponsorship) to three major efforts: (1) USDA NIFA funded workshop on artificial intelligence innovations in agriculture (Auburn University, Alabama; March 9-11, 2022); (2) the 2022 Virginia Agriculture and Natural Resources Summit (Richmond, Virginia; April 12-13, 2022) with the theme 'expanding the economy and security of Virginia's agriculture, natural resources, and food systems; and (3) the 2022 Virginia Agricultural Expo (Port Royal, Virginia; August 4, 2022) with the theme of 'Precision for Profits'. The impact will be greater awareness of needs and priorities for agricultural stakeholders and inform university faculty as they are developing interdisciplinary teams, proposals and student training. Through this effort, CCI Southwest is a recognized sponsor to a broad variety of agriculture and life science industries and a number of universities in Virginia and throughout the Southeast US. The estimated reach of promotion and engagement of CCI in agriculture, through partnership with the VT Center for Advanced Innovation in Agriculture and College of Agriculture and Life Sciences, is approximately 1,000 university, industry, and agricultural stakeholders.

- **Student Entrepreneurial Ideation Challenge (SEIC)**. The Student Entrepreneurial Ideation Challenge (SEIC) project was developed to provide a robust, guided entrepreneurial ideation experience for students interested in a cybersecurity career by allowing them to develop cybersecurity solutions/business ideas and then present them to a panel of industry and innovation professionals. The 8-week program brought together six teams of university students located in Southwest Virginia and partnered them with a cyber professional to shape and develop a solution to a cyber security challenge currently faced by companies across the Commonwealth. The challenge entitled, "Solutions to Enable Small Business to Prepare for, Identify and Defend Against the Largest Cybersecurity Threat Areas" allowed the teams to work collaboratively to develop a solution that addressed the top five cybersecurity threat areas that face small businesses. The challenge was posted on the CivilianCyber Workforce Innovation Network platform, which is where the students would submit their solutions. A panel of industry professional then judged the submissions against a standard rubric of five key criteria including creativity, application of new thinking and innovative approaches to the challenge topic. In addition to the ability to win cash prizes the program also allowed them to hone their critical thinking skills and then showcase their talents to potential future employers and development organizations that have the potential to help them to make their ideas reality. The last step in the project included each team virtually presenting their solution to an audience that included representatives from CCI SWVA, CivilianCyber, academia, industry as well as VA-based startup accelerators.

- **Tech Showcase**. This project was tasked with creating a Technology Showcase to demonstrate the work that VTTI has been doing for the past two funding cycles. Researchers from around the commonwealth were invited to take part and present or demo their CCI research as well. This event was designed to enable the sharing of research with the aim of fostering collaboration between CCI nodes moving forward. In total, the event had 14 presenters for research projects. Researchers presented on everything from security research in bitflipping DNNs (Deep Neural Networks) to the use and detection of "Deepfakes" artificially created photos and videos. The attached itinerary has the full list of speakers and their talk titles. Significant interest in presenting led to the creation of two poster sessions during the day and resulted in presentations by 14 (mostly) students from around the commonwealth. In total, the event had 24 active participants either providing a traditional presentation with slides or a poster presentation, and 32 total external (non-VTTI) attendees. As part of the event we also invited companies to attend and hear about the cyber research being performed through CCI. We were able to attract representatives from two companies (AT&T and Indra) with the intent of demonstrating potential avenues for working together moving forward on small-scale 5G test deployments to prove out use-cases and applications for the technology.

4.2.4 Central Virginia Node

The CVN funded two programs that involved both commercialization and workforce development. Those are described in Chapter 3.

Chapter 5

Collaborative Partnerships and Projects

5.1 Partnerships

5.1.1 Arlington County Smart Community Pilot

CCI's partnership with the Arlington County Smart Community Pilot has been continued into FY23 through the funding of one faculty member, Nirup M. Menon, Ph.D., professor and Associate Dean, George Mason University School of Business. This program has installed optical and auditory sensor technology in a designated, commercial zone through a public-private partnership with US-Ignite, Comcast, the Commonwealth Cyber Initiative, and Arlington County. The goals of the effort are to: 1. improve understanding of pedestrian movements and enhance first-responder response time to urgent calls, 2. provide awareness of the county's public safety efforts, and 3. leverage county public assets through a demonstration project designed to benefit residents' public health and safety.

Arlington County requested Dr. Menon's team to continue working on the project citing their work as invaluable to the success of the project thus far. In fact, The National Association of Counties has recognized Arlington County as the 2022 Number One Digital County for its population size. This will represent the fifth number one recognition in the last seven years and seven of seven being number one or number two. No other County has ever recorded such a run. The credit is due to the technology workforce that has been assembled. Arlington County, CTO Jack Belcher credits CCI, stating "The support we have and continue to receive from trusted partners as yourself and CCI has been extraordinary. Your participation and understanding of our mission have enabled the County to achieve where others can only aspire. I believe the most significant element of our success has been the culture we have created, where there is shared ownership of technology initiatives. We have tried to create a 'technology start-up in the business of government'. Your insight and support have created the opportunity to act in such a manner".

5.1.2 CyManII

Three Virginia universities participate in Cybersecurity Manufacturing Innovation Institute (CyManII), an inclusive national research Institute with major leading research universities in cybersecurity, smart and energy efficient manufacturing, and deep expertise in research and development, supply chains, factory automation, and workforce development. Led by The University of Texas at San Antonio and funded by the Department of Energy (DoE), CyManII aggregates the most advanced research institutions in smart and advanced manufacturing, securing automation and supply chains, workforce development, and cybersecurity. The research team brings to bear the most powerful expertise and infrastructure needed to secure the digital transformation that will continue to propel the U.S. in innovated research in manufacturing for decades.

CCI has provided cost sharing funds that enabled VT, VCU, and Mason's Living Innovation Lab in Arlington serving as the East Coast headquarters for CyManII, as well as, the CCI NoVa Node. CCI

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	207	$21M	$28M	$52M	$1.0M
Indirect	137	$10M	$14M	$25M	$0.8M
Induced	150	$8M	$14 M	$24M	$1.4M
Total	494	$39M	$56M	$101M	$3.3M

Table 5.1: Economic activity supported by CCI in Virginia: FY21. (Source: IMPLAN, RTI analysis of CCI spending data.)

institutions participation in CyManII open up opportunities for CCI researchers and industry partners to have a major impact on the security of manufacturing and supply chain.

5.1.3 Industry-led Consortia

O-RAN Alliance

In FY21, CCI joined the O-RAN Alliance, whose objective is to transform the radio access networks industry towards open, intelligent, virtualized and fully interoperable Radio Access Network (RAN). The expectation is that O-RAN standards will enable a more competitive and vibrant RAN supplier ecosystem with faster innovation, and that O-RAN based mobile networks will improve the efficiency of mobile network deployments and operations.

Using our NextG testbed, CCI is doing world-leading work in the integration of an open source 5G implementation, srsRAN, with the O-RAN architecture.

Next G Alliance

The Next G Alliance is a new initiative to advance North American mobile technology leadership over the next decade through private sector-led efforts. With a strong emphasis on technology commercialization, the work encompasses the full lifecycle of research and development, manufacturing, standardization and market readiness.

CCI is a contributing member of the Next G Alliance, with our researchers participating in each of the working groups of the Alliance. This provides a path to impact the emerging vision for 6G and to translate our researchers' work into commercially adopted solutions.

Open Generation Consortium

CCI is also a founding member of the Open Generation Consortium, a privately funded R&D community that brings together diverse technical experts and domain leaders to envision, design, develop, and demonstrate innovative solutions uniquely enabled by emerging 5G capabilities. The consortium is led by MITRE Engenuity, with members from industry, academia, and non-profit organizations.

The current focus of the consortium is in 5G connectivity for drones. CCI, in partnership with MITRE, led the first experiments conducted by the consortium, a proof-of-concept demonstration of 5G connectivity for control of drones, conducted in VT's Drone Park in Blacksburg.

