Commonwealth Cyber Initiative

Fiscal Year 2020 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 2020 REPORT

Commonwealth Cyber Initiative

October 1, 2020

Message from the Executive Director

The Commonwealth Cyber Initiative (CCI) creates a unique opportunity to establish Virginia as a global center of excellence at the intersection of security, autonomous systems, and data. With a mission of research, innovation, and workforce development, this initiative has the bold ambition to serve as a catalyst for the Commonwealth's long-term leadership in this sector.

The area of focus for CCI could not be more timely. We are on the verge of a new technology revolution, similar to what we experienced decades ago with the advent of the Internet. This time, the revolution in services and applications is being led by the ubiquity of cyber physical systems powered by Artificial Intelligence (AI). These range from drones to robotic arms, from sensors and actuators to autonomous vehicles. Trustworthiness and security are prerequisites for their adoption by major industries such as manufacturing, transportation, and energy. This technology revolution has the potential to fundamentally change how entire sectors of the economy operate, and CCI is well positioned to lead in research and innovation at the confluence of security, autonomy, and data.

I joined as the inaugural Executive Director of CCI in mid-March 2020, and the Node Directors and the interim leadership of the CCI Hub had already been hard at work laying the foundations of our research, innovation, and workforce development programs. I am extremely proud of what the network has already accomplished in such a short time and despite the challenges of the COVID-19 crisis. This report describes these accomplishments, as well as our strategy and plans for the near future.

I hope the report conveys the excitement that the entire team feels in creating this unique ecosystem of university and industry collaboration for Virginia. We deeply appreciate the investment that the Commonwealth is making in CCI and are confident in our ability to deliver lasting impact.

Luiz DaSilva, Ph.D.; Fellow, IEEE
Executive Director, Commonwealth Cyber Initiative
Bradley Professor of Cybersecurity, Virginia Tech

List of Figures

List of Tables

List of Acronyms

3GPP 3rd Generation Partnership Project

5GC 5G Core

5GPG 5G for the Power Grid

ADS Automated Driving System

AI Artificial Intelligence

AISLE AI-Security Living Lab Experience

AoA Angle of Arrival

AoD Angle of Departure

ARO Army Research Office

ATC Air Traffic Control

BER Bit Error Rate

BS Base Station

CATRDG Cyber Advanced Transitional Research Development Grant

CBRS Citizens Broadband Radio Service

CCI Commonwealth Cyber Initiative

CDN Content Distribution Network

CeVA Central Virginia

CIA Central Intelligence Agency

CoVA Coastal Virginia

CPI Critical Program Information

CPS Cyber Physical System

CPSS Cyber Physical Systems Security

CSI Channel State Information

CSIIP Commonwealth STEM Industry Internship Program

CTO Chief Technology Officer

CV2X Cellular Vehicle-to-everything

CYMANII Cybersecurity Manufacturing Innovation Institute

DARPA Defense Advanced Research Projects Agency

DDoS Distributed Denial of Service

DNS Domain Name System

DoD Department of Defense

DoE Department of Energy

DoS Denial of Service

DSRC Dedicated Short Range Communications

ECPI East Coast Polytechnic Institute

EPC Evolved Packet Core

FCC Federal Communications Commission

FY Fiscal Year

GIS Geographic Information System

GMU George Mason University

gNB Next generation NodeB

GPU Graphics Processing Unit

GRA Graduate Research Assistant

HMI Human Machine Interface

ICAP Innovation Commercialization Assistance Program

ICAT Institute for Creativity, Arts, and Technology

IDC Inclusion & Diversity Committee

IDIA Institute for Digital InnovAtion

IEEE Institute of Electrical and Electronic Engineers

I/O Input/Output

IoT Internet of Things

IP Intellectual Property

IT Information Technology

ITIF Information Technology and Innovation Foundation

ITS Intelligent Transportation System

JMU James Madison University

LC Leadership Council

M2M Machine-to-machine

MAAP Mid-Atlantic Aviation Partnership

MAC Medium Access Control

MEC Mobile Edge Computing

MIMO Multiple Input Multiple Output

ML Machine Learning

MTD Moving Target Defense

MURI Multidisciplinary University Research Initiative

NDN Named Data Networking

NHTSA National Highway Traffic Safety Administration

NICERC National Integrated Cyber Education Research Center

NIST National Institute of Standards and Technology

NN Neural Network

NOMA Non-orthogonal Multiple Access

NoVA Northern Virginia

NR New Radio

NRO National Reconnaissance Office

NSA National Security Agency

NSC National Spectrum Consortium

NSF National Science Foundation

NSU Norfolk State University

ODU Old Dominion University

ONR Office of Naval Research

P-BSM Pedestrian Basic Safety Message

PCA Pilot Contamination Attack

PI Principal Investigator

PKI Public Key Infrastructure

PLC Programmable Logic Controller

QoS Quality of Service

RAN Radio Access Network

RARE Radar and Radio Engineering

RD Random Direction

RF Radio Frequency

RFID Radio Frequency Identification

RT Real Time

RWP Random Waypoint

SAE Society of Automotive Engineers

SAS Spectrum Access System

SBDC Small Business Development Center

SBIR Small Business Innovation Research

SCADA Supervisory Control and Data Acquisition

SCMS Security Credential Management System

SDR Software Defined Radio

SGX Software Guard Extensions

SHM Structural Health Monitoring

SKA skills, knowledge, and abilities

SLS Sector Level Sweep

SNR Signal to Noise Ratio

STEM Science, Technology, Engineering, and Mathematics

STTR Small Business Technology Transfer

SUMO Simuation of Urban Mobility

SWVA Southwest Virginia

TAB Technical Advisory Board

TEE Trusted Executed Environment

TVWS Television White Spaces

UAV Unmanned Autonomous Vehicle

UE User Equipment

USDOT U.S. Department of Transportation

USIM Universal Subscriber Identification Module

USRP Universal Software Radio Peripheral

UVA University of Virginia

V2I Vehicle-to-infrastructure

V2N Vehicle-to-network

V2P Vehicle-to-pedestrian

V2V Vehicle-to-vehicle

V2X Vehicle-to-everything

VC Venture Capital

VCU Virginia Commonwealth University

VIPA Virginia Innovation Partnership Authority

VPRI Vice President for Research and Innovation

VRIC Virginia Research Investment Committee

VSBFA Virginia Small Business Financing Authority

VT Virginia Tech

VTTI Virginia Tech Transportation Institute

WICL Wireless Innovation and Cybersecurity Lab

W&M William & Mary

Contents

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).

CCI has a Hub and Nodes structure, with the Hub having a coordination role for the entire network, and each of the Nodes playing a more regional role. This structure allows us to establish a cohesive overall strategy for the Commonwealth while also having more targeted initiatives that are tailored to the needs and resources in Northern Virginia, Central Virginia, Coastal Virginia, and Southwest Virginia. The CCI Hub is anchored by Virginia Tech in Arlington, and the four regional Nodes are anchored by GMU, VCU, ODU, and VT (Blacksburg), respectively.

Funding for CCI started to flow in Fiscal Year 20 (FY20), with the Hub receiving its first infusion of funds in July 2019 and the Nodes in February 2020. We have an ambitious goal: to establish Virginia as a global leader in cybersecurity, and by doing so to help diversify the economy of the Commonwealth, attracting industry investment and jobs. This report highlights some of the major accomplishments from the past fiscal year, which are indicative of what the CCI network can still achieve for the Commonwealth:

1. **Leverage:** One key promise of CCI is that the investment that the Commonwealth is making will be leveraged to increase our competitiveness in attracting additional research funding. We already see clear results: In FY20, the eight faculty members in the CCI Hub have attracted a total of $19.4M in new research funding, a 2-to-1 return on the investment made by the Commonwealth. The four CCI regional Nodes report a combined total of $64.3M in active research grants to support CCI-related research. These impressive results demonstrate the multiplicative power of the investment made in CCI, and that we are extremely well positioned to establish Virginia as the premier location in the Nation for cyber innovation and research. A significant proportion of this external funding originates from the federal government, reflecting the strong investments being made at the national level in the CCI focus areas of cybersecurity, autonomous systems, and data.

2. **Scale:** A unique feature of CCI is that we bring together more than 300 researchers across 39 institutions of higher learning. This large-scale collaboration increases our visibility as a top player in the cybersecurity arena and enables us to compete for large programs. An example of this new ability to compete for large grants is the participation of CCI researchers in a major proposal for a trustworthy AI research center, led by VCU with participantion from GMU, UVA, ODU, VT, and Marymount University. Another example is a large effort in cyber-manufacturing involving VCU, GMU, and VT. These are areas where, without CCI, any individual university would not have the critical mass necessary to be competitive in a major program.

3. **Collaboration:** CCI actively promotes collaboration among Virginia researchers. The CCI Leadership Council, consisting of the Hub and Node leadership, meets bi-weekly and coordinates, encourages, and funds these collaborations. Examples abound: a program to build the cyber workforce, funded by the Northern Virginia Node of CCI, involves GMU, James Madison University (JMU), Marymount University, University of Mary Washington, Shenandoah University, Germanna Community College and Lord Fairfax Community College; the INNOVATE Cyber Challenge run by the Coastal Virginia Node of CCI funded students from ODU, Christopher Newport University, ECPI, NSU, W&M, and

Tidewater Community College; the CCI Fellows program funds researchers from GMU, UVA, VT, VCU, ODU, Radford University, and NSU working closely with the CCI Hub leadership and faculty.

4. **Innovation:** The CCI NoVA Node is supporting three Virginia start-ups through translational research development grants, each focusing on the commercialization of a cybersecurity technology. The CoVA Node graduated an inaugural class of 24 undergraduates from 6 institutions who took part in their INNOVATE Cyber Challenge: this next generation of innovators and entrepreneurs worked in teams to propose solutions to cybersecurity problems and advance their ideas by creating business models with support from the ODU Entrepreneurial Center. The newly formed CCI Innovation Committee is working with industry and local government to develop reverse pitch and proof-of-concept funding programs to be launched in FY21.

5. **Research Infrastructure:** We are establishing unique research infrastructure in 5G security and AI Assurance for use by researchers and innovators in Virginia. The CCI 5G testbed is distributed across five locations in Virginia and represents an investment of $8.7M by the CCI Hub and Nodes. Our 5G testbed is unique in its close alignment with key verticals empowered by 5G, its focus on cybersecurity, and unparalleled access to licensed spectrum. The AI Assurance testbed is establishing a distributed, interdisciplinary, virtual exchange to develop and test AI technologies. Both testbeds have already been attracting considerable interest from industry and government agencies. Through our 5G testbed investment we became a founding member of a commercial-grade testbed effort led by the CTIA, which represents the US telecommunications industry, from carriers and equipment manufacturers to mobile app developers and content creators.

6. **Experiential Learning:** From an internship program focusing on cybersecurity startups to a statewide drone competition, CCI is funding unique experiential learning opportunities for Virginia students, complementing the already strong degree granting cybersecurity programs available throughout the Commonwealth. These experiences expose students to state-of-the art technologies and problems in areas such as cyber-crime and data poisoning in satellite reconnaissance, and spark early interest in cybersecurity topics through involvement in a new drone racing competition. We are also funding internships in small and medium size cybersecurity firms to better prepare students for careers in cybersecurity.

7. **Relevance:** The CCI research fields are of particular relevance to the current times. This year, we ran a webinar series highlighting how our researchers work on technologies that impact our response to the COVID-19 crisis, from work at GMU in increasing the resilience of healthcare systems to cyberattacks, to advanced programs at W&M that support secure online operation of court proceedings. We are also discussing a partnership with local governments on privacy-preserving aspects of COVID-19 contact tracing and prevention.

In all of the above, we are actively engaging with industry: to build our 5G testbed, to design and fund an innovation challenge, and to interact directly with our students. There are a few things that industry partners look for when they seek to engage with academia: reputation, to work with the leading researchers in the world in their area of interest; capacity for Intellectual Property (IP) generation; and access to top quality graduates. In CCI, they can find all three. These engagements will ultimately lead to high-quality jobs and a thriving entrepreneurial ecosystem in cybersecurity and autonomous systems in Virginia.

Most of this report is devoted to the accomplishments of this first year of CCI. The last chapter outlines our long-term goals and the main activities that we have planned for FY21. The CCI strategic goals can be summarized as follows:

- CCI will establish organizational structures that incorporate advice from a broad array of stakeholders and mechanisms that assess the impact that the initiative has in Virginia, the Nation, and the world. These include a Technical Advisory Board with participation from leading industry practitioners, government representatives, entrepreneurs, and academic researchers, and an Inclusion and Diversity Committee charged with increasing participation of under-represented groups in the cybersecurity workforce.

- CCI will expand its unique research infrastructure in the areas of 5G security and AI Assurance, leveraging the existing research strengths of the partner universities.
- CCI will fund research that positions Virginia in the leadership in cybersecurity, autonomous systems and data, and that increases the competitiveness of Virginia researchers in obtaining further research investment from the federal government and industry.
- CCI will provide unique experiential learning and early work experiences to Virginia students that complement the instruction provided through degree-granting programs across the state. These experiences combine early exposure to the latest advancements in the field with essential skills in ethics, entrepreneurship, and communication, to produce the most qualified and diverse workforce in the country on cybersecurity, autonomous systems, and data.
- CCI will facilitate the translation of research at the intersection of cybersecurity, autonomous systems, and data into innovation, through the development and protection of intellectual property developed in the CCI network and the fostering of a robust ecosystem of Virginia-based start-ups.

As CCI reaches its two-year mark at the end of FY21, we will commission an economic impact assessment, looking at the effect of the initiative on jobs and economic development in Virginia. We believe even in its first year, the initiative has already had an outsized impact on research funding and economic development, and are confident that this impact will only grow as our initiatives in research, innovation, and workforce development expand.

Chapter 1

Introduction to the Commonwealth Cyber Initiative (CCI)

1.1 A Call to Action

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).

CCI is composed of four Regional Nodes led by public universities across Virginia, and a Hub in Northern Virginia (Figure 1.1). VT serves as the anchoring institution and coordinates the activities of the Hub, which is physically located in VT's facilities in Arlington, VA (Figure 1.2). The Northern Virginia Node is led by GMU; the Central Virginia Node is led by VCU; the Coastal Virginia Node is led by ODU; and the Southwest Virginia Node is led by VT.

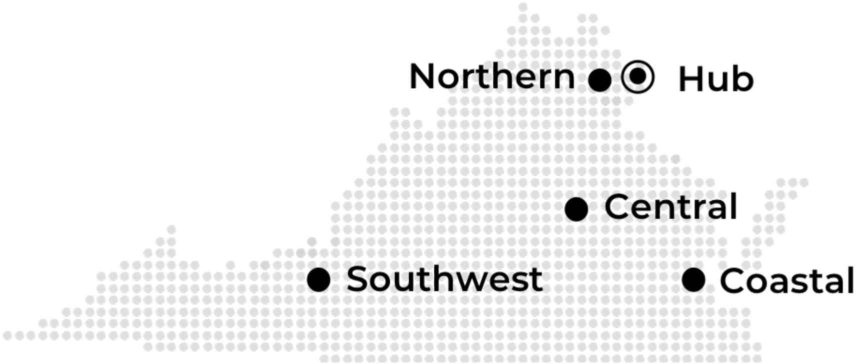
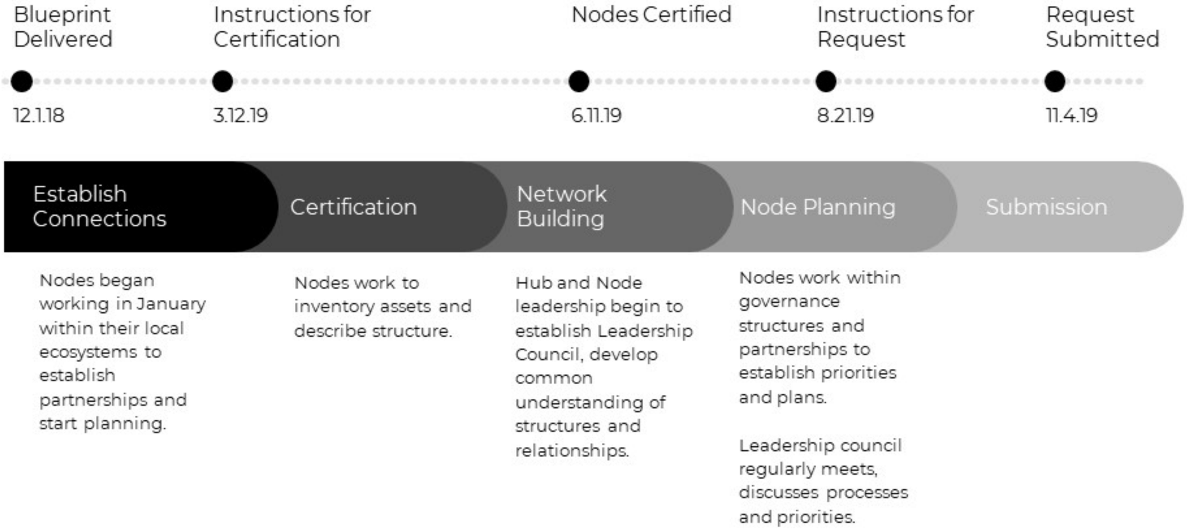


Figure 1.1: CCI Hub and Nodes structure.

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, these form the CCI Leadership Council (LC), which is responsible for setting the strategy and executing the CCI program.

Initial funding for the CCI Hub was received in July 2019, with the Nodes receiving their first infusion of funds around January 2020. In 2019, the Nodes went through a process of certification by the Virginia Research Investment Committee (VRIC) and strategic planning, summarized in Figure 1.3. In FY 2020, $10 million in funds were appropriated for the Hub, with an additional $10 million for the Nodes. Node funds were shared equally between the four Nodes, with each Node establishing its own governance structure and programs serving their geographical area and research focus.

Figure 1.2: The Virginia Tech Research Center - Arlington serves as the home for the CCI Hub.



Blueprint Delivered
12.1.18
Instructions for Certification
3.12.19
Nodes Certified
6.11.19
Instructions for Request
8.21.19
Request Submitted
11.4.19
Establish Connections
Certification
Network Building
Node Planning
Submission
Nodes began working in January within their local ecosystems to establish partnerships and start planning.
Nodes work to inventory assets and describe structure.
Hub and Node leadership begin to establish Leadership Council, develop common understanding of structures and relationships.
Nodes work within governance structures and partnerships to establish priorities and plans.
Leadership council regularly meets, discusses processes and priorities.

Figure 1.3: Node certification and funding process in FY19-20.

1.2 Opportunity for the Commonwealth

The opportunity that CCI presents to the Commonwealth is well articulated in the CCI Blueprint (Commonwealth Cyber Initiative, 2018). This section summarizes the main aspects of this opportunity.

Today, an overwhelming majority of Virginia's firms are focused on providing Information Technology (IT) cybersecurity services to the federal government. This subjects the Virginia economy to federal budget cycles. To build a high-growth, resilient economy, Virginia must also become a leader in consumer- and commercially-facing cybersecurity at the technological frontier.

CCI is focused on breakthrough research and innovation at the intersection of security, autonomous systems, and data, to diversify Virginia's economy and prepare for the continued digital evolution of society. It will also help develop a talented cybersecurity workforce, addressing a key challenge for Virginia's current economy.

CCI exists in a larger ecosystem of programs, platforms, and pipelines that will contribute to its long-term success. It is important to recognize their importance to Virginia's cybersecurity ecosystem. The Commonwealth's cybersecurity talent pipeline has many opportunities for growth before students even enter the higher education system. Early childhood education lays the foundation for a lifetime of learning and success in the digital economy, as interest in and preparedness for a career in cybersecurity start early. Cybersecurity principles and technologies must be incorporated into the curriculum throughout the education system, and increased partnerships with the business community throughout the education system will support robust talent development.

In addition, expanded opportunities and support for dual enrollment between Virginia's K-12 education system to higher education would strengthen the talent pipeline for years to come. By preparing students with targeted cybersecurity courses in high school, time to degree and educational debt can be decreased, giving students a better shot at success. Challenges include hiring and training certified dual-enrollment teachers, as well as enabling efficient articulation with multiple school districts.

Finally, cybersecurity is an all-hands-on-deck challenge. An intentional approach to diversifying the talent pipeline through special efforts to encourage women and minorities to consider a career in cybersecurity will be necessary to produce enough potential workers to meet industry's cybersecurity needs. In addition, cybersecurity permeates every industry and every career. Every student must be prepared to contribute productively and securely to the digital economy.

CCI's potential for success is bolstered by the dynamic, innovative, and growing cybersecurity research, education, and talent development programs across the Commonwealth and capital region. The CCI Blueprint development process highlighted the many programs that exist across Virginia that can be leveraged, amplified, and coordinated through the CCI Network. By building on the best practices of programs across Virginia, CCI will enable a system that is greater than the sum of its parts. The CCI Network will be strongest if it includes the widest possible array of universities and programs.

Virginia is well positioned to be a global leader in Cyber Physical System (CPS) security. It has a baseline of economic conditions primed for growth. For example, Virginia ranked fourth in the Information Technology and Innovation Foundation (ITIF)'s 2017 State New Economy Index. Virginia's stature is rising, having moved up three places since 2014 in that index, which is based on 25 indicators across five areas (knowledge jobs, globalization, economic dynamism, digital economy, and innovation capacity).

Virginia has exceptional strength in IT services and software across many of the indicators included in ITIF's analysis. For example, Virginia ranks highest for concentration of high-growth firms, based on the INC 5000 database. While many of those firms are in the government services sector, Virginia has more than its fair share of high-growth companies in IT services and software.

Another indicator of innovation and potential for economic growth is Venture Capital (VC) activity. A 2016 analysis by Martin Prosperity of VC clusters across the United States found high concentration of VC activity in IT services and software in the national capital region. This highly productive economic cluster in IT services, software, and security will serve as a substantive foundation upon which to build a world-leading research and education center-of-mass in CPS security technologies.

In addition to this economic activity in IT, other indicators of high-growth potential include a highly educated workforce (Virginia is sixth in the nation, and the DC region ranks second). In addition, Virginia ranks second in density of cybersecurity jobs (exceeded only by DC), with four times the national average. There is also a high level of research and development in Virginia. With about $10B in research and development (R&D) expenditures, Virginia ranks 13^{th} in the nation.

1.3 Vision

Advancements in communications, cyber physical systems, and AI are about to usher in a new era of highly-connected, intelligent autonomous systems. This will revolutionize key industries, with manufacturing, transportation, and healthcare as prime areas of innovation potential.

CCI Vision

The Commonwealth Cyber Initiative (CCI) is establishing 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.

1.4 Mission

CCI Mission

The Commonwealth Cyber Initiative serves as an engine for research, innovation, talent development, and commercialization of technologies at the intersection of security, autonomy, and data.

CCI is positioned at the intersection of security, autonomy, and data (Figure 1.4). In this year's Business Facilities State rankings report (Business Facilities, 2020), Virginia was ranked first in the nation in cybersecurity leadership, unmanned aerial systems, and digital infrastructure. CCI's mission lines of research, workforce development, and innovation aim at leveraging the Commonwealth's research and education strengths to firmly establish Virginia as a globally recognized leader in cybersecurity, autonomous systems, and data.

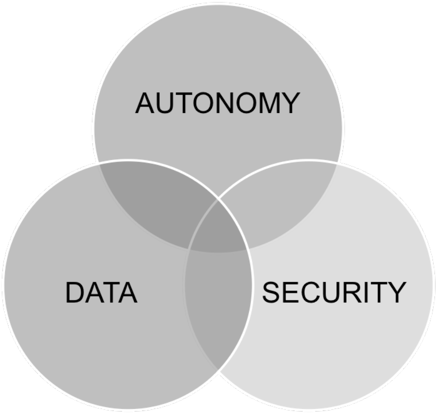


Figure 1.4: The CCI Venn diagram.

1.4.1 Research

The IT landscape is constantly changing, and cybersecurity approaches and technology must move faster. As new computing platforms, devices, and applications are developed—from cloud computing to 5G communications to autonomous systems—the cybersecurity challenges evolve. Putting the nation's most innovative minds to task to stay one-step-ahead of the cyber challenges of tomorrow presents an opportunity for increasing the economic growth of the Commonwealth of Virginia.

A survey of institutions of higher education in Virginia, along with more than 20 industry partners, found an opportunity in aligned industry interest and existing university capability in Internet of Things (IoT), 5G communications, cyber physical systems security, data analytics, machine learning, and AI. CCI targets this opportunity space.

The last decade of the social-mobile Internet is giving way to the next decade of the Internet of Things and the core technologies that will enable it such as 5G wireless. CCI seeks to ensure that as these new technologies are developed, standardized, and deployed, they have the needed security features to ensure that the next generation of the internet and the ecosystems built on top of it are underpinned with systematic security and privacy safeguards.

In each epoch of the internet, security has been bolted on after new technologies experience major breaches, leading to patchy and poorly integrated security solutions. Consumers entrust automobiles, factories, pacemakers, and energy distribution to the IoT, security must not be an afterthought.

Major technologies in autonomous systems are emerging, and 5G wireless standards have taken shape. This is an ideal time to systematically integrate security into edge computing, network slicing, and the protocols and frameworks that will enable smart infrastructure. CCI is leveraging a consortium of selected industry partners to build standards, ecosystems, prototypes, and testbeds and be recognized as a global leader in cyber physical systems security.

1.4.2 Workforce Development

Demand for cybersecurity professionals remains extremely strong in Virginia. As of Summer 2020, according to the Cyber Seek tool (Cyber Seek, 2020), Virginia has more than 10% of the job openings in cybersecurity in the entire country.

A key mission of CCI is to help produce qualified cybersecurity workforce that fills the skills gap, and to attract and retain cybersecurity jobs and professionals to the Commonwealth. CCI does that by creating experiential learning programs that provide hands-on experiences for Virginia students that complement the rich range of academic programs offered by universities and community colleges throughout the state.

1.4.3 Commercialization and Innovation

A core component of CCI's mission is to support cybersecurity innovation commercialization and new ventures in the Commonwealth, making Virginia the best place to start a business in advanced cybersecurity technologies.

The CCI Hub and Nodes work with incubators, accelerators, technology transfer offices, and other resources to connect CCI innovators with the resources they need to accelerate commercialization.

1.5 The CCI Network

Work in CCI started in earnest in 2019, with the naming of an Interim Executive Director, Professor Jeff Reed, and an Interim Managing Director, Dr. Laurel Miner. Directors of the four CCI Nodes were also named: Dr. Liza Wilson-Durant, GMU, leads the Northern Virginia Node; Dr. Brian Payne, ODU, leads the Coastal Virginia Node; Dr. Gretchen Matthews, VT, leads the Southwest Virginia Node; and Dr. Erdem Topsakal, VCU, leads the Central Virginia Node.

An international search for the inaugural Executive Director for CCI was conducted in 2019: Luiz DaSilva joined CCI as its Executive Director on March 16, 2020. He was also appointed the Bradley Professor of Cybersecurity at Virginia Tech. Dr. DaSilva was a professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech from 1998 to 2014, and a faculty member at Trinity College Dublin from 2009 to 2020, where he served as the Director of CONNECT, a national research center in Ireland, funded by the Science Foundation Ireland.

On June 24, 2020, John Delaney, formerly the Chief of Staff for the U.S. Army Cyber Command, joined CCI as its first permanent Managing Director.

The CCI Executive Director, Managing Director, and the four Node Directors form the CCI Leadership Council (LC), depicted in Figure 1.5. The CCI network today includes 39 institutions of higher learning across Virginia, depicted in Figure 1.6.

(a) Dr. Luiz DaSilva, Executive Director.

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

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

(d) Dr. Erdem Topsakal, Central Virginia (CeVA) Node Director.

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

(f) Mr. John Delaney, Managing Director.

Figure 1.5: CCI Leadership Council.

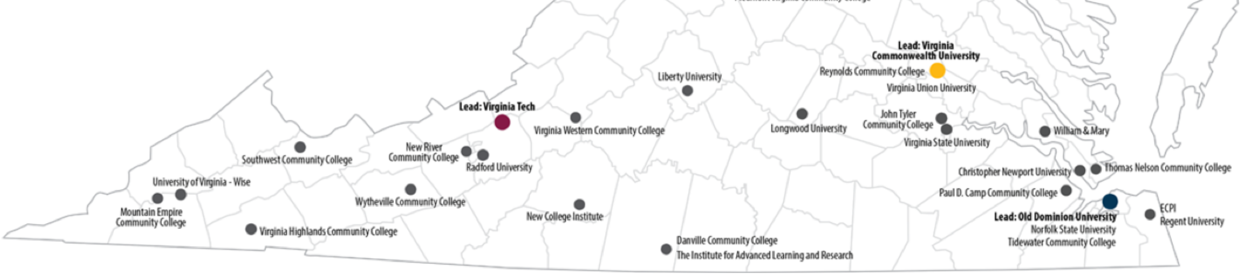

Shenandoah University
Marymount University
George Washington University
Lord Fairfax Community College
Lead: George Mason University
Northern Virginia Community College
James Madison University
Germanna Community College
University of Mary Washington
University of Virginia
Piedmont Virginia Community College
Lead: Virginia Commonwealth University
Reynolds Community College
Virginia Union University
Liberty University
Lead: Virginia Tech
Virginia Western Community College
Longwood University
John Tyler Community College
Virginia State University
William & Mary
Southwest Community College
New River Community College
Radford University
Christopher Newport University
Thomas Nelson Community College
University of Virginia - Wise
Wytheville Community College
Paul D. Camp Community College
Mountain Empire Community College
New College Institute
Lead: Old Dominion University
Norfolk State University
Tidewater Community College
ECPI
Regent University
Virginia Highlands Community College
Danville Community College
The Institute for Advanced Learning and Research

Figure 1.6: The CCI network.

Chapter 2

Hub and Regional Node Reports

This chapter describes the progress and achievements of the CCI Hub and four Regional Nodes throughout FY20. The seven reporting requirements specified in item 135, Chapter 1289, HB30, are explicitly addressed in Sections 2.1 to 2.5. These reporting requirements include:

- External grants attracted to support the work of CCI;
- 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.

Finally, in Section 2.6, a list of media hits from December, 2019 to September, 2020, is provided. These media stories highlight some of the more visible accomplishments of the CCI network in the past year.