5.2 Correlated Economic Outcomes

In the beginning of FY21, CCI commissioned an economic impact study, conducted by RTI International. Their report, delivered in August 2021, provides a baseline for benchmarking CCI results in future years, as well as early indicators of the economic impact that the initiative has already had. For references purposes, the correlated economic outcomes data from the RTI report for Fiscal Year 2020 and Fiscal year 2021 are listed in Tables 5.1 and 5.2. CCI plans to commission RTI for a second Economic Impact Study in early Fiscal Year 2024.

Below are the correlated Economic Outcomes from the Regional Nodes.

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	237	$23M	$30M	$55M	$1.2M
Indirect	143	$10M	$15M	$26M	$0.9M
Induced	161	$8M	$15 M	$26M	$1.5M
Total	541	$41M	$60M	$107M	$3.5M

Table 5.2: Economic activity supported by CCI in Virginia: FY20. (Source: IMPLAN, RTI analysis of CCI spending data.)

5.2.1 Central Virginia Node

In FY22, the Central Virginia Node created the Dreams to Reality (D2R) Incubator. D2R focuses on supporting engineering start-ups by creating faculty-student partnerships, encouraging students to pursue entrepreneurship and expanding cyber-related businesses in the commonwealth.

Through the Central Virginia Node Dreams to Reality Program (D2R), two start-ups were supported, VirtualIPLC and SymPLe Solutions Inc (SSI). SymPLe Solutions was incorporated as a C-Corps entity in early 2022 for the purpose of "transitioning safety and security computing intellectual property (IP) originally developed in the VCU Dependable and Secure Cyber Physical Systems (DeCyPS) Lab to the energy sector marketplace. In April 2022, SymPLe Solutions secured $120,000 of early seed funding from an industrial investor in the nuclear energy sector. External commercialization funding was secured from two sources in 2022: an external investor and the Electric Power Research institute.

SymPLe Solutions Inc is now a new high-tech company in the commonwealth headquartered int he Richmond area, employes three people and has a pre-market valuation of $5M. VirtualIPLC is still in the early stages of technical and business development but will continue to participate in D2R in fiscal year 2023.

5.2.2 Coastal Virginia Node

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.

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.

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 began working with the Port in the summer 2022.

5.2.3 Northern Virginia Node

The Northern Virginia Node has three successful workforce development and innovation programs and have three patents pending that have or will directly and positively contribute to the commonwealth's economic

and job growth metrics. Additional programs are ongoing including a new Apprenticeship program, and the new CCI+A Cybersecurity Incubator program that supports the development of 8 new companies. Their positive impact cannot be fully evaluated as these programs launched in early summer 2022.

Impact of High School Cybersecurity Internship Program: 30 New Internships

CCI Nova Node is currently funding 30 high school students for internships with cybersecurity companies. The experience includes a 2-week professional skills training program to prepare the students for the professional work environment. The program runs from June 20, 2022 – August 5, 2022. Following the FY21 experience, 4 interns were offered new paid internships as a result of their participation in the CCI NoVa Node FY21 program and 6 interns were invited to undertake cyber certifications at the expense of the host companies. In summary, 10 new positions were created.

Impact of University/College Cybersecurity Entrepreneurship Internship Program: 22 New Internship; 35 New Positions

CCI NoVa Node ran two cohorts of cybersecurity internships with early-stage companies during the 2021-2022 Academic Year. Overall, the program received 178 applications for a total of 40 available internships, hosted by 18 different companies. 50% of selected interns identified as female and 78% identified as minorities. 31 of the 40 students were offered a full-time position or another internship at the conclusion of their CCI experience. An additional four (4) students received employment offers for a position once they graduate college. In summary, the initiative yielded 35 new positions.

Impact of the Innovation commercialization Assistance Program (ICAP)

In FY22, seven (7) new cybersecurity companies completed the ICAP course, with additional entities identified and scheduled to join the July 2022 cohort. As such, the ICAP team has identified strategic opportunities to interface with companies who might benefit from ICAP and pursued them as such. A number of initiatives for FY23 – including personnel support for the CCI+A cyber accelerator and its own invite-only mini-summit – are currently being planned to boost the economic outcomes of this program. Overall, in addition to the 7 new companies, 33 cybersecurity companies benefitted from ICAP, generating over $7M in in economic impact, retaining 15 jobs in the Commonwealth, and creating 10 new jobs.

Patents Pending

- Moving Traffic Control System to 5G MECs, Santos Jha, Satish Kolli, M. Palash, and Duminda Wijesekera (George Mason University)
- Detecting Object not Visible in Color Images, Yongxin Wang and Duminda Wijesekera (George Mason University)
- Countering Autonomous Vehicle Usage for Ramming Attacks, Duminda Wijesekera, Steve Kan, Zoran Duric, and Fernando Camille (George Mason University)

5.2.4 Southwest Virginia Node

The Southwest Virginia Node seeks to impact the cyber economy in the southwest region by supporting faculty with funding for projects and initiatives that have a direct of potential positive impact on the regional economy.

Innovation: Ideation to Commercialization

The Innovation: Ideation to Commercialization program seeks to further innovation and product development by funding a project to the subsequent stage(s) in the process. Funds are available for market research and concept development, prototype creation (product development), and other mechanisms to advance commercialization. They may support proof of-concept testing; independent verification and validation to

be performed by a contract research organization; or costs associated with applying for a patent or a business license in Virginia. Three new programs were funded through this initiative in FY22, each promising to move research from the lab to products of benefit to society.

Wise Minds at Work

Wise Minds at work places student interns with startups to provide cybersecurity training. Comments from Medentum about the program include: "The interns are working on crucial projects to transition our products from prototypes to a minimum viable product. In doing so, we expect to have products on the market in early 2022 that will transform rural health and address health disparities in Southwest and beyond. This project has positively supported our product development and we are grateful for its support." One intern has "helped us identify FDA requirements for cybersecurity and is currently working on a manufacturing feasibility analysis to explore medical device supply chains and strategies to bring manufacturing to Southwest." Those involved with the PCCC project add: "For the industry, our primary benefit is that much of the work impacts over 30% of the domains on the internet today. And it allows us to continue our work with the McGrail Foundation and the open-source projects and research we support. The Commonwealth of Virginia will benefit primarily from keeping talent in-state and the applicable corporate and employee tax base." Atomicorp, a cybersecurity early stage company also involved in the program, has attracted $3M in venture capital and has won federal contracts in the 14 months since its establishment.

SmallSat and SmallSat Testbed for Cybersecurity and Resiliency

This program's goal is to streamline the economic climate for small satellite manufacturers in the Commonwealth. The SmallSat testbed is a one-of-a-kind testbed that allows for new R&D and technology development in space, cyber, networking, swarming, etc.

CCI SWVA Cyber Internships - GCAPS

The purpose of this project was to provide work-based experiences for students in the Danville Community College Cybersecurity program.

We expect to generate a number of additional research opportunities either through proposed CCI grants or outside sources depending on the exact projects pursued. In addition to these research opportunities, there are potential areas for collaboration with both of our industry partners made possible by demonstrating our work in cyber security and related fields.

Chapter 6

Financial Report

6.1 CCI Hub

The budget and expenditures for the CCI Hub in FY22 are shown in Figure 6.1.

The CCI Hub budget remained unchanged from FY21 at $7.5M to execute CCI's three mission lines: research, workforce development and innovation. FY22 was a year or organizational maturity and expansion of research capabilities and reach. CCI hired four additional staff members, two research faculty, three post-doctoral researchers, and 19 part-time graduate research assistants to support specific grant research projects and testbed development. With the staff hires, the CCI staff is now fully capable of supporting the growing number of CCI sponsored and hosted events, pre and post award grant management support to the research faculty, and standard administrative and operations functions for an organization of CCI's size.

In the research mission line, the CCI Hub awarded nine grants for a network-wide collaborative research program, Securing the Next Generation (NextG) of Networks. Communications networks are part of the nation's critical infrastructure, and this CCI research program strives to develop the technologies that make these networks secure. CCI made significant hardware and software investments in research infrastructure for the CCI network. The CCI xG Testbed became fully operational in FY22. The CCI xG Testbed is the first end-to-end ORAN compliant 5G/6G network with fully integrated artificial intelligence infrastructure capable of supporting researchers from the entire CCI network with its remote access capability. CCI's shared, network-wide, unique, state-of-the-art research infrastructure enables research and experimentation on 5G/6G networks, cyber manufacturing, medical device security, smart transportation, AI assurance, smart cities, and many other cybersecurity related functions and sectors. The CCI investment in testbeds is positioning Virginia as a national leader in 5G and NextG research and experimentation.