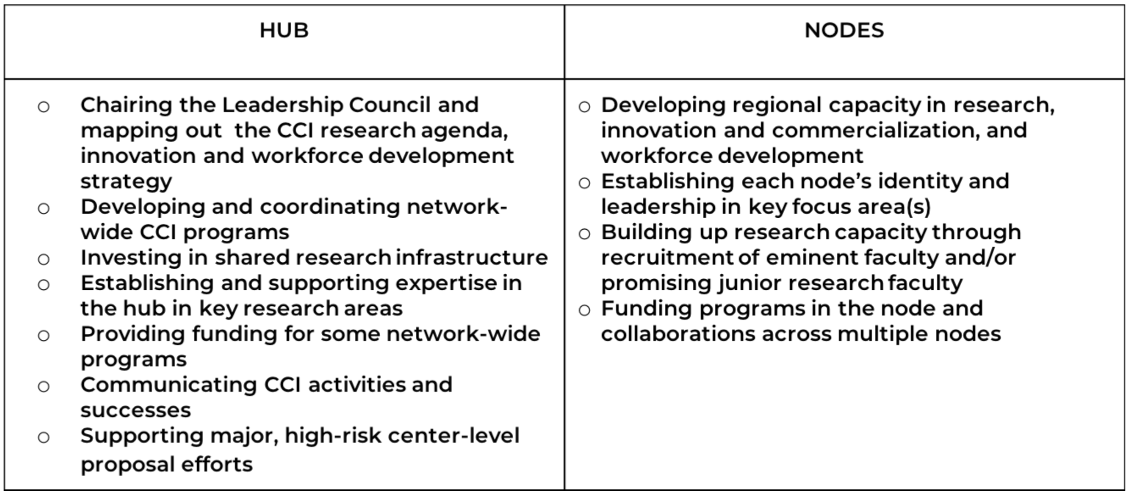
2.1 CCI Hub

2.1.1 Role of the Hub

The CCI Hub chairs the Leadership Council (LC) and is responsible for articulating the research agenda, and the innovation and workforce development strategy for the network. The Hub also designs, coordinates, and funds some network-wide programs. The Hub deploys key research infrastructure available to all CCI researchers, such as the 5G and AI Assurance testbeds. The Hub also houses faculty and graduate students with established expertise in key research areas in cybersecurity, autonomous systems, and data. 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 main roles of the Hub and the Nodes are summarized in Figure 2.1.

The CCI Hub has a lean administrative structure: the operations and research team are shown in the organization chart in Figure 2.2. Key personnel, including the Executive Director and Managing Director, were recruited in FY20, with additional leadership positions such as the Communications and Marketing Director and 5G Testbed Director being filled in FY21.

Affiliated Faculty are faculty attached to an academic department (Statistics, Electrical and Computer Engineering, Computer Science) conducting research in the CCI Hub. At present, there are eight Hub faculty members, five of whom are Institute of Electrical and Electronic Engineers (IEEE) Fellows (Figure 2.3). Their areas of expertise are:



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 2.1: Roles of the CCI Hub and Nodes.

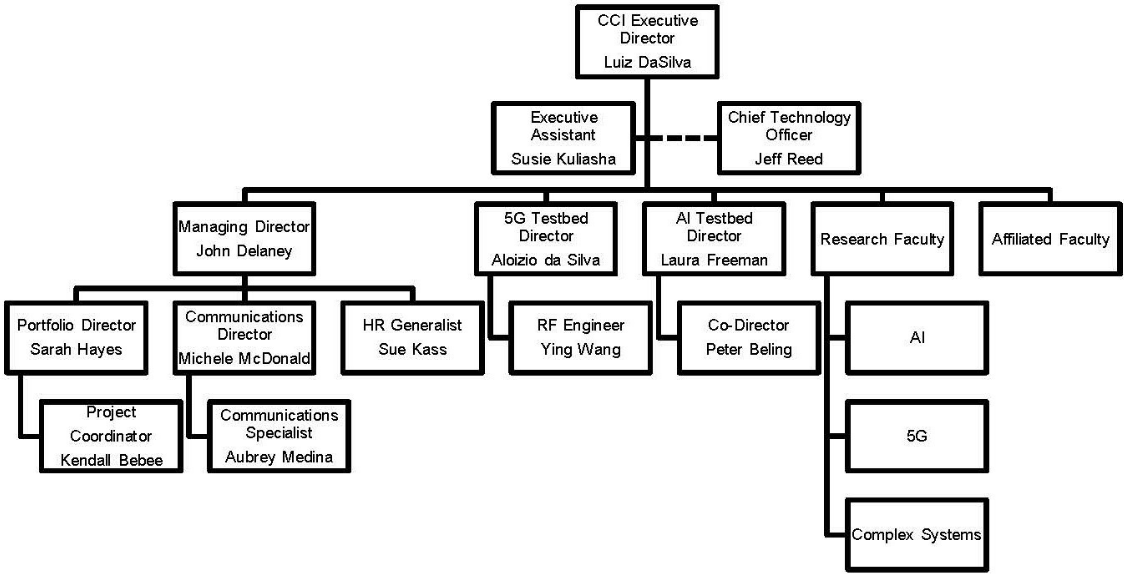


Figure 2.2: CCI organization chart.

- Tam Chantem: cyber-security for real-time Cyber Physical System (CPS);
- Luiz DaSilva: wireless networks, Unmanned Autonomous Vehicle (UAV) connectivity, 5G reliability;
- Laura Freeman: trustworthy AI;
- Ryan Gerdes: cyber-bio, resilience of the agro-industry to cyber attacks;
- Wenjing Lou: information and network security, autonomous vehicle security;
- Jerry Park: 5G and protocol security;
- Jeff Reed: spectrum, 5G, software-defined radio; and
- Haining Wang: e-commerce security, power system security.

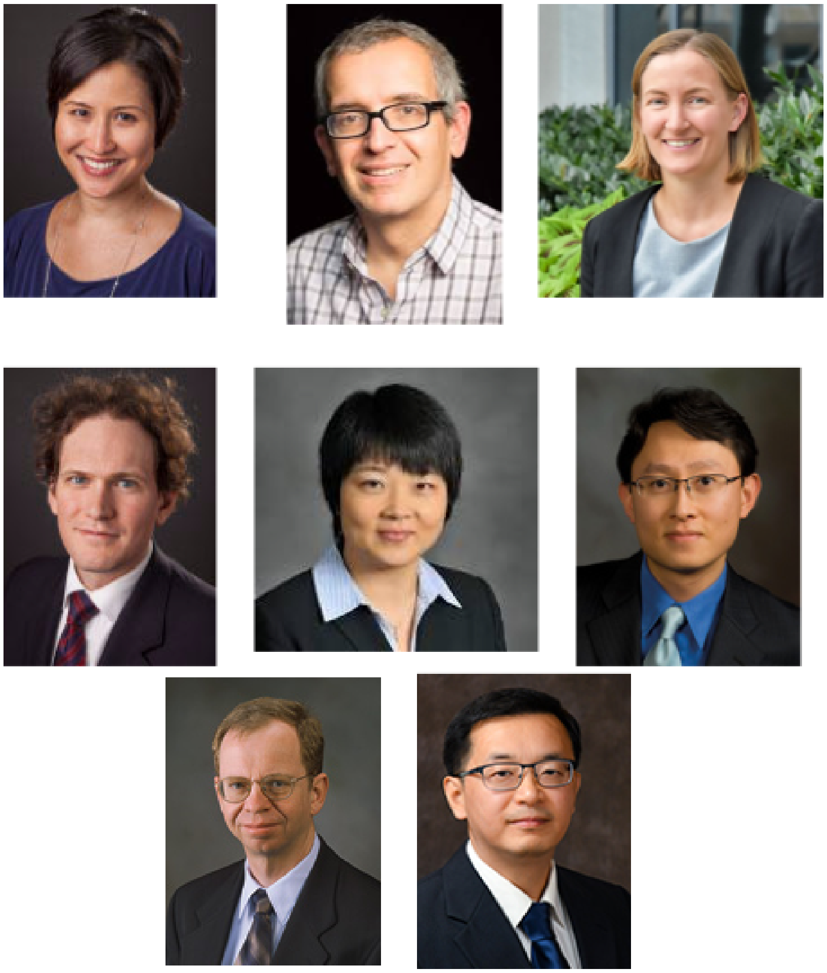


Figure 2.3: Hub faculty. From top left: Tam Chantem, Luiz DaSilva, Laura Freeman, Ryan Gerdes, Wenjing Lou, Jerry Park, Jeffrey Reed, and Haining Wang.

2.1.2 Report on the Seven Requirements as per Item 135, Chapter 1289, HB30

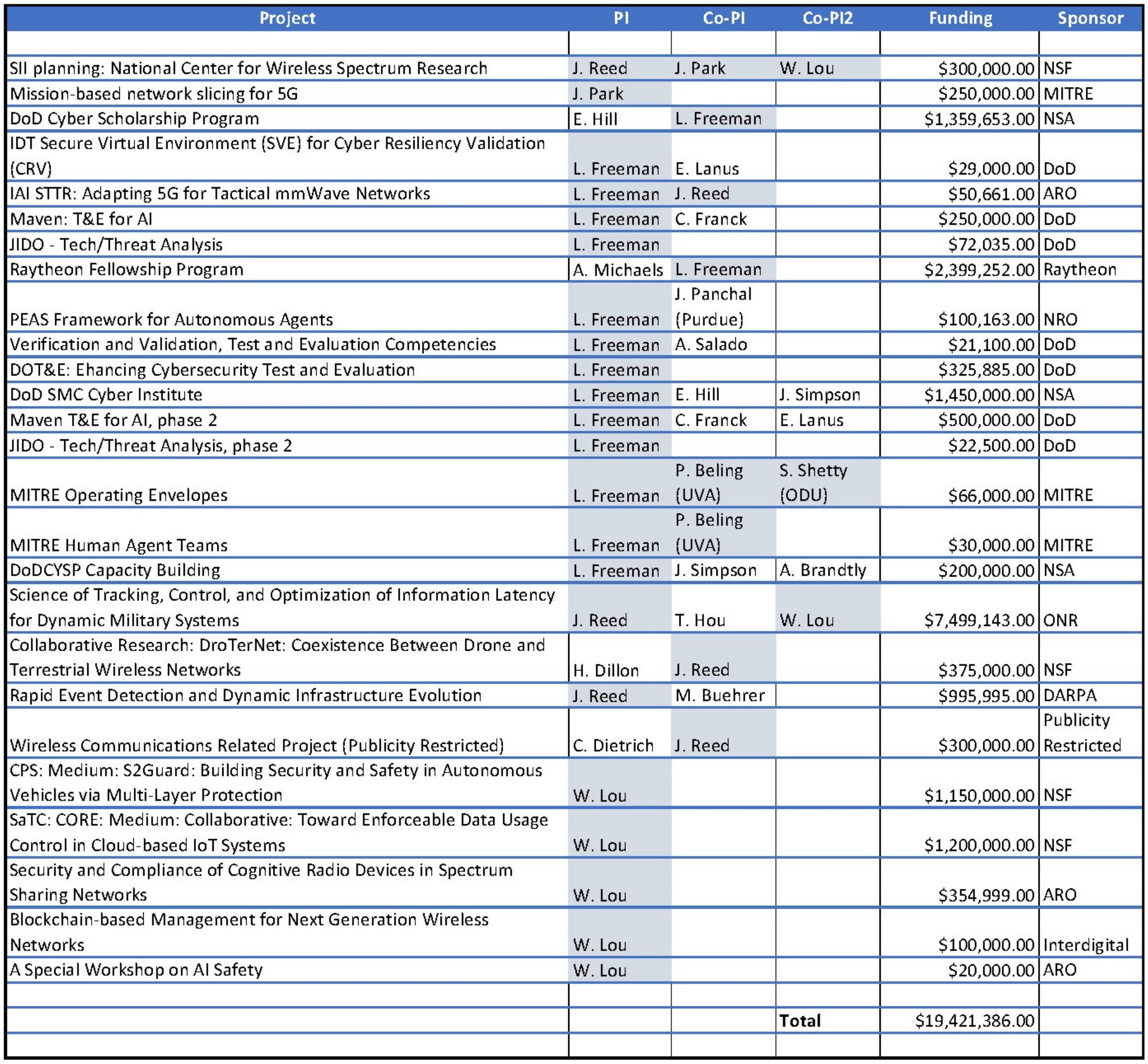
External Research Grants attracted to support the work of CCI

Leveraging the investment by the Commonwealth

CCI Hub faculty brought in $19.4M in external funding for projects starting in FY20. This represents a 2-to-1 return on the investment made by the Commonwealth, in terms of research funding alone, in the first year of CCI.

One key promise of CCI is that the investment that the Commonwealth is making in the initiative will be leveraged to increase the competitiveness of CCI in attracting additional research funding. We can already show clear results: in FY20, CCI Hub faculty attracted a total of $19.4M in external research funding. From this total, 85% comes from the federal government, reflecting the strong investments being made in the CCI focus areas of cybersecurity, autonomous systems, and data. Figure 2.4 shows the projects funded with starting dates in FY20, the CCI Hub faculty members involved, and the funding agency. The following federal agencies currently fund research in the CCI Hub: National Science Foundation (NSF), National Security Agency (NSA), Department of Defense (DoD), Army Research Office (ARO), National Reconnaissance Office (NRO), Office of Naval Research (ONR), and Defense Advanced Research Projects

Agency (DARPA). Other organizations funding this work include Raytheon, MITRE, and Interdigital.



Project	PI	Co-PI	Co-PI2	Funding	Sponsor
SII planning: National Center for Wireless Spectrum Research	J. Reed	J. Park	W. Lou	$300,000.00	NSF
Mission-based network slicing for 5G	J. Park			$250,000.00	MITRE
DoD Cyber Scholarship Program	E. Hill	L. Freeman		$1,359,653.00	NSA
IDT Secure Virtual Environment (SVE) for Cyber Resiliency Validation (CRV)	L. Freeman	E. Lanus		$29,000.00	DoD
IAI STTR: Adapting 5G for Tactical mmWave Networks	L. Freeman	J. Reed		$50,661.00	ARO
Maven: T&E for AI	L. Freeman	C. Franck		$250,000.00	DoD
JIDO - Tech/Threat Analysis	L. Freeman			$72,035.00	DoD
Raytheon Fellowship Program	A. Michaels	L. Freeman		$2,399,252.00	Raytheon
PEAS Framework for Autonomous Agents	L. Freeman	J. Panchal (Purdue)		$100,163.00	NRO
Verification and Validation, Test and Evaluation Competencies	L. Freeman	A. Salado		$21,100.00	DoD
DOT&E: Ehancing Cybersecurity Test and Evaluation	L. Freeman			$325,885.00	DoD
DoD SMC Cyber Institute	L. Freeman	E. Hill	J. Simpson	$1,450,000.00	NSA
Maven T&E for AI, phase 2	L. Freeman	C. Franck	E. Lanus	$500,000.00	DoD
JIDO - Tech/Threat Analysis, phase 2	L. Freeman			$22,500.00	DoD
MITRE Operating Envelopes	L. Freeman	P. Beling (UVA)	S. Shetty (ODU)	$66,000.00	MITRE
MITRE Human Agent Teams	L. Freeman	P. Beling (UVA)		$30,000.00	MITRE
DoDCYSP Capacity Building	L. Freeman	J. Simpson	A. Brandtly	$200,000.00	NSA
Science of Tracking, Control, and Optimization of Information Latency for Dynamic Military Systems	J. Reed	T. Hou	W. Lou	$7,499,143.00	ONR
Collaborative Research: DroTerNet: Coexistence Between Drone and Terrestrial Wireless Networks	H. Dillon	J. Reed		$375,000.00	NSF
Rapid Event Detection and Dynamic Infrastructure Evolution	J. Reed	M. Buehrer		$995,995.00	DARPA
Wireless Communications Related Project (Publicity Restricted)	C. Dietrich	J. Reed		$300,000.00	Publicity Restricted
CPS: Medium: S2Guard: Building Security and Safety in Autonomous Vehicles via Multi-Layer Protection	W. Lou			$1,150,000.00	NSF
SaTC: CORE: Medium: Collaborative: Toward Enforceable Data Usage Control in Cloud-based IoT Systems	W. Lou			$1,200,000.00	NSF
Security and Compliance of Cognitive Radio Devices in Spectrum Sharing Networks	W. Lou			$354,999.00	ARO
Blockchain-based Management for Next Generation Wireless Networks	W. Lou			$100,000.00	Interdigital
A Special Workshop on AI Safety	W. Lou			$20,000.00	ARO
			Total	$19,421,386.00	

Figure 2.4: External funding attracted by CCI Hub faculty (highlighted cells) in FY20.