As the COVID-19 restrictions eased in FY22, CCI hosted several in-person events and the CCI researchers increased travel to conferences and workshops meeting the objective to foster collaboration and cooperation among researchers and students in Virginia. CCI hosted the inaugural CCI Symposium in Richmond, Virginia with over 200 researchers and students from the CCI network meeting in-person for the first time. The symposium included speakers, poster presentations, research presentations, and research focused training for both faculty and students. Going forward, the CCI Symposium will be the annual gathering of CCI network researchers and students to discuss cybersecurity topics, present research findings, attend training events and hear from industry, government, and academic leaders in the field. CCI hosted the Cyber Innovation Boot Camp and the CCI Cyber Camp that educated community college, undergraduate, and graduate students in how to bring cybersecurity ideas and inventions to market and provided hands-on cyber training, as well as, soft-skills training and resume writing to better prepare students to enter the Virginia job market following graduation and continue to close the cyber jobs gap in the state.

In FY22, CCI expenditures exceeded the total of appropriated funds by just over $500,000 due to commitments from FY21 that materialized during FY22.

CCI Hub Fiscal Year 2022		
FY22 Appropriation: $7,500,000		
Mission	Committed	Expenditure
Operations		
Labor		$ 2,497,184.00
IT/Phone/Print	$ 25,384.00	$ 207,762.00
Supplies	$ 177.00	$ 20,812.00
Professional Development	$ -	$ 74,593.00
Communications	$ 2,300.00	$ 83,371.00
Travel/Conferences/Workshops	$ 32,585.00	$ 115,754.00
CCI Symposium/Camps		$ 79,913.00
Operations/Rent/RTI Contracts	$ 61,352.00	$ 671,545.00
Sub Total	$ 121,798.00	$ 3,750,934.00
Workforce Development and Innovation		
Sub Awards (Programs)	$ 235,655.00	$ 1,503,905.00
Women in Cybersecurity Sponsor		$ 3,500.00
CATAPULT Co-Sponsorship		$ 200,000.00
Sub Total	$ 235,655.00	$ 1,707,405.00
Research		
Hub Faculty		$ 361,694.00
Securing NextG Research Program		$ 299,567.00
xG Testbed	$ 33,212.00	$ 938,997.00
xG Testbed Contract Support		$ 72,603.00
ECE Graduate Student Funding		$ 239,981.00
GRA Tuition		$ 42,959.00
SWVA Node Equipment		$ 250,000.00
Sub Total	$ 33,212.00	$ 2,205,801.00
Totals	$ 390,665.00	$ 7,664,140.00
Total Expenditure & Committed		$ 8,054,805.00

Figure 6.1: Budget and expenditures for CCI Hub in FY22.

6.2 CCI Nodes

In FY22, the CCI Regional Nodes developed spend plans that supported Node objectives, initiatives, and programs that were aligned with their cybersecurity focus areas and the expertise of their research faculty. The Nodes apportioned their funds into three categories: Operations, Research, and Innovation/Workforce Development. Although the categories are the same and all focused on the cybersecurity field, each Node has the flexibility to plan and execute funds so as to best meet the needs of their region and reinforce the cybersecurity research focus of their region's universities and verticals. In FY22, the Nodes continued to support collaboration across the CCI network of university researchers and students by sponsoring Node funded and administered collaborative research programs. Additionally, the Regional Node's funded and hosted events, workshops, and initiatives within the region.

Additionally, one of the Node's hired a Program Manager to oversee the day-to-day functions of the Node and assist the Node Director with operations and administration tasks. With this hire, all of the Regional Nodes now have a full-time Program Manager. One Node hired a Communications Specialist to manage the Node web site, perform public and media relations, and promote and brand the Node across the CCI network and their region.

6.2.1 COVA Node

The budget and expenditures for the CoVA Node in FY22 are shown in Figure 6.2.

The Coastal Virginia Center for Cyber Innovation, as a CCI Node, serves as southeastern Virginia's engine for research, innovation, and commercialization of next-generation cybersecurity technologies, particularly in the areas of Cyber Physical Systems Security and Artificial Intelligence in maritime, defense, and transportation industries.

Funds to support research were used in five areas: (1) continued funding of research scientists, (2) cross-node research project funding, (3) computing infrastructure support at node institutions, (4) enhancements of the Coastal Virginia Shared Academic and Research Environment, and (5) the creation of a dissertation fellowship program.

Funds are also used in cross-node research studies that promote collaboration between faculty across institutions. While $750,000 will be used for these projects in FY23, a third of those funds are targeted for projects that involve institutions across the entire commonwealth. Two proposal tracks will be used: one that funds fundamental and applied research and innovation and a second one that increases understanding about the social dynamics of cyber victimization for individuals and businesses in the Commonwealth. The Node also upgraded the computing infrastructure across institutions in the Coastal Virginia region. In addition, funds were used to purchase upgrades and additional licenses for the Coastal Virginia Shared Academic and Research Environment.

Funds to support regional innovation and development of the talent pipeline were used to promote experiential learning, support undergraduate research, promote student-led innovation programs, continue to provide experiential learning programming for graduate students, develop cybersecurity curricula, support commercialization, and develop the CoVA CCI Regional Student Association. The undergraduate research program matches students and faculty from across the node to engage in cybersecurity research programs. The Innovate Cyber Challenge brings together students from across the node to identify and propose solutions to cybersecurity challenges. The graduate student experiential learning program assigns graduate students from one of the research institutions as graduate assistants to help instructors in node institutions that do not have graduate assistant help.

6.2.2 CVN

The budget and expenditures for the CVN in FY22 are shown in Figure 6.3.

CVN continued to support CCI mission items, particularly focusing on Smart City Technologies and Medical Device Security. CVN saw progress on existing projects throughout FY22 and made improvements in commercialization.

For research, VCU continued to support ongoing CVN projects at VCU including the Smart City Testbed, Medical Device Security Testbed, and related ongoing research. UVA continued the previously started

CCI Coastal Virginia Node Fiscal Year 2022		
FY22 Appropriation: 2,500,000		
Mission	Budget	Expenditure
Operations		
CoVa CCI Staff (Salary & Fringe)		240,000
Misc Operations		58,890
Sub Total		298,890
Workforce Development and Innovation		
Experiential Learning Admin Support		348,000
Undergraduate Research Program		65,600
Innovate Cyber Challenge		90,000
Graduate Student Experiential Learning		100,000
Cybersecurity Regional Student Assoc		15,000
Cyberseucity Curriculum Devel Project		50,000
Cyber Policy & Law Symposium		3,770
Sub Total		344,370
Research		
Research Scientist (Salary & Fringe)		348,000
COVA SHARE (Research lab)		18,180
Node Cybersecurity Lab Upgrades		510,560
Research Projects		880,000
Doctoral Fellowships		100,000
Sub Total		1,856,740
Total Expenditure		2,500,000

Figure 6.2: Budget and expenditures for the CoVA Node in FY22.

research, workforce, and innovation programs that show the best potential for impact, as well as, identified new opportunities focused on collaborating with partners within the CCI Central Virginia Node.

In workforce development and innovation, CVN supported several internal projects for experiential learning and innovation and commercialization.

CCI Central Virginia Node Fiscal Year 2022		
FY22 Appropriation: 2,500,000		
Mission	**Budget**	**Expenditure**
Operations		
Salary and Fringe		100,000
Support		150,000
Sub Total		250,000
Workforce Development and Innovation		
Experiential Learning CFP		250,000
Innovation Programs (VCU)		125,000
Innovation Programs (UVA)		125,000
Sub Total		500,000
Research		
Hub Research Programs		250,000
Research Programs (VCU)		750,000
Research Programs (UVA)		750,000
Sub Total		1,750,000
Total Expenditure		2,500,000

Figure 6.3: Budget and expenditures for the CVN Node in FY22.