The CCI Hub is also funding nine CCI fellows across the network, as discussed in the next subsection. Their involvement in CCI enhances their competitiveness to attract external funding. Of particular note is a recent award to Dr. Kai Zeng, a CCI fellow at GMU: through Dr. Zeng, GMU was awarded $1.6M from the DARPA 5G-OPS program for the project 'EPIC SWaPD: Energy-Preserving IoT Cryptography for Small Weight and Power Devices,' with period of performance from 2020 to 2024.

Research Grants awarded from the funds contained in HB30

CCI Hub funds have provided seed funding for the Hub faculty in Figure 2.3; approximately $1M was allocated to directly fund this research. Some of the projects that are being carried out with this seed funding are highlighted in this subsection. An additional allocation of $450K was made by the CCI Hub to fund the research of CCI Fellows, faculty in member institutions who collaborate closely with the CCI leadership and Hub faculty. The CCI Fellows program is also discussed in this section.

Securing machine learning and blockchain consensus protocols

Dr. Wenjing Lou is making machine learning more robust against attacks and securing blockchain-based spectrum management.

Dr. Wenjing Lou is an internationally recognized researcher in system security. In the past year, her group has been working on multiple research topics, including: IoT security; security and safety in autonomous vehicles; security of blockchain networks; data usage control through blockchain, smart contract, and trust execution environment; and security and privacy in machine learning-based systems.

Complementing multiple externally funded research projects, CCI funds provide the group with additional resources to leverage the existing research and to invest in exploring new research domains. In particular, the new research problems pursued with CCI seed funding fall in the following two areas:

1. Robust machine learning against adversarial security and privacy attacks: Dr. Lou's group has thoroughly studied the impact of various security and privacy attacks (e.g., data poisoning, disclosure, inference, evasion, model inversion, and backdoor attacks) to machine learning-based systems. They are currently developing robust machine learning methods that incorporate differential privacy into meta-learning methods to provide both theoretical privacy guarantees and more robust anomaly detection, particularly in detecting data samples that do not fit the distribution, such as outliers within the dataset and new samples, and for scenarios in which only a very small number of data examples are available to individual learners.

2. Security of blockchain consensus protocols and blockchain-based wireless spectrum management: Per Federal Communications Commission (FCC) guidance, for licensed commercial spectrum bands (e.g., Television White Spaces (TVWS) and Citizens Broadband Radio Service (CBRS)), unlicensed users are allowed to access the spectrum of incumbent users according to the latter's usage rules. For unlicensed spectrum bands (e.g., the 6 GHz band), all users will share the spectrum in a more flexible manner; a set of common rules will help avoid excessive collisions and provide better Quality of Service (QoS). For both scenarios, due to the heterogeneity of spectrum demand across regions, a complex hierarchy of trusted entities (e.g., the Spectrum Access System (SAS) in CBRS) are needed to enforce such spectrum rules globally. Blockchain can provide an alternative rule-abiding spectrum access framework without the need for central trusted entities. All spectrum users may operate a blockchain node and participate in the consensus process. The rules can be encoded in the consensus protocol or in the form of a blockchain smart contract. The security of rule enforcement and record keeping is provided by the honest majority of consensus participants. Dr. Lou is currently developing a novel spectrum management system that harnesses blockchain technology for the access control and usage record keeping. The system architecture and functionalities are illustrated in Figure 2.5. This research is at the very beginning phase and the team has received a research gift from InterDigital for this research.

Curbing the practice of incentivized reviews in e-commerce

Dr. Haining Wang's research team has devised a graph-based method to detect incentivized review groups, a practice that can lead to biased and fake reviews. He was able to show the effectiveness of the method on an extensive Amazon review dataset.

Online reviews play a crucial role in the current business ecosystem. To manipulate consumers' opinions, some sellers of e-commerce platforms outsource opinion spamming with incentives (e.g., free products) in exchange for incentivized reviews. These incentives, by nature, are likely to drive more biased reviews or even fake reviews. The process is illustrated in Figure 2.6.

Despite e-commerce platforms such as Amazon having taken initiatives to squash the incentivized review practice, sellers turn to various social networking platforms such as Facebook to outsource the incentivized reviews. The aggregation of sellers who request incentivized reviews and reviewers who seek incentives forms incentivized review groups.

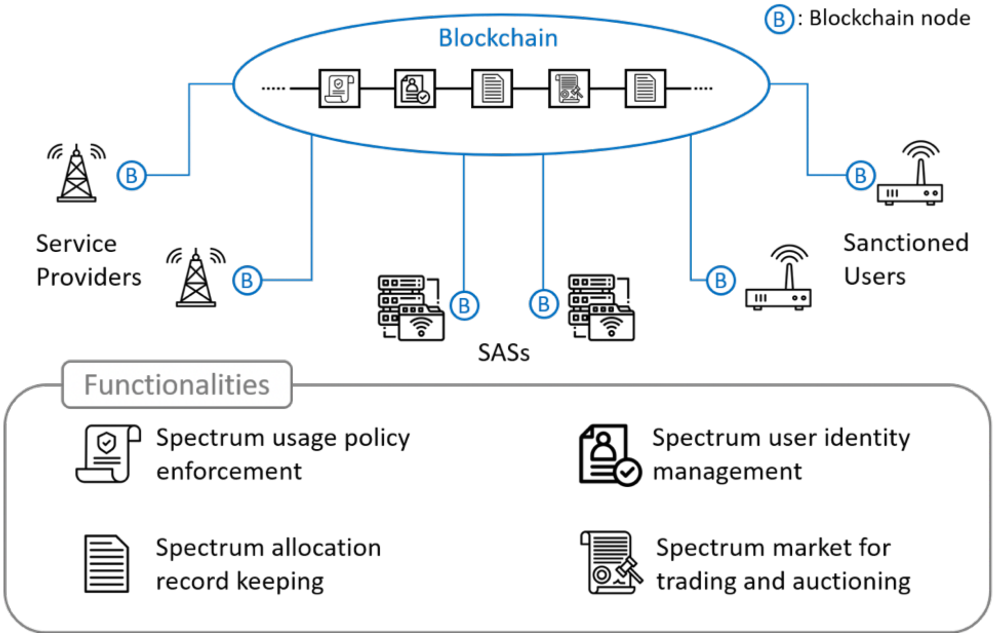

B: Blockchain node
Blockchain
Service Providers
SASs
Sanctioned Users
Functionalities
Spectrum usage policy enforcement
Spectrum user identity management
Spectrum allocation record keeping
Spectrum market for trading and auctioning

Figure 2.5: System architecture and functionalities of the proposed blockchain-based spectrum management.

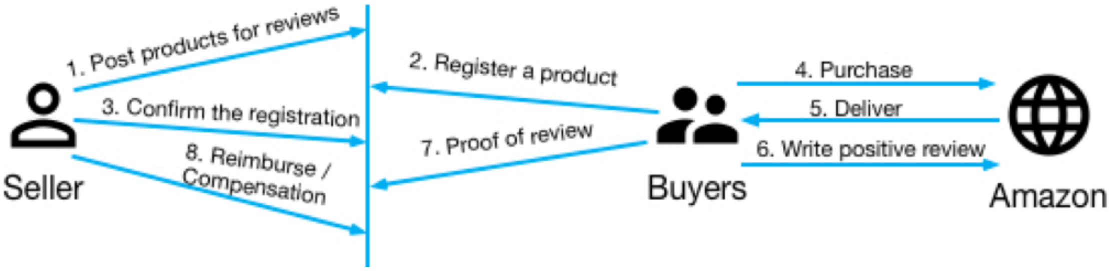


Figure 2.6: Amazon incentivized review group.

Dr. Wang's research focuses on incentivized review groups on e-commerce platforms such as Amazon. To understand the breadth of the problem, his team investigates incentivized review groups across several different platforms, including Facebook, WeChat, and Douban. With the data collected from different platforms, Dr. Wang integrates the data from different data sources and examines incentivized review groups. He has found that different platforms play different roles in the ecosystem of incentivized review groups. Specifically, incentivized review groups on Facebook act like blackboards, where a set of merchants post their products directly in these Facebook groups. Meanwhile, incentivized review groups on Douban are of service for merchants and brokers, which educate them how to effectively obtain incentivized reviews; and incentivized review groups on WeChat are mostly private and generally are owned by a single person, who recruits reviewers to join the group and posts review requests for a set of products.

To understand the incentivized review groups, Dr. Wang has conducted a measurement study to characterize real review groups from different aspects. He investigates the number and the increment rate of review members, as well as the number of merchants in collected incentivized review groups. In terms of incentivized review requests, Dr. Wang's team inspects the incentivized review requests in different groups as well as from individual merchants. They also examine the categories, questions and answers, and the relationship between sellers and manufacturers of products.

Based on the measurement study, Dr. Wang has proposed a graph-based method to detect incentivized review groups on Amazon. The novelty of this detection method lies in leveraging the co-review behavior among reviewers. Co-review means two reviewers post reviews on the same product. To this end, Dr.

Wang first constructs co-review graphs of reviewers and then employs the community detection method to find suspicious communities. Specifically, he not only considers the frequency of co-reviews, but also uses important features of the co-review behavior, such as co-reviews in a burst. A burst of favorable reviews of a product could imply the existence of incentivized reviews. Therefore, the solution leverages bursts of favorable reviews to improve the detection accuracy of incentivized review groups. The detection of incentivized review groups can be further integrated into the existing spam review detection framework to improve its coverage and effectiveness.

To evaluate his detection method, Dr. Wang constructed a “gold standard” dataset from the data collection. The “gold standard” dataset is guaranteed by using the collection of real incentivized review groups, which enables the research team to validate the effectiveness of their method and even shed light on further fake review research. They also examined an extensive Amazon review dataset ranging from 1996 to 2018 and found that incentivized review groups posed little threat on the ecosystem before 2014 but became a critical issue after 2014.

Developing the building blocks for an assurance program that will allow AI to be adopted in the defense and national security communities

Dr. Laura Freeman’s team works on making AI trustworthy, from model selection to robust parameterization, using AI for human-agent team evaluation and to enhance cybersecurity testing.

In addition to leading research under the AI Assurance thrust of CCI, Dr. Laura Freeman is a Research Associate Professor in the Department of Statistics and the Director of the Intelligent Systems Lab at the Virginia Tech Hume Center. Her research leverages experimental methods for conducting research that brings together CPS, data science, AI, and machine learning to address critical challenges in national security. A focus is developing new methods for test and evaluation focusing on emerging system technology focusing on new methods in machine learning and AI. She is also the Assistant Dean for Research in the National Capital Region, and in that capacity she works to shape research directions and collaborations in across the College of Science in the National Capital Region.

Dr. Freeman’s current research projects span a broad range of AI assurance topics. They focus on developing the building blocks for an assurance program that will allow AI to be adopted in the defense and national security community. Her projects bring an interdisciplinary approach to concepts of AI Assurance and include faculty collaborators from electrical and computer engineering, computer science, psychology, industrial systems engineering, aerospace engineering, and statistics. A short summary of these programs:

- Certifying operating envelopes for machine learning and AI. This project seeks to identify data and model-agnostic approaches to learning about a models operating environment (where a model is expected to work) and make risk-based decisions on using models in new environments.
- Model selection based on available data. This research takes a structure approach to making model use recommendations based on the quantity and balance of training/testing data available.
- Experimental approaches to developing robust parameterizations of natural language processing models. The goal of the system that this research supports is to identify areas of emerging technology and threats based on publication, patent, and other curated data sources. The research focuses on developing robust implementations to ensure that a diverse user base will develop successful queries on the system.
- Assessing the effectiveness of human agent teams via new metrics and structured experiments. This project seeks to develop new metrics in trust, cooperation, collaboration, and mutual learning coupled with existing mission and task based criteria. Ultimately, the goal of the new metrics is to identify optimal team configurations for a given set of tasks via simulation study.
- Enhancing cybersecurity test and evaluation via automated data collection, synthetic data generation, algorithmic based approaches, and machine learning. The goal of this project is to develop fundamental capabilities to support red team cyber support software tool. The goal of the tools is to expand the capacity of limited human resources in DoD red team testing.

- Developing strategies for verification and validation of a virtual cyber environment enabling the measurement cybersecurity attack effectiveness on a virtualized system without risk to actual systems or networks.

Ensuring security and privacy in V2X and M2M communications

With seed funding from CCI, Dr. Jerry Park is establishing a program focusing on security and privacy in 5G systems and beyond, with key application areas including vehicular communications, smart homes, and smart cities.

A significant shift in cellular technology is currently underway as wireless service providers around the world are pitted against each other in a heated race to be the first to deploy and operate fifth-generation cellular networks, better known as 5G. As illustrated in Figure 2.7, 5G technology is expected to usher in a plethora of new technologies and applications, including smart cities and factories, IoT, drone-based communications, and Vehicle-to-everything (V2X) communications. The successful implementation and deployment of the 5G applications will be possible only if we are able to address the difficult security and privacy challenges that remain unaddressed.