6.2.3 NOVA Node

The budget and expenditures for the NoVA Node in FY22 are shown in Figure 6.4.

In May 2021, the NoVa Node opened the Cyber Living Innovation Lab at George Mason University's Arlington Campus in space leased and paid for by George Mason University as part of ongoing contributions

to CCI. The Living Innovation Lab includes robotic platforms to evaluate 5G performance and security vulnerabilities. The lab is also used to study the impact of 5G on industry, internet of things or Industry 4.0, and smart manufacturing, as well as the vulnerability of the supporting power grid. The lab includes autonomous vehicle sensor study, 5G performance, and security vulnerability assessment capabilities. These platforms support LIDAR, radar, stereo, and night vision cameras that will be deployed on the NoVa Node's fleet of vehicles to simulate autonomous driving.

In research, the NoVa Node created the Cybersecurity Research Collaboration Funding Program that fosters cross-pollination opportunities for NoVa Node cybersecurity researchers to collaborate across the Commonwealth with researchers from one or more Nodes in support of the development of a Commnwealth-wide ecosystem of innovation excellence in cybersecurity. Research focused on the intersection of cyber physical systems security, particularly in the defense, transportation, energy, manufacturing, and connected communities/infrastructure sectors. Additionally, research exploring the impact of human behavior on cybersecurity, Resilience of Cyber systems to Human Behavior and Robust and Adaptive Cyber-Human Systems was funded. The NoVa Node also worked towards developing an ecosystem for collaborative, commercialized cybersecurity R&D in Northern Virginia. This initiative strives to advance the CCI NoVa Node's strategic goal to develop an ecosystem which fully utilizes existing private sector capabilities, in combination with those of the higher education community, in order to pursue and maximize collaborative, commercially viable cybersecurity research and development (R&D) opportunities in the region. Industry/government were also invited to submit concepts for calls for proposals to support a partnership between industry and institutes of higher education to collaborate in applied cybersecurity research.

In FY22, the CCI NoVa Node made significant investments in cybersecurity related experiential learning opportunities for high school students, college/university students, and those seeking to upskill into cybersecurity positions within industry and government. These opportunities enabled students to apply classroom knowledge to real world challenges and bridge the "experience" divide. These investments endeavor to expand the pipeline of cybersecurity career-ready talent. The NoVa Node invested in a mix of internships, apprenticeships, and research assistantships to maximize the number and variety of opportunities available to NoVa Node students. In addition, the NoVa Node expanded George Mason University's Clearance Readiness Program to increase the number of students across the NoVa Node who are prepared to enter and complete the security clearance process and denote that preparation with an electronic badge so employers can quickly identify these candidates. The most significant investment was in subsidized internships and to assist up-skill, non-degree seeking candidates, with special emphasis on displaced workers as a result of the pandemic. These candidates have the opportunity to complete a subsidized apprenticeship in conjunction with their training to support the successful transition to full-time employment in cybersecurity. NoVa Node also supported research assistantships that enabled undergraduates to participate in the cybersecurity research enterprise and prepare them for work in established or emerging companies working at the leading edge of R&D. Finally, the NoVa Node invested resources in K-12 teacher training in cybersecurity to bring cybersecurity modules and expertise to teachers and enable them to transfer the knowledge across the spectrum of K-12 age groups and classroom subjects.

6.2.4 SWVA Node

The budget and expenditures for the SWVA Node in FY22 are shown in Figure 6.5.

The Southwest Virginia Node of the Commonwealth Cyber Initiative (CCI SWVA) continued to provide alignment of efforts in cyber research, innovation, and workforce development across a variety of stakeholders to demonstrate efficiencies and economies of scale. CCI SWVA partners coupled cores of technical excellence in wireless communications, emerging technologies, and cybersecurity with unique and expansive capabilities in the application domains of transportation, power systems, manufacturing, and agriculture, to discover, demonstrate, and commercialize technological solutions that will enable the next industrial revolution.

CCI SWVA continued major research initiatives in: 5G Protocol Enhancements for Multi-Scale Latency; Emerging Technology and Crypto; 5GPG: 5G Power Grid; Secure communication between Autonomous Systems - Drones, Automobiles, and Infrastructure; SmallSat Testbed for Cybersecurity and Resiliency; Artificial Intelligence and Visual Analytics in Cybersecurity Research; and Networking Optimization in Rural Agriculture Testbeds. The research mission of CCI SWVA was advanced through its Research Engagement and Cross-Node Research Programs.

CCI Northern Virginia Node Fiscal Year 2022		
FY22 Appropriation: 2,500,000		
Mission	**Budget**	**Expenditure**
Operations		
Admin/Operations		255,000
Sub Total		255,000
Workforce Development and Innovation		
Undergraduate Research Assistants		80,000
Cybersecurity Apprenticeship		400,000
Undergraduate Internships		500,000
Cyber.org Teacher Program		25,000
High School Internships		90,000
CCI+A (CATAPULT)		200,000
ICAP		100,000
Sub Total		1,395,000
Research		
Collaborative Research 2022		250,000
Industry-Faculty Collaboration Acceleration Program (IFCAP)		400,000
Impact of Human Behavior on Cybersecurity		200,000
Sub Total		850,000
Total Expenditure		2,500,000

Figure 6.4: Budget and expenditures for the NoVA Node in FY22.

CCI SWVA continued its Regional Innovation thrust by providing Tech Transfer Support, holding a Cyber Tech Summit, and equipping participants with an Entrepreneur Toolkit. Talent Pipeline programs were expanded to include the CCI SWVA Internship Program designed to incorporate all partner institutions. Additionally, SWVA Node initiated Talent Pipeline programs including: Artificial Intelligence and Visual Analytics in Cybersecurity Experiential Learning for Workforce Readiness, HackHouse: Open Access IoT Lab in a Box, Research Experiences for Community College and K-12 Teachers, and Competition Training to Increase Pathways to Cybersecurity Workforce. Throughout the year, SWVA Node continued its collaboration with the Virginia Cyber Range is included.

CCI Southwest Virginia Node Fiscal Year 2022		
FY22 Appropriation: 2,500,000		
Mission	**Budget**	**Expenditure**
Operations		
Personnel		279,383
Other Operations Costs		8,194
Sub Total		287,577
Workforce Development and Innovation		
Innovation Programs		180,000
Workforce Programs		598,557
Sub Total		778,557
Research		
Major Thrust Areas		1,169,500
Research Collaboration Program		250,000
Research Engagement Program		14,366
Sub Total		1,433,866
Total Expenditure		2,500,000

Figure 6.5: Budget and expenditures for the SWVA Node in FY22.

6.3 Geographic distribution of the awards from funds contained in HB30

Figure 6.6 shows the distribution of awards from funds in HB30.

Node	Number of Awards	Grant Total
Central Virginia	7	$2,980,000
Coastal Virginia	4	$2,816,040
Northern Virginia	8	$3,329,784
Southwest Virginia	9	$6,402,678
CCI Hub	1	$100,000
Total	**29**	**$15,628,502**

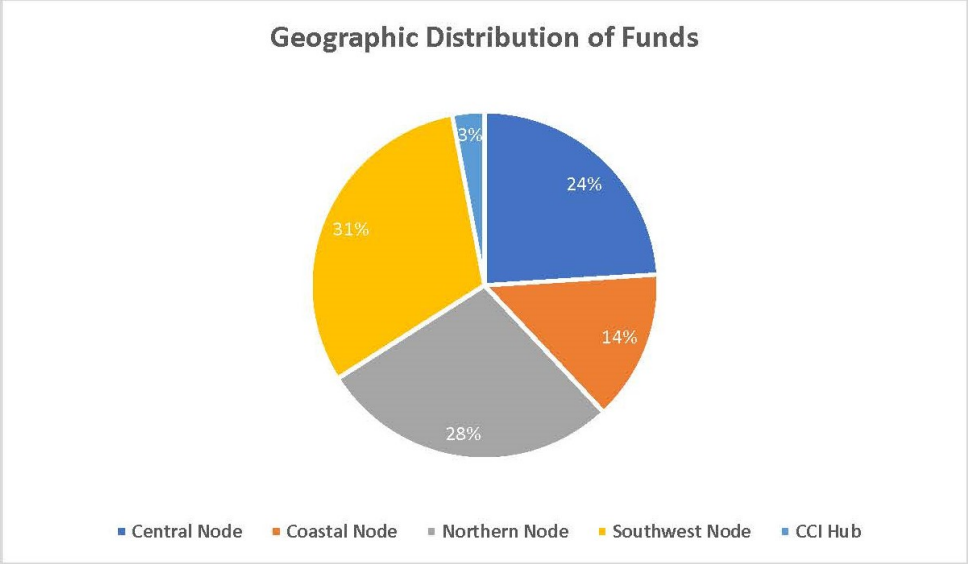


Figure 6.6: Geographic distribution of awards using FY22 funds.

Chapter 7

Looking Ahead: FY23

FY22 saw a vast expansion in the research, innovation, and workforce development programs launched by the CCI Hub and by each of the regional Nodes. Most of this report thus far has been devoted to describing the main accomplishments of the CCI network in FY22. In this chapter, we outline the main activities and programs planned for FY23.

Our major goals for the coming fiscal year include:

- Continuing to develop trans-disciplinary approaches to cybersecurity, focusing on the research theme of securing human-machine interactions and exploring technical, legal, social, and public policy aspects of the problem.
- Strengthening and supporting multi-institution teams in Virginia to compete for large-scale research and workforce development grants from the federal government and industry.
- Expanding our innovation programs, bringing our researchers together with venture capital, and continuing to align our innovation initiatives with those available through the VIPC and other sources.
- Scaling up our internship and apprenticeship programs.
- Extending our research infrastructure with a new outdoor 5G and Next G testbed using CBRS licensed spectrum.
- Raising our profile and building new partnerships nationally and internationally.

We discuss each of these goals in turn.

7.1 Transdisciplinary Cybersecurity

In FY22, we have proceeded with a refresh of CCI's research themes. The new research themes align with our focus on cybersecurity and show strong potential across our three mission lines of research, innovation, and workforce development. The process of arriving at the new research themes included in-person workshop at each of the four CCI Nodes as well as consultation with our Technical Advisory Board (TAB) and industry partners. The research themes reflect our view of cybersecurity as an intrinsically multi-disciplinary field.

The new research themes are as follows:

- **Securing the Next Generation of Networks**: Communication networks are part of the country's critical infrastructure, and in CCI we develop the technologies that make these networks secure. The US industry has made an investment of more than $350 billion in the fifth generation of mobile networks, or 5G. Even larger investments have been made by industry and government in Europe and Asia. Cybersecurity is an area where the US has historically led, and CCI plays a leading role in securing the deployment of 5G and in the vision for the next generation of mobile networks (NextG). CCI is a member of the NextG Alliance, the major industry-led effort in mapping out a North American

vision for NextG, providing us a unique opportunity to transition our research into the standardization process. Key research areas include: open interfaces and standards; virtualization and network disaggregation; integration of cyber physical systems; quantum information science; secure and flexible spectrum.

- **Securing Human-Machine Interactions**: Recent evolution in artificial intelligence, cyber physical systems, and communications are leading to a world where humans and autonomous machines increasingly interact. In CCI we view cybersecurity as intrinsically cross-disciplinary and devise solutions that lead to secure, resilient, and harmonious interactions between people and robots, drones, autonomous vehicles, and other cyber physical systems. Our research focuses on the technological challenges in securing this enhanced digital world experience, in close collaboration with experts from the social sciences, life sciences, health sciences, law and humanities. Key research areas include: AI Assurance; hacking humans; the metaverse; security and privacy for embedded devices; and ethical cybersecurity.

In FY22 we continued to make a large investment in securing NextG, including $900K in seed funding for CCI researchers and continued development of the CCI xG Testbed. In FY23, our major research seed funding program will focus on the theme of Securing Human-Machine Interactions, requiring close collaboration between researchers in STEM disciplines and those in the humanities, social sciences, public policy, and law.

In Fall 2022, we are launching a call for proposals to all CCI researchers to build trans-disciplinary capabilities in the technological challenges in securing an enhanced digital world experience, in close collaboration with experts from the social sciences, life sciences, health sciences, public policy, law and humanities. Topics of interest include, but are not limited to: artificial intelligence assurance; securing the metaverse; security and privacy for embedded and/or wearable devices; the role of human behavior in securing the digital world; and ethical cybersecurity.

This program will be co-funded by the CCI Hub and the NoVA and SWVA Nodes. Objectives of the program include:

- To produce seminal contributions to securing the interactions between humans and machines, targeting the expansion of this research through competitive grants from the federal government, private sector, philanthropic foundations, and other sources.
- To contribute to workforce development in cybersecurity with cross-disciplinary domain knowledge.
- To explore opportunities for innovation (commercialization, entrepreneurship, etc.) in security and privacy for the interaction between humans and machines.

7.2 Large-scale, Multi-institution Collaborations

CCI has built unprecedented strong collaboration among institutions of higher education in Virginia. This has already made us competitive for large grants that require breadth of expertise and critical mass to deliver on large-scale projects. A good example is a $13M DoD grant to five CCI universities, led by Virginia Tech Applied Research Corporation (VT-ARC), to build a 5G smart warehouse pilot in the Marine Corps logistics facilities in Albany, GA. This is a grant that Virginia would not have been competitive for before the advent of CCI; the ongoing project started in FY21. In FY22 we obtained a $3M grant from the NSA National Centers for Academic Excellence in Cybersecurity program focusing on workforce development in election security, in collaboration with the Virginia Department of Elections. The project is led by CCI Fellow Jack Davidson, at UVA, with co-investigators at ODU, VT, NSU, VCU, and Mason.

In FY23, we will continue to focus on these large-scale, multi-disciplinary projects. We are uniquely positioned to attract research funding for large projects in securing NextG, in particular from DoD, and we are working on a multi-university project proposal in that area. We will also explore opportunities in O-RAN research and workforce development that are expected to arise from the recent CHIPS and Science Act.

CCI Hub funds will support our revised CCI Fellows program. This program provides funding for CCI researchers to lead center-scale proposals. PIs funded under this call will be designated as CCI Fellows.

Proposals must involve at least three CCI institutions of higher education (from any Node). A CCI institution of higher education must play a coordination role in the project. The budget associated with CCI institutions in the center-scale proposal must be at least $3 million. Proposals must be in response to a published call or a direct solicitation from a funding agency or company.

7.3 Expanding Innovation Programs

In FY22, we have significantly increased our innovation programs, launching several new programs that help form a new generation of entrepreneurs, transition CCI research into commercializable IP, enable CCI spin-outs, and support the startup ecosystem in Virginia.

For example, the CATAPULT program, launched in early 2022, advances collaborative translational research projects among CCI partners, with the goal of speeding the transition of academic research outcomes to the marketplace.

In FY23, we will continue to grow the CCI innovation programs, described in more detail in Chapter 4, with particular emphasis in bringing CCI researchers funded by those programs in contact with the venture capital community. We also continue to have monthly meetings with the VIPC Division of Commercialization to align our innovation programs with opportunities available through the VIPC, such as the Commonwealth Commercialization Fund (CCF), and to make our researchers competitive for such funding.

This coming year we are also commissioning a study to be conducted by RTI to assess CCI's innovation programs, benchmark them against best practices, and provide recommendations. The team has set the following objectives for this study:

- Conduct an early assessment of CCI programs developed to assist the cybersecurity innovation ecosystem in Virginia.
- Identify and qualitatively and quantitatively characterize best-in-class examples and best practices to inform and inspire CCI about enhanced and successful innovation programs.
- Provide recommendations to improve or augment both existing and future CCI innovation programs: what works, where there are gaps, and where there are opportunities to improve.

7.4 Scaling Up Internship and Apprenticeship Programs

Our internship and apprenticeship programs have been among the most successful experiential learning programs that CCI has created. They have attracted an extremely diverse population of students, a particular victory in cybersecurity, where women and Black and Latino professionals are still severely underrepresented. These programs are also heavily oversubscribed, and we are able to only select a small portion of the applicants for funding.