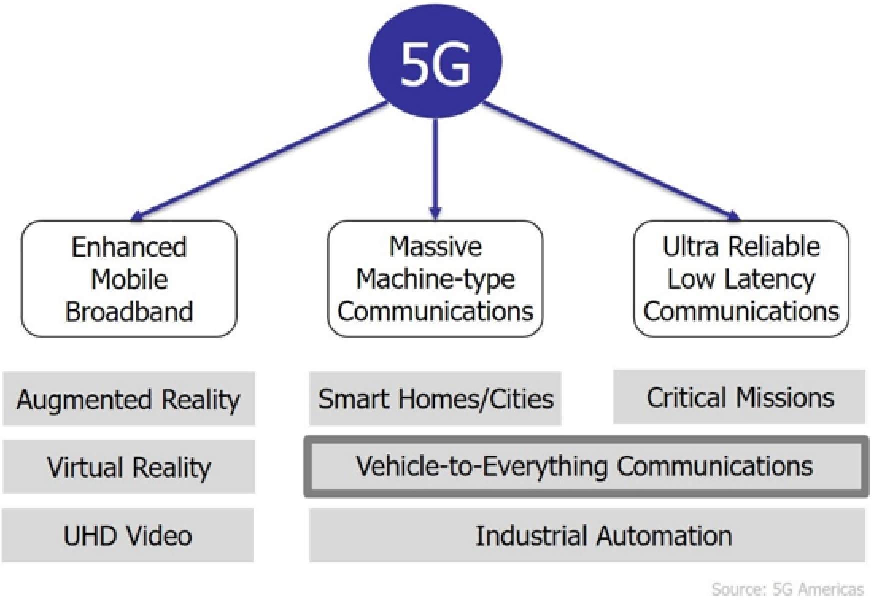

5G
Enhanced Mobile Broadband
Massive Machine-type Communications
Ultra Reliable Low Latency Communications
Augmented Reality
Virtual Reality
UHD Video
Smart Homes/Cities
Critical Missions
Vehicle-to-Everything Communications
Industrial Automation
Source: 5G Americas

Figure 2.7: Application domains enabled by 5G [Source: 5G Americas].

Using seed funding from CCI, Dr Park recently established a research program that focuses on the security and privacy challenges in 5G and beyond. His research team is focusing on security and privacy problems in the application domains identified in Figure 2.7, with a particular focus on V2X communications and networking and Machine-to-machine (M2M) communications that enable smart homes and smart factories. This research program will promote close collaboration between CCI researchers to develop novel algorithms and protocols; carry out comprehensive evaluations of today's and emerging wireless standards; perform large-scale simulations; implement prototypes; and carry out experiments on testbeds.

This program will utilize the CCI 5G security testbed, which is currently under construction, and will provide the 'research layer' that is needed to research and develop technically rigorous and commercially viable security solutions.

The research thrusts that constitute the research program include:

1. Security and privacy for V2X communications and networking: Automotive Intelligent Transportation System (ITS) applications based on Vehicle-to-vehicle (V2V), Vehicle-to-infrastructure (V2I), Vehicle-to-network (V2N), and Vehicle-to-pedestrian (V2P) communications – collectively referred to as V2X –

constitute one of the most important application domains that 5G is envisioned to support. Given the safety requirements of most V2X applications, ensuring security and privacy for V2X communications is critical. The focus will be on challenging problems that relate to message confidentiality, entity authentication, message integrity, and user's privacy. The the existing V2X technology, viz., Cellular Vehicle-to-everything (CV2X) based on 3rd Generation Partnership Project (3GPP) Rel. 14 will be studied, as well as emerging technologies, viz., 5G New Radio (NR) V2X based on 3GPP Rel. 16 and beyond.

2. Security for M2M communications and IoT: Massive M2M communications and IoT enables wearable devices, smart home appliances, industrial control devices and other smart devices/sensors to share and communicate information via 5G networks. The connectivity between these smart devices is one of the core underpinnings of smart cities, smart homes, and smart factories. Given the sensitivity and the privacy implications of some of the information exchanged between smart devices, it becomes obvious why ensuring security and privacy for M2M and IoT applications is important. Since IoT devices are often battery-powered and constrained in terms of computational/communications capabilities, the focus will be on lightweight solutions that do not pose a burden on the capabilities of the devices.

3. Security and privacy for network slicing: Network slicing is one of the key technologies that enable 5G networks to offer dedicated resources to different types of services, applications, and even industries. However, cyberattacks that exploit the vulnerabilities of network slicing could severely impact the performance and availability of the slices, or violate the confidentiality and integrity of the information carried on those slices. Network slicing is especially vulnerable to Denial of Service (DoS) attacks, as a large number of services and applications share the same physical resources in a multi-tenant virtualized networking infrastructure. Preserving user privacy is also an important requirement since slice isolation is an essential requirement for 5G network slicing. The security and privacy vulnerabilities of network slicing will be studied, and pragmatic security solutions will be developed.

4. Pre-authentication message exploits in 5G networks: In the current 5G specifications, the User Equipments (UEs) and the Next generation NodeB (gNB) may need to exchange messages in the clear before a cryptographic handshake has taken place. Prior research has shown this is the root cause of many known protocol exploits. A study is planned that will focus on the challenge of securely handling pre-authentication messages and other protocol exploits.

5. Public Key Infrastructure (PKI) infrastructure and key management for 5G: One pragmatic approach for addressing pre-authentication message exploits and other protocol exploits is to adopt a PKI-based architecture in 5G. A PKI would provide a scalable approach for addressing some of the known protocol exploits. However, instead of using public keys burned into the Universal Subscriber Identification Module (USIM) – as prescribed in the current 5G standard – a more flexible approach is needed. One such approach is to adopt a global hierarchy of 5G certificate authorities that is integrated into a corresponding PKI. The technical challenges related to this approach will be investigated.

Protecting the security of Real Time Cyber Physical Systems

Dr. Tam Chantem's group is using CCI seed funding to protect CPSs with real time requirement, and to achieve data protection through software anti-tamper.

Many CPSs have Real Time (RT) requirements. For these RT-CPS, such as a network of UAVs that deliver packages to customers' homes or a robot that performs/aids in cardiac surgery, deadline misses may result in economic losses or even have fatal consequences. At the same time, as these RT-CPS interact with, and are depended on by, humans, they must also be trustworthy.

The first research thrust of Dr. Chantem's team is in balancing predictability and security in RT-CPS design. A key research goal is to design secure RT-CPS that are less complex, easier to analyze, and reliable for critical application domains such as defense, medicine, transportation, manufacturing, and agriculture, to name just a few. Since RT-CPSs now permeate most aspects of daily life, especially in the smart city and IoT context, this research will improve confidence in automated systems by users, thereby increasing appetite for automation, which will help to stimulate the economy and create jobs. This goal will be accomplished by: (i) securing the scheduling infrastructure from the ground up, (ii) using a formal framework for trading off security against timeliness while accounting for system dynamics, and for the cost of security to be explicitly quantified, and (iii) performing state- and function-dependent on-demand recovery. Said RT-CPS will be able to proactively prevent attacks using moving target defense, as well as detect and recover from attacks that cannot be avoided. This research will pave the way for RT-CPS and IoT to be implemented with confidence, their timely and correct operation guaranteed. Specific contributions of this research, as shown in Figure 2.8, are: (i) a trusted scheduling infrastructure that can protect the integrity of the real-time tasks, the scheduler, its task queues, and I/O, and which can recover from (intentional) errors, (ii) a probabilistic real-time/security co-design framework that exploits trusted execution to protect the security of the real-time tasks, (iii) novel schedulability analysis techniques, (iv) an incremental recovery mechanism for continuous operation, and (v) validation on automated ground vehicles, drones, and robot arms. Contributions expanding the knowledge base will be made to the fields of CPS, IoT, real-time systems, security, and control systems.

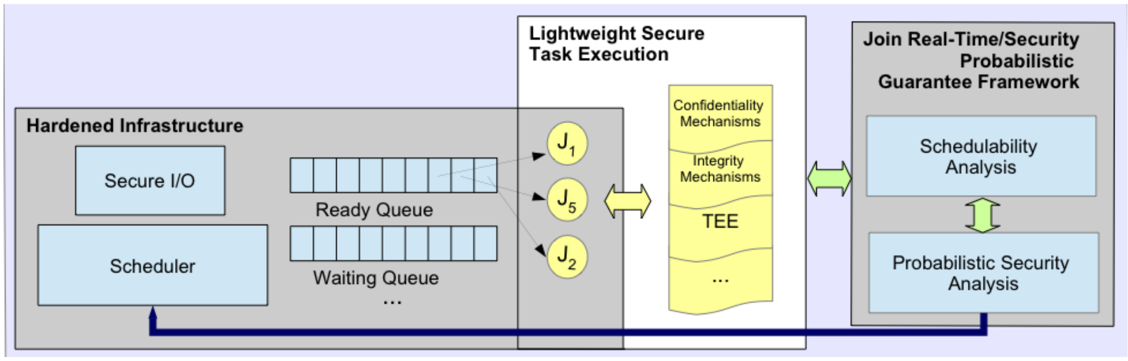

Lightweight Secure Task Execution
Join Real-Time/Security Probabilistic Guarantee Framework
Hardened Infrastructure
Secure I/O
Ready Queue
Scheduler
Waiting Queue
...
J_1
J_5
J_2
Confidentiality Mechanisms
Integrity Mechanisms
TEE
...
Schedulability Analysis
Probabilistic Security Analysis

Figure 2.8: Overview of our system. The scheduler, various queues, and I/O, collectively referred to as the scheduling infrastructure, will be hardened using a combination of security mechanisms to achieve a trusted, yet lightweight foundation. The real-time jobs will execute on top of this trusted infrastructure, with appropriate security mechanisms added on a job-by-job basis based on system state and threat level (reactive security), as determined by the joint real-time/security probabilistic guarantee framework. Said framework also performs proactive moving target defense by judiciously adding extra security mechanisms for a given job subject to probabilistic deadline guarantees.

The second research thrust of Dr. Chantem's research team is on data protection through software anti-tamper. To further secure RT-CPS, the team will identify portions of source code that are sight- or modification-sensitive. Prototype compilers that are compatible with trusted execution environments have been developed that are able to take these annotations and map them into binary objects that are either "secure" or "nonsecure." Middleware was developed that is able to lay code out on heterogeneous processors and automatically schedule code for execution in trusted execution environments, such as the ARM TrustZone. These techniques demonstrated the ability to create effective code partitions and scheduling algorithms were able to improve code execution performance, thus reducing the overhead associated with size, weight, and power needed for Critical Program Information (CPI) protection. The goal will be to (i) develop automated program analysis and transformation techniques for use by application programmers for engineering Trusted Executed Environment (TEE)-based applications, as current program analysis and automated transformations cannot be applied to help developers in engineering TEE-based applications, (ii) facilitate and enrich TEE-related programming experience by creating a new programming model that treats TEE as a server that deploys sensitive functions as secure services, (iii) secure the fundamental components that are critical to the correct and timely operation of mission-critical, resource-constrained systems in order to provide a sanitized platform for CPI protection, (iv) assess the dynamic attack surface of Software Guard Extensions (SGX)-based encapsulation against security vulnerabilities both inside and outside enclave code, (v) assess and improve the performance and scaling of SGX-based encapsulation with a special emphasis on the number of distinct classes and boot-up latency, and expand support for additional trusted processors/platforms.

The CCI Fellows

The CCI Hub has dedicated $450K in FY20 Hub funds to fund nine CCI Fellows who interact closely with Hub faculty and the CCI leadership to build collaborations across the entire network.

In the second half of 2019, a call was issued for interest for the CCI Fellows program. As a representative of CCI, fellows must:

- Actively contribute to the research mission of CCI and to demonstrate its impact on the Commonwealth of Virginia, in terms of workforce development, innovation, industry partnerships, and/or additional funding from other sources;
- Participate in monthly Fellows meetings;
- Participate in meetings, workshops, symposia, or other CCI activities, as appropriate;
- Participate in strategic planning activities at Node and Network levels;
- Participate in developing collaborative research proposals, as appropriate.

The Fellows were selected competitively by the LC, and started engaging directly in CCI activities in FY20. Each fellow received $50K in funding in FY20, with the possibility of renewal for one year in FY21. The fellows represent a cross-section of the expertise of relevance to CCI and come from all four regions in the Commonwealth. The first class of CCI fellows is depicted in Figure 2.9.

The work of the CCI fellows is described here, as well as under the headings of entrepreneurship and workforce programming, and collaborative partnerships.

CCI fellow develops secure connectivity for autonomous vehicles

Dr. Duminda Wijesekera, a faculty member at GMU, is building an in-lab, in-field experimental system to investigate the viability of automated driving systems.

Dr. Duminda Wijesekera is a CCI fellow from GMU and he is leading a team of researchers from the Radar and Radio Engineering (RARE) lab on the future of autonomous vehicles.

Significant advances in research, development and prototyping of automated and connected vehicles have been advocated and encouraged for inclusion in autonomous vehicle communications by the National Highway Traffic Safety Administration (NHTSA) and the Society of Automotive Engineers (SAE). These efforts describe six levels of vehicular automation, ranging from level 0 (no automation) through level 5 (full automation). To assure autonomous vehicles of levels 3 and above operate safely together on the road, information is exchanged between these vehicles detailing their respective views of their state and operating environment.

In addition, roadside units also transmit timely information to support operation of the autonomous and semi-autonomous vehicles. Examples of this information include weather and road conditions, surrounding vehicles and their trajectories, and potential road obstructions such as stalled and disabled vehicles, and other road debris that may result in operational hazards. NHTSA says that Automated Driving Systems (ADSs), including those contemplating no driver at all, have the potential to significantly improve roadway safety in the United States.

Dr. Wijesekera's team is building an in-lab, in-field experimental system to investigate the viability of these proposals and their safety and cyber security implications under realistic conditions. There are a number of open research problems introduced by autonomous vehicle communications which their research addresses. Some of these problems are articulated below:

- Does the CV2X system have sufficient capacity within operating environments under varying conditions to transmit and receive information? The CCI NoVA Node provides a particularly robust test environment to explore the full realm of possible conditions, i.e. urban, suburban, rural, highway, varying landscape, field of view, congestion.

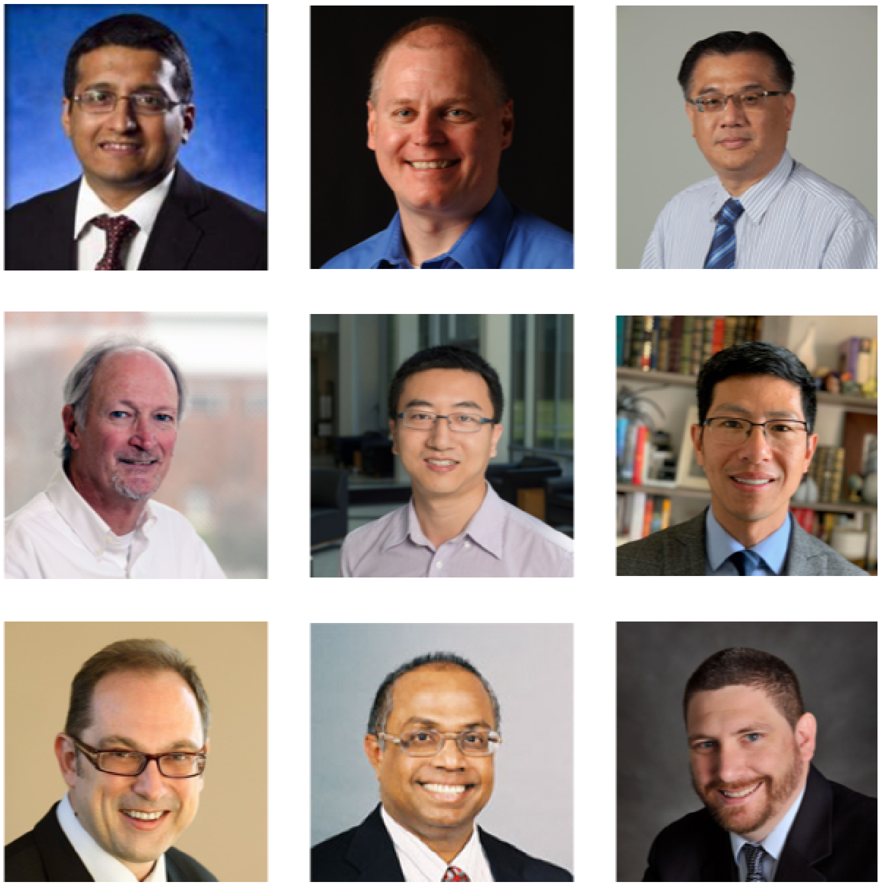


Figure 2.9: CCI fellows. From top left: Sachin Shetty (ODU), Jeff Pittges (Radford University), Frank Hu (NSU), Jack Davidson (UVA), Kai Zeng (GMU), Hongyi Wu (ODU), Milos Manic (VCU), Duminda Wijesekera (GMU), and Kevin Heaslip (VT).