The numbers from some of our recent programs tell the story:

- A high school internship program run by the CCI NoVA Node in FY22 received 181 applications for 30 available positions. Of those selected, 37% are female, 20% will be the first in their families to attend college, and 40% self-identify as part of an underrepresented group in STEM.
- For the first cohort of interns in our Cyberstartups program, funded by the CCI Hub, we received 145 applicants for 15 positions. A total of 80% of the selected interns come from underrepresented groups; 11 of the 15 interns received post-internship job offers.
- A new apprenticeship program launched this year by the CCI NoVA Node received 400 applications for 21 positions. Of those selected, 43% are female, 19% are veterans, and 90% belong to underrepresented population groups in cybersecurity.

The demand for these programs confirms that they fill an important need: practical experience is critical for retention of students in cybersecurity and in these students' competitiveness for good jobs once they graduate. In FY23 we plan to expand our internship programs, from high school to graduate school, and our apprenticeship opportunities.

7.5 Extending Our Research Infrastructure

The CCI testbeds have been expanding rapidly. This year, we inaugurated three new testbeds at VCU. The medical device security testbed is outfitted with real commercial medical devices to be tested for security vulnerabilities and that researchers use to develop mitigation solutions. The OpenCyberCity testbed (pictured) is a realistic, small-scale cityscape in which to run experiments related to smart cities and autonomous vehicles. It has a fully operational water treatment plant, miniature UAVs, and a range of smart city sensors. And, complementing CCI's xG testbed, VCU now has an isolated environment where we can conduct 5G and Next G experiments without causing or suffering interference.

In FY23 we plan to deploy the first outdoor testbed in CCI. It will complement the xG Testbed deployed in the CCI Hub, providing the ability to experiment with new technologies for 5G and NextG networks in an outdoor environment. The testbed will have dual use for production and research. It is being planned jointly by the VT Information Technology division and CCI.

The testbed will operate in CBRS spectrum. The Virginia Tech Foundation (VTF) acquired four CBRS Priority Access Licenses (PALs) in each of Montgomery County and Craig County in FCC Auction 105. This spectrum is to be used for research, operations, and rural and regional broadband, through partnerships.

The outdoor testbed is being planned for deployment around Stroubles Creek in Blacksburg, as a private wireless network. The tentative sites and expected coverage map are shown in Figure 7.1.

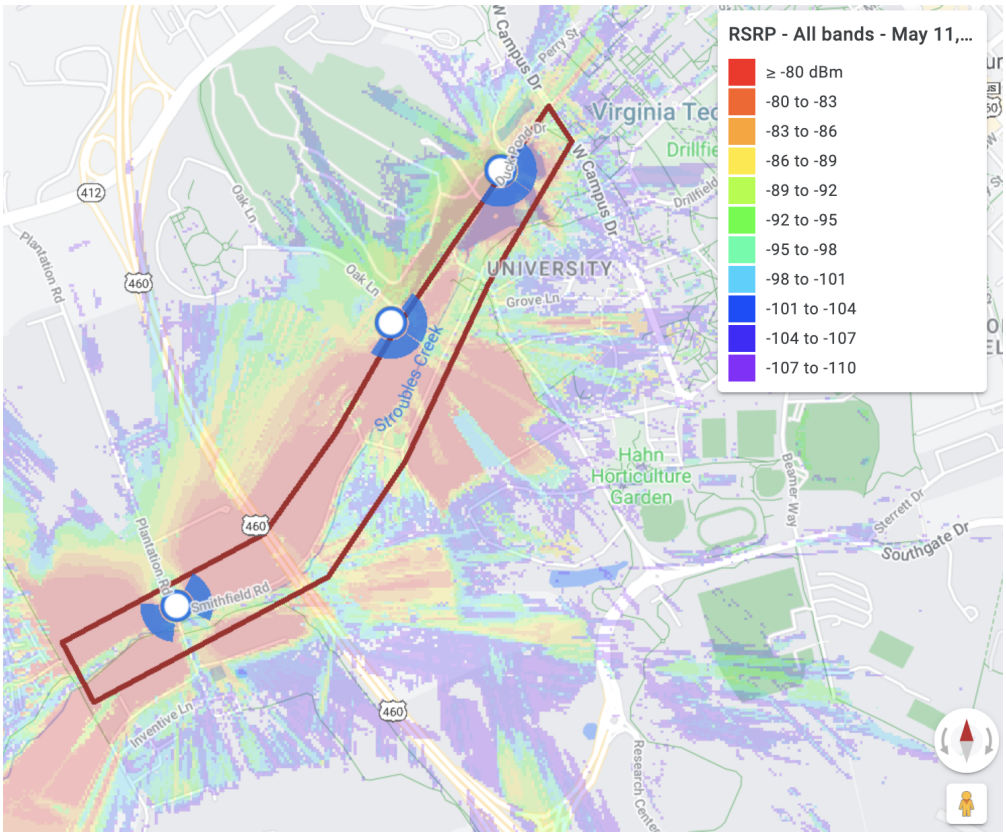


Figure 7.1: Planned site locations and coverage for outdoor component of CCI xG Testbed in Blacksburg.

The production component of the testbed will be used for flood monitoring in Stroubles Creek. The initial deployment will include three sites, outfitted with commercial and test/research radio equipment, including the same family of SDR that is used in the xG Testbed in the CCI Hub. The basic network and node concepts are illustrated in Figure 7.2.

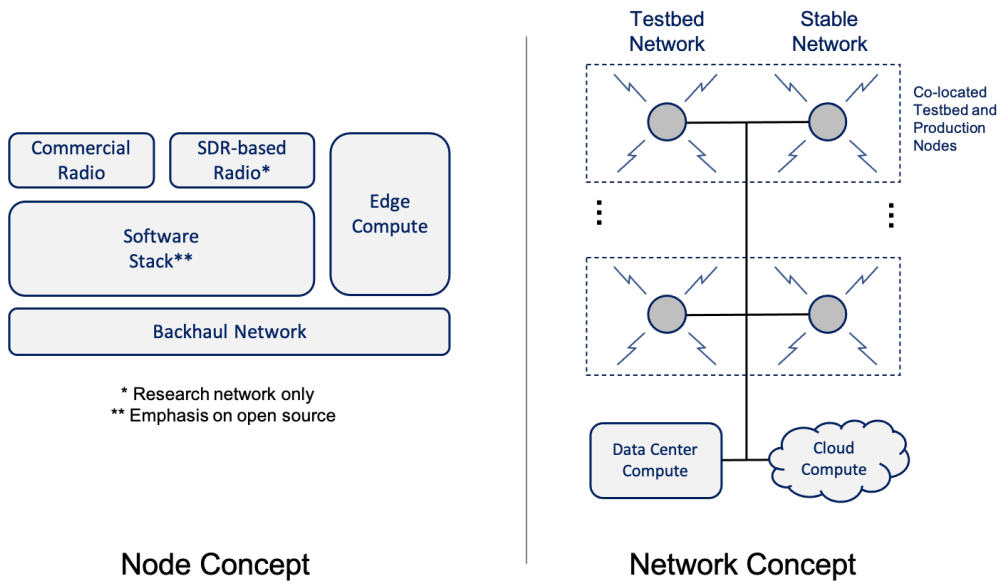


Figure 7.2: Network and node concepts for the outdoor component of the CCI xG Testbed.

7.6 Building New Partnerships

In the first years of CCI we focused on capacity building and investing in new programs that made Virginia more competitive for research grants, more capable of translating that research into commercializable products and services, more effective in growing and diversifying our cyber workforce. In FY23, we will place additional emphasis on building partnerships with institutions in other states and other countries, raising our profile and increasing awareness of our unique research infrastructure, depth and breadth of expertise, and rich workforce development and innovation programs.

For the first time, we will participate in the Mobile World Congress (MWC) Americas, to be held in Las Vegas, NV, in September 2022. MWC Las Vegas, in partnership with CTIA - The Wireless Association (CTIA), is the Global System for Mobile Communication Association (GSMA)'s flagship event in North America, showcasing the hottest trends in connectivity and mobile innovation. The event has strong representation from the North American Wireless communications industry. CCI will have a booth highlighting our testbed capabilities, in particular the first end-to-end fully O-RAN-compliant testbed, as well as a CCI-developed SDR implementation of a CBRS access point.