- What are the related security and safety concerns and limitations in CV2X systems and possible mitigations for these issues?
- What cellular capacities are required in different areas with physical obstructions to transmission (big buildings vs. hills) and environmental conditions (snow, rain, sleet and dust)?
- In cases of insufficient capacity, what kind of traffic back-off schemes should be implemented on vehicle-based and infrastructure-based radios?
- How should wireless misuse or misbehavior within the CV2X system be detected or prevented?
- Are the Security Credential Management System (SCMS) architectures proposed by the U.S. Department of Transportation (USDOT) sufficient under observable traffic conditions and emerging cyber threats and, if not, what mitigation can be proposed to alleviate the deficiencies?

CCI fellow designs security mechanisms for 5G

Dr. Kai Zeng, a CCI fellow, is exploring 5G security issues, conducting experimental research on a millimetre wave communication network testbed.

Dr. Kai Zeng is a CCI Fellow from GMU who is leading a research team of four PhD students to investigate 5G wireless network security. 5G wireless communication technologies are considered as the key enabler of many IoT applications, including autonomous driving, smart manufacturing, intelligent transportation, smart healthcare, smart city, smart grid, and environmental sustainability. Although there is significant ongoing work on the development of advanced 5G wireless communication techniques, the security aspects of these 5G wireless networks have not been sufficiently investigated.

In particular, the potential security benefits brought by 5G technologies, as well as new security threat against these new technologies, have not been well understood. Dr. Zeng's team is investigating the following topics in 5G security:

- 5G device authentication;
- Robust 5G physical layer key generation;
- Efficient pilot contamination attack detection and mitigation;
- Eavesdropping risk control for 5G wireless networks;
- Secure 5G wireless communications under mobility; and
- Testbed development.

Dr. Zeng has built a small-scale 60GHz testbed based on TP-link Talon ad 802.11ad routers and Talon Tools. After flashing the firmware, this testbed allows researchers to extract physical layer information such as Signal to Noise Ratio (SNR) and Channel State Information (CSI), which is very useful for the proof-of-concept evaluation of the proposed key generation and mmWave communication security mechanisms. This platform allows CCI researchers to investigate various aspects of 60 GHz millimeter-wave communication through realistic on-site experiments and evaluate security mechanisms physical layer authentication and fingerprinting.

In the Wireless Innovation and Cybersecurity Lab (WICL) at GMU, a 60GHz mmWave testbed based on the 60GHz Radio Frequency (RF) transceiver HMC6300 is also in development to conduct proof-of-concept experiments. The prototype consists of three parts: 60GHz RF frontend (HMC6300), baseband transmitter module (USRP NI-2922), and horn antenna (WR-15 waveguide transition). The RF frontend based on HMC6300 operates from 57 GHz to 64 GHz with up to 1.8 GHz modulation bandwidth, which supports multiple Gbps data communication. HMC6300 is compatible with the external local oscillator and universal I/Q interface, which thus supports for a wide variety of modulation formats (up to 256QAM). Three nodes will be built to perform as Alice, Bob, and Eve in a security attack. Currently, the RF front end has been evaluated and we are working on the development of baseband data processing units based on the Universal Software Radio Peripheral (USRP) N210.

Dr. Zeng's team proposed a unique physical layer feature in IEEE 802.11ad networks, namely the SNR trace obtained at the receiver in the Sector Level Sweep (SLS) process, to achieve efficient physical-layer spoofing attack detection. They conducted experiments using off-the-shelf 802.11ad devices, Talon AD7200s and MG360, to evaluate the performance of the proposed scheme. Experimental results confirm the effectiveness of the proposed scheme, and the detection accuracy can reach 98% using small sample sizes under different scenarios.

Dr. Zeng also proposed a physical layer key generation scheme for 5G networks. It can achieve a very low bit disagreement ratio even at low SNR, i.e., when the antenna number at Alice and Bob are equal to 128 with 3 clusters. For instance at an SNR of -10 dB, the bit disagreement ratio is around 10^{-2}, which is not achievable by existing schemes. In general, the bit disagreement ratio is decreased by two orders of magnitude using our proposed scheme compared to existing CSI based schemes. This is a very promising preliminary result that shows the advantage of using virtual channel Angle of Arrival and Angle of Departure as the new channel characteristics for key generation.

Based on the virtual channel representation, two effective pilot contamination attack detection schemes tackling static and dynamic environments were proposed. Simulation results show the proposed detection scheme can reach a high detection accuracy. The detection rate reaches 100% with 10^{-3} false alarm rate in the static environment and above 95% in a dynamic environment.

The secrecy performance was studied with combinations of two typical random mobility models: Random Waypoint (RWP) and Random Direction (RD). A general analytical framework to numerically calculate the average secrecy rates of Non-orthogonal Multiple Access (NOMA) mobile users under steady state is provided. By comparing secrecy performance of mobile users with static users, findings reveal that RWP mobile users can achieve higher average secrecy rates than the users with other mobility combinations. Meanwhile, two types of secrecy fairness for mobile users are fully considered and a novel sum average secrecy rate maximization problem was proposed, subject to average power limits and users' QoS requirements. Considering eavesdropper's CSI is unknown to the Base Station (BS), a threshold power allocation strategy was proposed to improve the sum average secrecy rate of NOMA mobile users.

The research results have been published in prestigious journals and conferences, including IEEE Wireless Communications, IEEE Internet of Things Journal, IEEE Transactions on Information Forensics and Security, IEEE Infocom, and IEEE CNS. Two papers have been presented at IEEE CNS 2020, and one will be presented in IEEE Infocom 2020.

Research Faculty recruited

Three full-time faculty members joined Virginia Tech and the CCI Hub specifically thanks to CCI funding: Dr. Luiz DaSilva joined as the Executive Director, and Bradley Professor of Electrical Engineering; Dr. Laura Freeman joined as a Research Associate Professor in the Department of Statistics and leads the AI Assurance thrust of CCI; and Dr. Haining Wang joined as a Professor in the Bradley Department of Electrical and Computer Engineering. Additionally, CCI Hub faculty have recruited several junior research faculty, post-doctoral researchers, and graduate students to join CCI.

Dr. Luiz DaSilva joins CCI as its inaugural Executive Director

Dr. DaSilva is a former faculty member at Virginia Tech, and most recently served as Director of CONNECT, a national research center in Ireland. [In the press: Powell, 2019]

After an international search, Luiz DaSilva was named the inaugural Executive Director of the Commonwealth Cyber Initiative (CCI) and professor of electrical and computer engineering in the College of Engineering at Virginia Tech. He was also named Bradley Professor in Cybersecurity by the Virginia Tech Board of Visitors. The Bradley Professor in Cybersecurity recognizes faculty excellence. Recipients hold the professorship for five years, and it is renewable.

Dr. DaSilva has spent more than 20 years in academia, including 17 years as a professor at Virginia Tech, where he established an international reputation for leadership and innovation in wireless communications and networks research. Before joining academia, he worked at IBM for six years.

A prolific scholar, DaSilva has co-authored two books and authored or co-authored 13 book chapters, approximately 100 journal or magazine articles, and 150 conference or workshop papers. Among his journal articles, 74 were published in prestigious IEEE transactions or magazines. He has given more than 60 invited talks, lectures, seminars, or keynotes around the world as an IEEE Distinguished Lecturer.

Dr. DaSilva is a Fellow of the IEEE for his contributions to cognitive networking and to resource management in wireless networks. He pioneered the application of game theory to analyze and design wireless networks and is also responsible for seminal work on cognitive networking and spectrum and network sharing. Dr. DaSilva has served as principal investigator on 39 research projects funded by U.S., Irish, European, and other international funding agencies and from industry partners.

In 2018, he was named director of the CONNECT Communications and Networks research center, a consortium of 250 researchers across Ireland. Similar to CCI, CONNECT has a mission of research, industry partnerships, innovation, workforce development, and public engagement.

Dr. DaSilva has a strong record of advising and mentoring of graduate students. Over his academic career, he has advised 11 master's degree thesis students to completion and 19 Ph.D. students, and he has also been an external examiner or opponent for 13 Ph.D. defenses in Europe, Singapore, and India.

In addition, DaSilva has chaired or co-chaired 10 international conferences, served on 12 National Science Foundation review panels, and reviewed proposals for at least 15 other organizations in various countries around the globe. Recently, he chaired the Technical Program Committee for ICC 2020, the flagship conference of the IEEE Communications Society.

When he was at Virginia Tech, he was recognized as a Virginia Tech College of Engineering Faculty Fellow in 2006. He received his bachelor's degree, master's degree, and Ph.D. from the University of Kansas.

Dr. Laura Freeman attracted $5M in external funding for her research in CCI

Dr. Laura Freeman was the first research faculty member hired with direct salary support from CCI. She leads CCI's AI Assurance thrust and has been immensely successful in attracting external research funds.

Dr. Laura Freeman joined Virginia Tech in February 2019 supported by a combination of College of Science (COS) and CCI funds. Funding from these two organizations (75% COS, 25% CCI) through June of 2019 allowed Dr. Freeman to accelerate the development of a research portfolio, leveraging her knowledge of defense, national security, test and evaluation. As a result, during the period of July 1, 2019 – July 2020, Dr. Freeman was the PI on programs totaling $914,844 spanning seven sponsors. She is also the Co-PI on two additional programs that support cybersecurity scholarships and fellowships totaling $3,758,905. Dr. Freeman's awards are accelerating in 2020: she has confirmed award of $2,268,500 in funding where she is the PI and has another $1,646,008 of proposals that have been submitted or are in progress. In addition to Dr. Freeman's funded awards, she submitted an additional $1.5M in proposals in 2020 that were not awarded. Dr. Freeman's salary contributions from CCI in FY20 was $54,000.

In 2020, Dr. Freeman spearheaded the first large CCI multi-disciplinary NSF research institute proposal on Trustworthy AI, with a budget of $20M. She recruited the research team including the PI on the proposal, Dr. Milos Manic from VCU. Dr. Freeman's efforts in hosting collaborative workshops enabled the development of strong relationships enabling the team to coalesce quickly and develop a $20M proposal on a short timeline. The proposal was evaluated as Good/Very Good by the NSF and showcases the likelihood that CCI will be successful on future large, center-size NSF proposals. Dr. Freeman also coordinated the CCI Summer Academy on AI Assurance. This academy was originally envisioned to bring graduate students and postdocs together from across the CCI networks for research presentations and educational opportunities.

Dr. Haining Wang is elevated to IEEE Fellow

Dr. Wang was elevated to IEEE Fellow this year, for contributions to network and cloud security. In any given year, this honor is reserved to at most 0.1% of the professional society's membership.

Dr. Haining Wang was recruited as a Professor in the Bradley Department of Electrical and Computer Engineering at VT, and in the past year his salary was funded in part by CCI. Prior to joining VT, Dr. Wang was a Professor of Electrical and Computer Engineering at the University of Delaware. His primary research goals lie in the general area of security and networking systems, in particular, an emphasis on cloud and Internet of Things security.

The main thrusts of his current and past research include security issues in Domain Name System (DNS) and Content Distribution Networks (CDNs), defense against use-after-free vulnerabilities in software, security issues in IoT devices, online reputation systems, energy/power attacks and countermeasures inside data centers, covert channel attacks and countermeasures in the cloud, behavioral biometric-based user authentication, automatic online bot detection, transparent anti-phishing, and countering distributed denial-of-service attacks.

The IEEE is the premier professional society for Electrical and Computer Engineers. It is the world's largest technical professional organization for the advancement of technology, with more than 400,000 members in 160 countries. In 2020, Dr. Wang was elevated to the rank of IEEE Fellow, for his contributions to network and cloud security. IEEE Fellow is a distinction reserved for select IEEE members with extraordinary accomplishments. In any given year the number of new IEEE Fellows cannot exceed 0.1% of the society's voting membership.

Three junior research faculty and five graduate students have been recruited to join CCI

The team of Hub Faculty and CCI fellows is complemented with junior research faculty and graduate students.

CCI Hub Faculty have attracted a number of junior researchers to join in research faculty roles and as graduate students, listed in Table 2.1. A number of these researchers were recruited from abroad and their arrival has been delayed by travel and visa restrictions in response to the COVID-19 pandemic.

Researcher	Role	Supervisor	Note
Jacek Kibilda	Research Assistant Professor	L. DaSilva	Awaiting visa
Anway Mukherjee	Postdoctoral Associate	T. Chantem	
Joao Santos	Research Associate	L. DaSilva	Awaiting visa
Tanmaya Mishra	Ph.D. student	T. Chantem	
Uzma Wajeeh Shaikh	Ph.D. student	T. Chantem	Awaiting visa
André Gomes	Ph.D. student	L. DaSilva	Awaiting visa
Jonathan de Almeida	Ph.D. student	L. DaSilva	Awaiting visa
Kriti Kansal	M.S. student	T. Chantem	Awaiting visa

Table 2.1: Junior research faculty and graduate students recruited in the CCI Hub.

Results of Entrepreneurship and Workforce programming

CCI Builds a New Experiential Learning Program for Cybersecurity in Virginia

In 2020, CCI devoted $700K in funding for six novel experiential learning programs that provide students in Virginia with hands-on experiences that complement degree programs in cybersecurity across the Commonwealth. [In the press: Washington, DC Citybizlist, 2020]

In 2020, CCI sought proposals for scalable pilot programs for experiential learning from member institutions across Virginia that would provide students with industry experience and enhance their skill sets to better prepare them to enter the cybersecurity workforce. Proposals were evaluated by a panel of experts coming from the four CCI Nodes; to avoid conflicts of interest, no expert evaluated any proposals coming from their own Node.

The CCI-funded program aims to create a statewide ecosystem of excellence in CPS and serve as a catalyst for research, innovation, talent development, and commercialization of technologies at the intersection of security, autonomy, and data. A panel of faculty and staff from CCI member institutions reviewed the submissions and awarded funding for six experiential learning projects to faculty and their students across the state:

1. Cyber startups: Pilot program for novel experiential learning – Startup companies are an important part of the Virginia cybersecurity ecosystem and they need cybersecurity talent, but are often limited in hiring because they do not have adequate financial resources and the cost of labor is high. By offering opportunities for students to obtain experiential learning at cybersecurity startups with a focus on innovation, this program is fostering creativity and entrepreneurship in students and connect startups with potential future employees. Participating students will not only develop their technical skills with real-world experience, but will also gain valuable soft skills, such as critical thinking and communication, that are essential in the dynamic startup environment. Furthermore, being part of the cybersecurity innovation ecosystem during their college education will encourage students to take advantage of these connections to stay in Virginia once they graduate and begin their professional careers. Lead faculty are: Karen L. Livingston, Associate Director of Entrepreneurship Programs at GMU; Diane R. Murphy, Professor of Information Management at Marymount University; and

Sarah M. Spalding, Interim Associate Dean of the School of Business and Technology at Marymount University.

2. Experiential learning through the Commonwealth Science, Technology, Engineering, and Mathematics (STEM) Industry Internship program – In this project, the Virginia Space Grant Consortium is expanding on its existing Commonwealth STEM Industry Internship program to build and grow state-wide experiential learning opportunities for Virginia students majoring in CPS, cybersecurity, autonomous systems, and data. The existing infrastructure will facilitate the connections between Virginia industry and STEM students who will develop professional and essential job-readiness skills they will need in their careers. When students graduate they will have established relationships with Virginia companies and be more likely to stay in the commonwealth as they enter the workforce. This project is led by Mary Sandy, Virginia Space Grant Consortium Director, ODU.

3. AI-Security Living Lab Experience (AISLE) – This program will offer multidisciplinary teams of undergraduate and high school students the opportunity to work together on problems of direct relevance to the development of secure and trustworthy AI, a growing field with a high demand for talent. AISLE will take place over five consecutive Saturday mornings at GMU and five additional consecutive Saturday mornings at JMU. Each five-Saturday period will have a dedicated theme, such as cyber-crime, finance cybersecurity, health data security, cybersecurity in transportation, or detection of cyber-threats that will be decided in collaboration with industry partners. The program is envisioned as a group of project-based learning activities, rather than a hackathon. Lead faculty are Nektaria Tryfona, Executive Director of Digital Innovation and Strategy at GMU and Director of the Mason DataLab; Kamaljeet Sanghera, Executive Director of STEM Outreach and associate professor of engineering at GMU; and Samy El-Tawab, associate professor of engineering at JMU.

4. Training in the integration of CPS and security – Graduate students are a critical component of the pipeline for cyber talent, especially in fields like cyber physical system security. In this project, researchers at UVA will adapt three graduate-level CPS courses with associated hands-on labs that can be adopted by universities throughout the Commonwealth. The courses will address real-world industry needs and problems, based on input from an established industrial advisory board, and will feature workshops on verbal and written communication, leadership opportunities through group projects, and sessions on ethics and entrepreneurship. The course, Signal Processing, Machine Learning and Control, will be taught by John A. Stankovic, the BP America Professor of Computer Science. Formal Methods, Safety, and Security will be taught by Lu Feng, an assistant professor of computer science. Mobile and Internet of Things Security and Privacy will be taught by Yian Tian, an assistant professor of computer science.

5. Drone racing competition: learning, defending, and attacking – Drones can accomplish diverse tasks, from delivering packages to military reconnaissance. Advancements in drone technology have spawned an entirely new competitive high-speed sport with a first-person view that involves piloting a drone against other racers through a course with several checkpoints. This project will build multidisciplinary teams of students who will compete in a series of "battle" drone-based AI competitions. The competitions will increase in course difficulty, include local companies for mentoring, and evolve to include cybersecurity challenges such as positioning communications systems degradation, jamming, and adversarial AI. Students will be encouraged to understand the existing infrastructure and to find ways to increase their chances of surviving and defeating their opponents. The project will be led by Jonathan Black, professor of aerospace and ocean engineering and Director of the Aerospace and Ocean Systems Laboratory in the Virginia Tech Hume Center for National Security and Technology.

6. Data poisoning and satellite reconnaissance: bridging application and education – Convolutional neural networks have been extensively used to assess road networks using imagery collected in two ways: on the ground via smartphone and aerially via satellites or drones. Imagery collected on the ground is largely used for road quality or as input into self-driving algorithms, whereas imagery collected by satellite or airborne systems is largely used to identify the growth or change in road networks in inaccessible areas. In this project, students will work with W&M faculty and external industry partners to design a data collection app and construct a convolutional neural network to predict road roughness across

Virginia, incorporating data from ground and aerial imagery. The second part of the project will be a cybersecurity competition in which student teams will explore ways to identify potential malicious changes to imagery and ways to mitigate the impact of such data poisoning. Lead faculty are Daniel Runfola, assistant professor of computer science; Anthony Stefanidis, professor of computer science; and Peter Kemper, associate professor of computer science.

CCI fellow focuses on preparing students for industry employment

Dr. Jeff Pittges developed and runs an online Cyber Camp, focusing on preparing students from under-served communities for a career in cybersecurity.

Dr. Jeff Pittges is a CCI Fellow from Radford University and he is leading a project 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.

In order to recruit K-12 students from underserved Lancaster County, VA into the STEM fields and build basic competencies for success in college programs, Dr. Pittges teamed with the National Integrated Cyber Education Research Center (NICERC) from Bossier City, Louisiana to develop a K-12 curriculum and training program for an online Cyber Camp. The Cyber Camp included three activities:(1) capture the flag contest, (2) cyber fundamentals with micro:bit processors, and (3) Python programming. In addition to the K-12 students, faculty from Lancaster and Pulaski Counties received cyber fundamentals training with micro:bits.

Collaborative partnerships and projects

CCI Partners with Virginia Cyber Range

CCI and Virginia Cyber Range partnered to run the Virginia Cybersecurity Workshop in the summer of 2020, dedicated to training high school and community college faculty who teach cybersecurity.

The Virginia Cyber Range has been hosting GenCyber camps for high school teachers since 2015, with funding from the NSA. With the advent of COVID-19, an in-person camp was no longer feasible, and the NSA decided not to fund the activity in 2020. CCI stepped in to fund a fully online Virginia Cybersecurity Workshop, which took place from June 22 to July 2. At CCI's request, the scope was broadened to include both high school teachers and community college faculty tasked with teaching cybersecurity courses. Dr. David Raymond was the chief architect and instructor for the program, with several invited lectures, including one from the CCI Executive Director, in which Professor DaSilva presented the mission of CCI and lectured on 5G security.

The workshop counted with 48 participants: 5 of them teach community college exclusively; 9 teach both community college and high school; and the remainder teach high school exclusively. The group was gender balanced, with 25 female and 23 male participants. Participants self-reported on race as: 30 Caucasian; 12 African American; 1 Asian; and 5 'other.' Six of the participants were retired or honorably discharged veterans of US Military service, or active National Guardsmen or Reservists.

Before the workshop, each participant was mailed a box of resources for the workshop and their classrooms. The box included: a headset to ensure high audio quality during the workshop; a Linux for Hackers book, used for homework and as a reference; The Code Book, which explores cryptography's use throughout history; A Yubiky 5 for two-factor authentication; and fun items including Virginia Cyber Range sticker, pen, and socks. The full package that participants received is shown in Figure 2.10.

At the end of the workshop, participants completed an extensive survey, with results described in (Raymond, 2020). Participants reported significant increase in their confidence in performing a number of cybersecurity tasks, as shown in Figure 2.11.

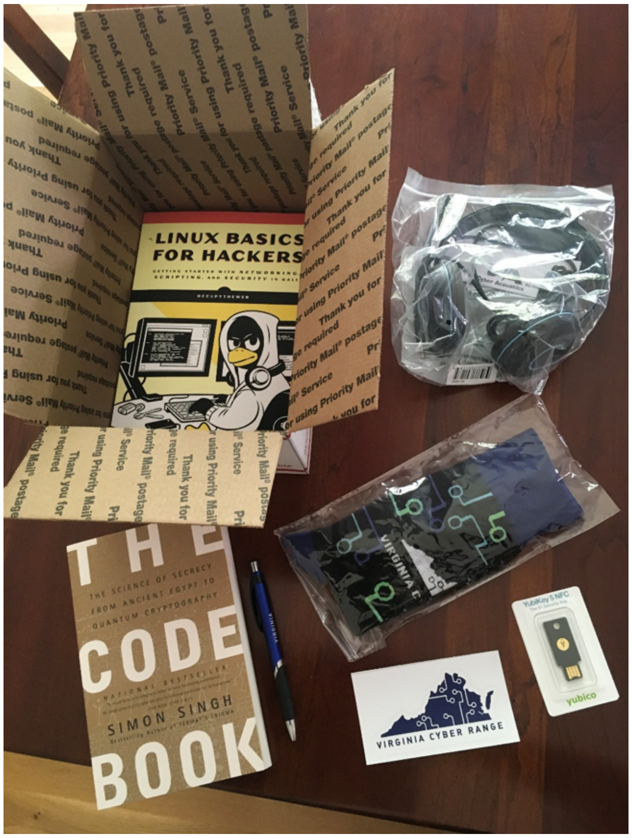


Figure 2.10: Package shipped to participants prior to the workshop (Raymond, 2020).

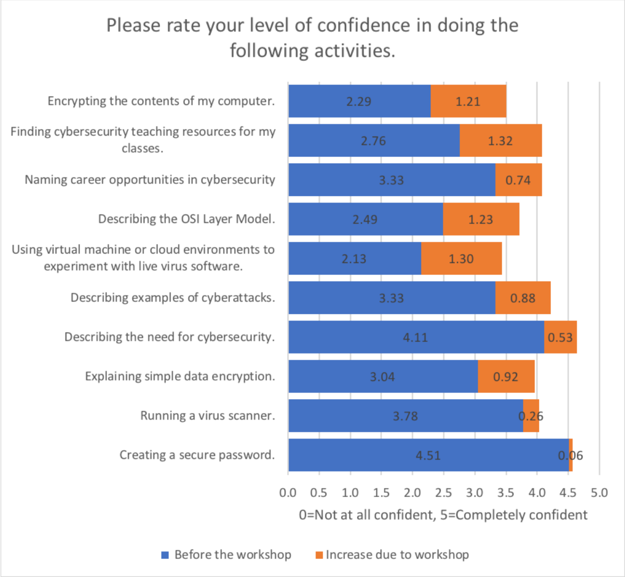


Figure 2.11: Participants' reported confidence in performing cybersecurity tasks (Raymond, 2020).

Innovation in using blockchain to create a trusted platform for tracking wireless devices

CCI fellow Sachin Shetty is working with Sentara Healthcare, from Norfolk, VA, to develop a 5G- and blockchain-empowered platform for tracking wireless devices.

Dr. Sachin Shetty is a CCI Fellow who is working with Sentara Healthcare from Norfolk, Virginia and Reliability First, a power grid regulator from Independence, Ohio on a research project to develop a blockchain and 5G empowered platform to realize a trusted platform for tracking wireless devices.

The ubiquitous adoption of networked IoT devices across sectors, such as healthcare, manufacturing, automotive, etc., has led to operational, financial, and risk management impacts on 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 QoS 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. There is a need to detect both insider and external adversaries by identifying the presence of rogue devices, unauthorized communications among authorized devices in real time, and to provide early detection that would facilitate proactive cyber defense capabilities. In addition, there is a need for the solution to be resilient itself to cyber-attacks and to be able to provide trusted alerts despite adversarial attacks. The goal of the project is to develop a blockchain- and 5G-empowered platform to realize a trusted platform for tracking wireless devices. Blockchain has attracted attention as the underpinning technology for cryptocurrencies, such as bitcoin. However, its capabilities extend beyond financial applications and provide security and privacy capabilities to a wide range of technology applications on distributed systems such as cloud and IoT. At its core, blockchain technology is about providing trust in data. This is valuable for businesses, as a blockchain network can serve as a digital ledger system that allows secure sharing of information. The 5G infrastructure will also be leveraged to leverage the low power and high latency capabilities required to track IoT devices in congested and contested communication environments.

Correlated economic outcomes (jobs and new business formation)

CCI is starting to have a direct impact on the jobs and research landscape in Virginia through the establishment of partnerships with industry and local governments and through the funding of student internships in small and medium businesses. In FY21, as described in section 4.1, we will commission an economic assessment study that identifies the total impact that CCI is having on the economy of the Commonwealth. In FY20 we can already see demonstrable impact in the creation of paid internship programs for Virginia students, programs that support translation of CCI research into products, and numerous partnerships with industry and local government. Here is what some of these partners say about the role of CCI:

AT&T is the leading mobile operator in the US. Vince Apruzzese, president of AT&T Virginia, characterizes the opportunities to partner with CCI as follows:

> The Commonwealth Cyber Initiative is yet another example of how Virginia is leading the way in higher education and technology,. We're excited to collaborate with these innovators, educators and technology leaders on the transformative potential of 5G and the critical importance of cyber security – issues that are so important to our Commonwealth and our country.

CCI is also building partnerships with key manufacturers in the 5G arena. Michael Shepherd, from Cisco, describes his view of how both Cisco and CCI can benefit from this relationship:

> Cisco is excited to be involved in and to collaborate on the CCI project and looks forward to working with the participating universities to investigate new capabilities that 5G will enable and how it will support enterprises that mobilize their workforces, extend automation and support new applications through higher data rates and increase network capacity and capabilities.

CCI is also building a partnership with Arlington County government. Richard Archambault, Arlington County Department of Technology Services, describes this partnership as:

> Arlington County and CCI are working together on a research program using AI/ML techniques to gather new insights from the enormous amounts of security alert data that Arlington County collects on a daily basis. Arlington specifically wants to include students in this research program, and are hoping that student participation will help increase workforce readiness. Researcher contributions to the development of novel threat analysis methods or deeper intelligence from data can also be shared with other, perhaps less well-funded, municipalities across the state. This is an excellent opportunity for students to get involved in real-world data-based research and to gain insight into internship and employment opportunities within the local government sector across the Commonwealth.

CCI is partnering with US Ignite to create a new program to bring innovation created in Virginia research institutions to the market. Bill Wallace, US Ignite, says:

> US Ignite, a high-tech, public-private non-profit has run over 30 successful reverse pitch competitions across the country as part of its NSF-funded Smart & Connected Communities program. The organization is now working with CCI to create a reverse pitch competition in IoT Security to be open to research faculty and graduate students from across the Commonwealth. US Ignite has the demonstrated expertise to guide an expert panel to encourage proposals, make down-selections, and select winners. The team also brings experience coaching these winners on to next steps for successful commercialization. This program will yield innovations and research opportunities in the field of IoT Security from across Virginia, and is also expected to result in a successful company and job creation.

Some elements of the partnership with US Ignite also involve Arlington County. Here is Jack Belcher, Arlington county Chief Information Officer:

> Working with US Ignite, Arlington County is the "customer" for a pilot program collecting data from sensors in public areas about social distancing compliance. CCI will serve as experts regarding the privacy and security of the data collected. This is an incredibly important aspect to the success of the pilot and could lead to important and interesting research and innovation.

Geographic distribution of awards from the funds contained in HB30

The CCI Hub allocated approximately 26% of its FY20 budget directly to the Nodes. These allocations were in the form of direct funding for equipment purchase to augment the 5G testbed ($1M), funding for the CCI Fellows ($0.9M), and funding for the winning proposals in the experiential learning call ($0.71M) described in Section 2.1.2. The allocations for each node are shown in Figure 2.12 and detailed in Table 2.2. The testbed funds are being moved to the respective Nodes as these Nodes become ready to purchase and deploy testbed equipment.