We are also building international collaboration with large groups in Europe. We recently hosted a delegation from Finland, led by the Minister of Economic Affairs Mika Lintila, and the Ambassador of Finland to the U.S., Mikko Hautala. The delegation, shown in Figure 7.3, explored opportunities for collaboration between CCI and some of the leading universities in Finland on the topic of 5G and NextG security. Following the visit, we have started a collaboration with researchers in the University of Oulu, Finland, who are global leaders in research on 6G systems.

We are also building a partnership with a group in Ireland focusing on workforce development. We are partners in the Cyber Skills Initiative in Ireland, which is designing, in close partnership with industry, cybersecurity pathways for students to follow. The CCI Executive Director, xG Testbed Director, and Portfolio Director have been invited to participate, with funding from NSF and from Cyber Skills, in the "Transatlantic (US-Ireland-Northern Ireland) Workshop on Collaborative IoT/CPS Cybersecurity Research," taking place in October 2022.

Figure 7.3: Left to right: (Back) CCI NextG Testbed Director Aloizio DaSilva, Special Adviser to the Minister Teppo Säkkinen, Director-General Riku Huttunen, CCI Managing Director John Delaney, Under-Secretary Petri Peltonen, Science Counselor Petri Koikkalainen, 6G Flagship Government Relations and Public Affairs Director Iina Peltonen. (Front) Counselor, Embassy of Finland to the U.S., Heli Hyypiä, Adviser to the Minister of Economic Affairs Nina Alatalo, CCI CTO and Virginia Tech Professor Jeffrey Reed, Minister Mika Lintilä, CCI Executive Director Luiz DaSilva, and Ambassador Mikko Hautala. Photo by Hilary Schwab for CCI.

Appendices

Appendix 1

CCI Extramural Funding for FY22, CCI Hub

Project Title	PI	Lead Institution	Funding Amount	Funding Agency
JBPHH 5G Initiative Aircraft Mission Readiness Application: C-17 - Growler/EA-18G Project		Virginia Tech	$208,096	DoD
Collaborative Research: SaTC: CORE: Medium: A Networking Perspective of Blockchain Security: Modeling, Analysis, and Defense		Virginia Tech	$600,000	NSF
Measuring and Investigating Internet Censorship through Ground-truth based, End-to-End Framework		Old Dominion University	$200,000	Open Technology Funds
Total			**$1,008,096**	

CCI Extramural Funding for FY22
Coastal Virginia Node

Project Title	PI	Lead Institution	Funding Amount	Funding Agency
Toward Safe, Private and Secure Home Automation: From Formal Modeling to User Evaluation		William & Mary	$799,839	NSF
W&M Cybersecurity Awareness Initiative for Public Interest Technology University		William & Mary	$90,000	New Venture Fund
Tribe Venture Cohort: William & Mary Student Venture Incubator Program		William & Mary	$1,000	Alan B. Miller Entrepreneurship Center
Extended Reality Enabled 5G Telementoring		Old Dominion University / Virginia Modeling and Simulation Center	$115,000	HRBRC
Top Down 5G Network Security Design		Old Dominion University / Virginia Modeling and Simulation Center	$50,000	Deloitte
Cyber Risk and Resilience Analytics		Old Dominion University / Virginia Modeling and Simulation Center	$70,000	FTI
Analytically Based Frameworks for AI Model Verification and Improvement in Cyber Physical Systems		Old Dominion University / Virginia Modeling and Simulation Center	$60,000	NSF
Center of Excellence in Machine Learning		Old Dominion University / Virginia Modeling and Simulation Center	$350,000	DoD
Collaborative Research: CCRI: New: Medium: A Development and Experimental Environment for Privacy-Preserving and Secure (DEEPSECURE) Machine Learning		Old Dominion University	$780,000	NSF
Backdoor Detection, Mitigation and Prevention in Deep Neural Networks		Old Dominion University	$500,000	NSA
Blockchain-based AI/ML Management to Enable Smart NextG Wireless Networks		Old Dominion University	$100,000	InterDigital
Cybersecurity Job Creation System (CJCS)		Old Dominion University	$1,450,000	GoVA

CCI Extramural Funding for FY22
Coastal Virginia Node

Project Title	PI	Lead Institution	Funding Amount	Funding Agency
2021 DoD CySP Grant Program: Training Cyber Talents for DoD Workforce		Old Dominion University	$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		Old Dominion University	$145,000	NSA
JROTC Students and Teachers Interactive Learning		Old Dominion University	$175,000	NSA
VA-CNIP: A Coalition for the Virginia Cyber Navigator Internship Program		Old Dominion University	$210,000	NSA
A Graduate Certificate in Web Archiving		Old Dominion University	$98,361	IMLS
Total			**$4,580,200**	

CCI Extramural Funding for FY22
Northern Virginia Node

Project Title	PI	Lead Institution	Funding Amount	Funding Agency
RINGS: Learning based Distributed SDN for Immersive Experience over Directional Wireless Edges		George Mason University	$899,975	NSF
Collaborative Research: SaTC: CORE: Medium: UNIC: Towards a User-Centric Trust Secured Internet of Things		George Mason University	$991,364	NSF
RINGS: Security, Privacy and Trust Establishment (SPaTE) for the NextG Edge-to-Cloud Continuum		George Mason University	$1,000,000	NSF
CAREER: Securing Protections of Internet- Scale Cybersecurity System with Continuous Evaluation and Evolution (CEE)		George Mason University	$588,756	NSF
CManII		George Mason University	$880,000	DOE/UTSA
EAGER: DCL: SaTC; EIC: Inclusive Scam Detection Methods for Social Media to Design Assistive Tools for Protecting Individuals with Developmental Disabilities		George Mason University	$299,248	NSF
Safety Evaluation of Positive Train Control		George Mason University	$840,000	Federal Railroad Association/Ensco
Commercial Grade 5G Testbed Equipment		George Mason University	$455,000	COMSovereign
Commercial Grade Building Automation Systems Equipment		George Mason University	$65,000	Siemens
CIF: Signal Processing and Learning for NOMA Millimeter-Wave Massive MIMO Systems		George Mason University	$320,000	NSF
NSF Convergence Accelerator Track G: Secure Texting over Non-Cooperative Networks and Anti-Jamming Enhancement in 5G		George Mason University	$750,000	NSF
Collaborative Research: SWIFT: Intelligent Dynamic Spectrum Access (IDEA): An Efficient Learning Approach to Enhancing Spectrum Utilization and Coexistence		George Mason University	$750,000	NSF
Total			**$7,829,343**	

CCI Extramural Funding for FY22
Central Virginia Node

Project Title	PI	Lead Institution	Funding Amount	Funding Agency
Digital forensic Tools and Techniques for Investigating Control Logic Attacks in Industrial Control Systems		Virginia Commonwealth University	$150,000	DHS
SymPLe Phase III: Technology Advancement of SymPLe with Respect to Nuclear IEC61508 Certification Requirements		Virginia Commonwealth University	$171,000	Electric Power Research Institute (EPRI)
Context Aware Augemented Reality for Cognitive Assistance in Emergency Medical Services		Virginia Commonwealth University	$1,139,275	NIST
MoodRing: A Multi-Stakeholder Platform to Monitor and Manage Adolescent Depression in Primary Care with Passive Mobile Sensing		Virginia Commonwealth University	$1,700,000	NIH
Repurposable Devices for a Greener Internet of Things		Virginia Commonwealth University	$700,000	NSF
Adaptive Ventilation Strategies for Optimizing Indoor Air Quality and Building Energy Consumption		Virginia Commonwealth University	$123,548	Trane
Socially Informed Service Conflict Governance Through Specification, Detection, Resolution and Prevention		Virginia Commonwealth University	$2,300,000	NSF
Opportunities and Challenges for Indirect Sensing in Smart Buildings		Virginia Commonwealth University	$50,000	LMI
Electric Vehicle Integrated Safety, Intelligence, Operations (eVISION)		Virginia Commonwealth University	$150,000	Battelle Energy Alliance/INL
Protective Relay Master Fault Detector AI Algorithm		Virginia Commonwealth University	$75,000	Battelle Energy Alliance
Cyber Physical Anomaly Detection for Wind		Virginia Commonwealth University	$150,000	Battelle Energy Alliance
Solar Assisted State Aware and Resilient Infrastructure System Data Driven Models for Threat Detection and Visualization		Virginia Commonwealth University	$247,725	Battelle Energy Alliance
INL Fleet and Technology Support		Virginia Commonwealth University	$20,000	INL
VA-CNIP: A Coalition for the Virginia Cyber Navigator Internship Program		University of Virginia	$2,880,005	NSA/DHS
CICI: UCSS: Helix++: Securing Open Science Platforms		University of Virginia	$498,021	NSF
Total			**$10,354,574**	

CCI Extramural Funding for FY22
Southwest Virginia Node

Project Title	PI	Lead Institution	Funding Amount	Funding Agency
Identification and Impact Assessment of ADAS Dependent Technologies		Virginia Tech	$331,888	DoT
GenCyber RU Secure Camp for K-12 Teachers		Virginia Tech	$89,944	NSA
DALNIM: Dependency Based Assessment of Litigious Network Events Impacting the Mission		Virginia Tech	$260,000	Agency for Defense Development (ADD-ROK)
Cybersecurity Research and Advanced Training of ROTC Students (CREATORS)		Virginia Tech	$812,269	Griffiss Institute
CRII: SaTC Backdoor Detection, Mitigation and Prevention in Deep Neural Networks		Virginia Tech	$175,000	NSF
Collaborative Research: CCRI: New: Open AI Cellular (OAIC); Prototyping Artificial Intelligence-Enabled Control and Testing Systems for Cellular Communications Research		Virginia Tech	$999,947	NSF
IARPA SCISRS		Virginia Tech	$279,549	BAE Systems
Educational Supplement to NeTS: Medium: Implications of Receiver RF Front End Nonlinerarity on Network Performance: Fundamentals, Limitations and Management Strategies		Virginia Tech	$165,238	NSF
Collaborative Research: SWIFT: Contect-aware Spectrum Coexistence Design and Implementation in Satellite Bands (ASCENT)		Virginia Tech	$562,500	NSF
Demonstration of Indoor Positioning for 5G Systems		Virginia Tech	$490,178	National Spectrum Consortium
QuIC-TAQS: Interconnected Superconducting and Color Center Qubits in Silicon Devices		Virginia Tech	$480,000	NSF
Identification and Impact Assessment of ADAS Dependent Technologies		Virginia Tech	$508,000	AOR
SaTC: CORE: Small: Empowering Network Attack Detection with Complex Graph Modeling		Virginia Tech	$500,000	NSF
Empowering Cyber Threat Hunting Using Cyber Threat Intelligence		Virginia Tech	$70,183	Cisco

CCI Extramural Funding for FY22
Southwest Virginia Node

Project Title	PI	Lead Institution	Funding Amount	Funding Agency
Towards an AI Powered Active Phishing Protection Scheme		Virginia Tech	$25,000	4-VA
Energy Centric Wireless Sensor Node System for Smart Farms		Virginia Tech	$573,750	NSF
Unrestricted Gift for Research on blockchain based Management for Next Generation Wireless Networks		Virginia Tech	$100,000	InterDigital
Secure and Resilient Operations Using Open-source Distributed systems Platform (OpenDSP)		Virginia Tech	$600,000	DoE
Power Electronics Power Distribution Systems (PEPDS)		Virginia Tech	$150,000	ONR
Universal Interoperability for Grid-forming Inverters (UNIFI) Consortium		Virginia Tech	$750,000	DoE
Custom Made 5G RAN and CORE		Virginia Tech	$400,000	Widality and Comsoverign
White Rabbit Based PNT Solution		Virginia Tech	$200,000	OPNT
Cybersecurity Characterization Study of Electric Vehicle Battery Management Systems		Virginia Tech	$757,486	NHTSA/DoT
NEC 5G Deployment and 5G Implementation. Short Title: NEC 5G Smart Intersection		Virginia Tech	$113,285	NEC (Private)
Private 5G Technology		Virginia Tech	$55,950	Safe-D UTC
Remote Experimenter		Virginia Tech	$25,000	NSTSCE
Open AI Cellular: Prototyping Artificial Intelligence-Enabled Control and Testing Systems for Cellular Communications Research		Virginia Tech	$295,000	NSF
Broadband Adoption Rise in Rural Communities Using Rail Tracks		Virginia Tech	$80,000	IFCAP
Senior Military College Cyber Institute		Virginia Tech	$2,849,997	DoD
Soft Auditing on Trust for Detecting Clandestine Executions with Maximum Deployability		Virginia Tech	$900,000	ONR
Total			**$13,600,164**	

Appendix 2

Securing NextG Research Grants

Central Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Secure Federated Learning for Autonomous Vehicles in the NextG Networks	H.Shen	University of Virginia		$100,000
Securing Smart Microgrid with DERs in NextG	Z. Wang	Virginia Commonwealth University	Y. Zao / VCU	$100,000

Coastal Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Blockchain-based Deep Learning Management to Enable Smart NextG Wireless networks	R. Ning	Old Dominion University	H. Wu / ODU C. Xin / ODU H. Guo / NSU	$100,000

Northern Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
HEaaS: Securing Cyber Physical Systems in NextG Using Homomorphic Encryption	B. Han	George Mason University	S. Chen / Mason	$100,000
Energy Preserving NextG Cryptography for Power Constrained Devices	K. Khasawneh	George Mason University	S. Dinakarrao / Mason	$100,000
Securing Sofwarization and Disaggregation in NextG: Call to Disaggregate Trust Management	D. Wijsekera	George Mason University	A. DaSilva / VT V. Shah / Mason	$100,000

Southwest Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Secure Management and Orchestration of NextG Networks	L. Freeman	Virginia Tech	S. Shetty / ODU D. Jakubisin / VT T. Erpek / VT	$100,000
Securing Non-Terrestrial Networks in NextG	N. Tripathi	Virginia Tech	J. Reed / VT	$99,567

CCI Hub

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
DoS Attack-Resilient Initial Access for mmWave/Thz based NextG Communications	J. Kibilda	CCI Hub / Virginia Tech	V. Shah / Mason K. Zang / Mason P. Pathak / Mason	$100,000

Southwest Virginia Node Research Engagement Program

Project Title	PI	Lead Institution	Grant Amount
Improving routing security with a complete view of Routing Origin Validation (ROV) in RPKI	T. Chung	Virginia Tech	$15,000*
Secure Federated Multi-Agent Deep Reinforcement Learning For Dynamic Spectrum Access in NextG Communication Systems	T. Doan	Virginia Tech	$7,500*
Verifiable and Privacy-Preserving Machine Learning as a Service	T. Hoang	Virginia Tech	$15,000*
Cyber Intrusion Detection in Substation Automation Systems based on Adversarial Machine Learning	M. Jin	Virginia Tech	$15,000*
Security Issues and Challenges of Voice-based Social Networks	Y. Jung	Virginia Military Institute	$13,898
Electromagnetic Side-Channel Attacks Leveraging Solid-State Quantum Sensors	L. Shao	Virginia Tech	$14,539*
Improving BIM Security and Trust in Built Environment Using Distributed Data Environment and Authentication Through Blockchain	A. Shojaei kol kachi	Virginia Tech	$5,237* $468
			*FY21 Funds executed in FY22

Southwest Virginia Node Ideation to Commercialization Program

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Automated Functional Scenario Creation	M. Perez	Virginia Tech		$30,000
Cyber RADaR: Cybersecurity Rapid Asymmetric Discovery and Reporting via AI-driven Social Media Crowdsourcing	J. Pittges	Radford University	Bobby Keener / Civilian Cyber	$30,000
Market Research for No-train AI in Enterprise Defense-in-depth Applications	D. Yao	Virginia Tech		$30,000

Bibliography

Virginia State Budget. (2018). Budget Bill - HB5002 (Chapter 2) [Accessed: 15 July 2020]. https://budget.lis.virginia.gov/item/2018/2/HB5002/Chapter/1/252/PDF/