	NoVA	CeVA	SWVA	CoVA	
5G Testbed Development	$250K	$250K	$250K	$250K	$1M
CCI Fellows	$200K	$200K	$200K	$300K	$0.9M
Experiential Learning Program	$179K	$77K	$150K	$304K	$0.71M
	$629K	$527K	$600K	$854K	$2.61M

Table 2.2: Allocation of FY20 Hub funds to the Nodes.

2.1.3 Additional Programs, Projects, Accomplishments

We are deploying two unique pieces of research infrastructure, available for use by all researchers in the CCI network: a 5G testbed and an AI Assurance testbed. Both are described in this section.

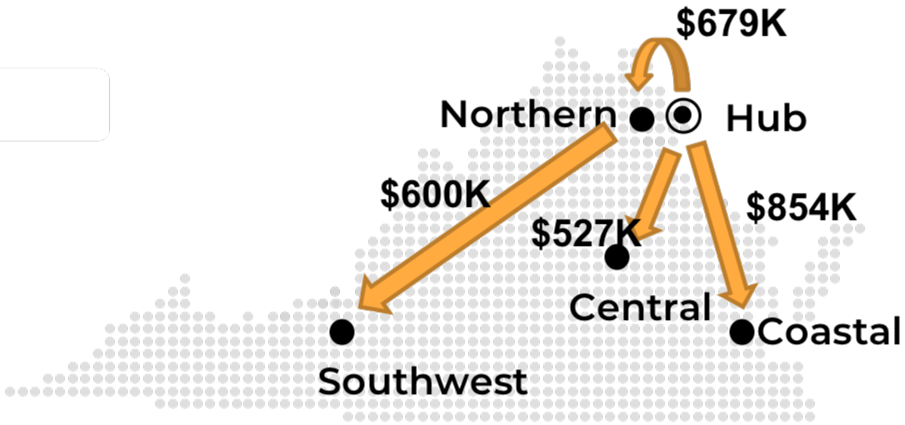


Figure 2.12: Allocation of FY20 Hub funds to the CCI Nodes.

CCI 5G Testbed

CCI Deploys a Unique 5G Testbed in Virginia

We are deploying the first 5G testbed in the Commonwealth, with sites in the Hub and each of the four CCI Nodes.

The US has fallen behind Europe and Asia in the development and deployment of the 5^{th} generation of mobile communications, or 5G. According to (Deloitte, 2020), China has built 350,000 new 5G sites, while the U.S. has built 30,000. We also lag in the development of IP, and the major hardware vendors are based in Europe (Finland, Sweden) and Asia (China, South Korea). The lack of a U.S.-based vendor, the increased softwarization of 5G, and the threats to a new generation of services empowered by 5G lead to unique security challenges in this space.

CCI is deploying a 5G testbed in the Commonwealth, as unique shared infrastructure for researchers and enterprises to test new technologies and services. The strategy is to closely align the testbed with the verticals that have the biggest potential to be revolutionized by 5G, including smart transportation, manufacturing, energy, and medical devices.

The CCI 5G testbed enables fast and targeted 5G innovation, hands-on implementation, and realistic evaluation and demonstration of new concepts and uses cases. It provides a scalable infrastructure for a wide range of 5G components, including user equipment, base stations, core network, and edge computing. The testbed has Sub-6 GHz and mmWave 5G implementations of the 5G architecture, empowering security research irrespective of 5G frequency or iteration, be it non-standalone or standalone. The testbed is equipped both with open-source end-to-end systems and carrier-grade emulation systems with commercial hardware and software. The open-sourced core network and network slicing functions enable the vertical design and innovation in 5G core and beyond in the CCI 5G testbed. Carrier-grade emulations are benchmarked for production quality level delivery.

The CCI 5G testbed counts with the transparency and modularity of open source development necessary for pinpointing security vulnerabilities within the 5G network architecture. The designed testbed architecture supports a seamless interface to various applications, including V2X, healthcare, smart farms, and power plants. As the testbed grows, the collaboration between CCI and other research organizations and industry partners is stimulating scaling of device testing and security implementation. In its mature state, in addition to research conducted at the CCI Hub, the testbed will be remotely accessible to all CCI researchers interested in pursuing 5G-related research. Its architecture will allow for scalable and dedicated user resources, preserving 5G network functionality while carving out an isolated modular slice of each research party's network. RF emulation functionality is equipped as an alternative for real-world device testing in the testbed.

The initial set-up of the testing and experiment support equipment in the 5G testbed is shown in Figure 2.13. The following equipment has been purchased to date for the 5G testbed with CCI funds:

- Amari Callbox Pro
  - Level of effort for installation and training: 2-3 days of training;
  - Base station and Evolved Packet Core (EPC)/5G Core (5GC), support for both standalone and non-standalone modes;
  - Allows external EPC/5GC or base station connection.
- Wavejudge
  - Level of effort for installation and training: 1-2 days of training;
  - Passive receiver for L1, L2, L3 data.
- USRP B210
  - Level of effort for installation and training: depends on the application, 1-3 weeks;
  - All-in-one Software Defined Radio (SDR) supporting open source 5G user equipment and base station.
- USRP X310
  - Level of effort for installation and training: depends on the application, 2-4 weeks.
  - High performance SDR supporting open source 5G user equipment and base station.
- Rohde & Schwarz SMW200A Vector Signal Generator
  - Level of effort for installation and training: 2-3 days of training;
  - Vector signal generator for the most demanding applications.
- Rohde & Schwarz FSW Signal and Spectrum Analyzer
  - Level of effort for installation and training: 2-3 days of training;
  - Signal and spectrum analyzer supporting a frequency range of 2-60GHz.
- X86 Server for 5GC Hardware
  - Level of effort for installation and training: 2-3 days of training (including 5GC);
  - Open Source 5G Core and other applications, including MEC.

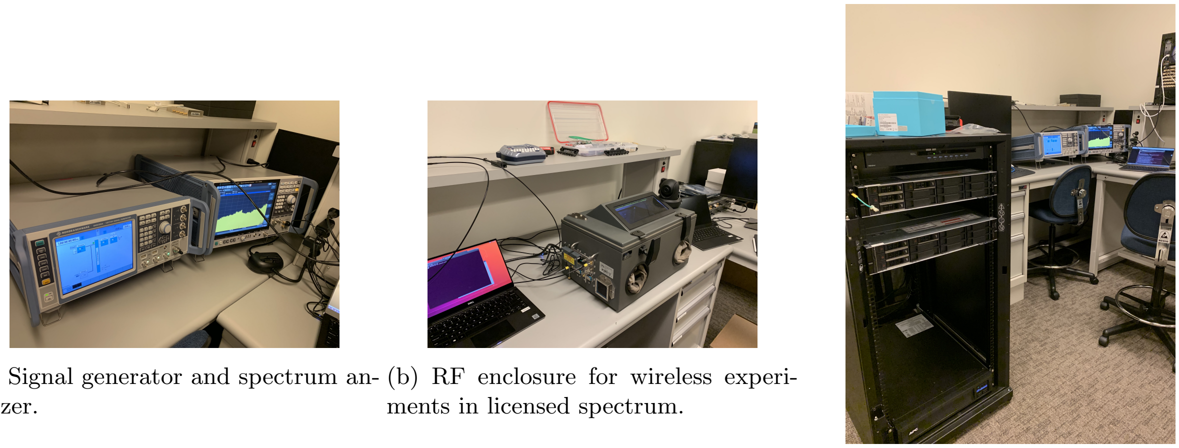
CCI AI Assurance Testbed

CCI Deploys an AI Assurance Testbed

CCI is deploying a unique AI Assurance testbed, with state-of-the art hardware tailored to support AI applications and curated models and datasets.

The AI Assurance testbed started to be deployed in FY20, led by CCI Hub Faculty Dr. Laura Freeman. An NVIDIA DGX-2 was purchased and installed in October 2019; the DGX-2 provides processing power for large-scale AI projects and integrates 16 Graphics Processing Units (GPUs). Initial accounts for CCI researchers to use the DGX-2 system were set up in December 2019. Additional 200 TB of storage were provisioned in February 2020. The installation of additional servers for user administration and system scheduling control is planned in FY21.

Currently, 15 researchers from the disciplines of Statistics, Computer Science, Electrical and Computer Engineering, and Transportation use the testbed. Examples of impact from the testbed to date include:



(a) Signal generator and spectrum analyzer.

(b) RF enclosure for wireless experiments in licensed spectrum.

(c) Rack and bench in indoor testbed lab.

Figure 2.13: Testing and experiment support equipment for 5G testbed in the CCI Hub.

- The plans for this testbed were used by Dr. Jeff Reed's team as supporting research infrastructure for a successful application to a prestigious Multidisciplinary University Research Initiative (MURI) grant, demonstrating a new application of the Age of Information metric.
- The testbed enabled users to scale a new capability to identify and predict radio signal anomalies using an adversarial machine learning approach.
- These resources enabled a reduction of training time from a month to 2 weeks for a state-of-the-art computer vision deep learning model.
- The testbed enabled simulations to study the robustness of deep learning methods and conduct uncertainty quantification of deep learning predictions. This research would not have been possible on regular computing clusters.

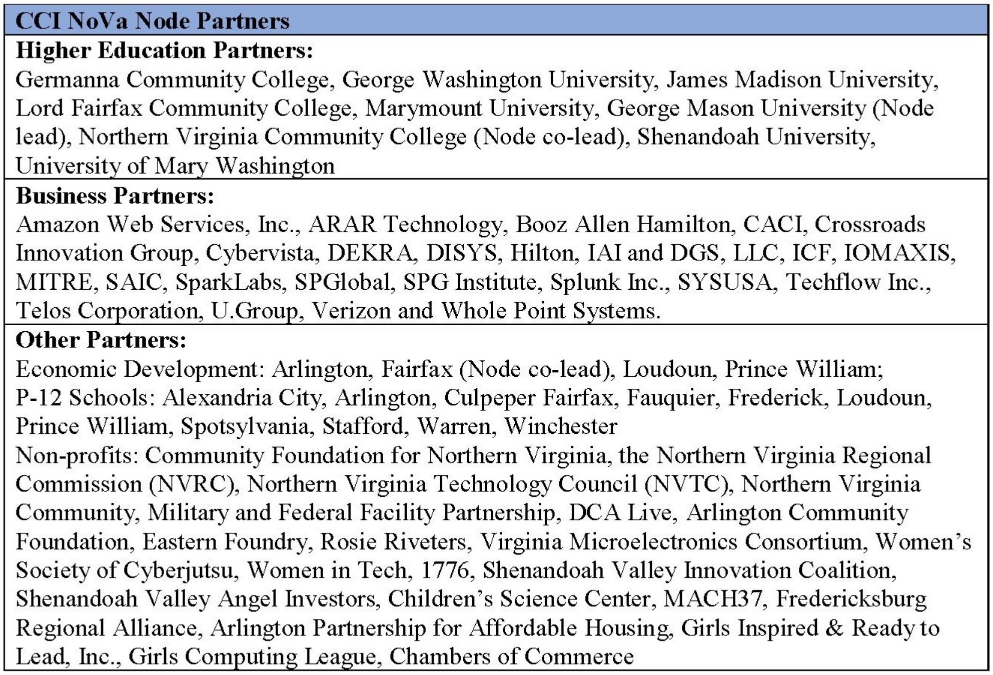
One of the major investments by the CCI Hub in FY21 is to expand the capabilities of the AI Assurance testbed. These plans are further described in Section 4.2.1.s

2.2 CCI Northern Virginia Node

2.2.1 Role of the CCI Northern Virginia Node

The NoVA Node is comprised of more than 75 partners (Figure 2.14) representing academic institutions of higher education, industry and government entities, economic development authorities, non-profit organizations and P-12 school systems that anchor the pipeline of future cyber security professionals. Focusing on autonomy, security, promoting technology commercialization and entrepreneurship, and preparing future generations of diverse practitioners, innovators, educators, and research leaders, the NoVA Node is poised to play an out-sized role in ensuring the Commonwealth is recognized as a global leader in trustworthy CPS and in the tech innovation economy more broadly for decades to come.

Developed through a consensus building process, the NoVA Node strategic plan addresses the four goals of CCI. The Proposed NoVA Node Programs were also curated through a consensus building process and support shared equipment and resources, scalable results and knowledge, and technology transfer. From these efforts, new partnerships across institutions have been forged and all partners have been engaged in program formation, and will benefit from their output.



CCI NoVa Node Partners
Higher Education Partners: Germanna Community College, George Washington University, James Madison University, Lord Fairfax Community College, Marymount University, George Mason University (Node lead), Northern Virginia Community College (Node co-lead), Shenandoah University, University of Mary Washington
Business Partners: Amazon Web Services, Inc., ARAR Technology, Booz Allen Hamilton, CACI, Crossroads Innovation Group, Cybervista, DEKRA, DISYS, Hilton, IAI and DGS, LLC, ICF, IOMAXIS, MITRE, SAIC, SparkLabs, SPGlobal, SPG Institute, Splunk Inc., SYSUSA, Techflow Inc., Telos Corporation, U.Group, Verizon and Whole Point Systems.
Other Partners: Economic Development: Arlington, Fairfax (Node co-lead), Loudoun, Prince William; P-12 Schools: Alexandria City, Arlington, Culpeper Fairfax, Fauquier, Frederick, Loudoun, Prince William, Spotsylvania, Stafford, Warren, Winchester Non-profits: Community Foundation for Northern Virginia, the Northern Virginia Regional Commission (NVRC), Northern Virginia Technology Council (NVTC), Northern Virginia Community, Military and Federal Facility Partnership, DCA Live, Arlington Community Foundation, Eastern Foundry, Rosie Riveters, Virginia Microelectronics Consortium, Women's Society of Cyberjutsu, Women in Tech, 1776, Shenandoah Valley Innovation Coalition, Shenandoah Valley Angel Investors, Children's Science Center, MACH37, Fredericksburg Regional Alliance, Arlington Partnership for Affordable Housing, Girls Inspired & Ready to Lead, Inc., Girls Computing League, Chambers of Commerce

Figure 2.14: CCI NoVA Node Partners.

CCI NoVA's plans are ambitious and represent a long view to positioning NoVA and the larger Commonwealth as the leader in Cyber Physical Systems Security (CPSS). In addition to CCI funding, NoVA is seeking external sponsors to support their plans and also work together to leverage ongoing activities where convergence of efforts and pooling of resources will enable faster and wider scale of the goals. These efforts are ongoing and complement the resources received from CCI. The following summarizes the endeavors of NoVA in the three primary goals of CCI in research, innovation, and workforce development.

Research

To meet the CCI Goal of building world-leading CPSS research capabilities, the NoVA Node has been working with its partners to develop cross-node research programs to promote collaborative interdisciplinary research teams to enable applying advanced cyber technologies to Node focus areas:

- Cyber security of the transportation network;
- Cyber research for the National Defense;
- Impact of human behavior on cyber security and resilience of cyber systems to human behavior; and
- cyber security of electric/power distribution.

The strategic areas of focus are areas where the geographical location in the Northern Virginia Region, the interests and challenges of the constituents of the region, or the expertise of the university and industry researchers in the region confer some significant advantage in terms of strategic impact compared to other regions. These strategic focus areas will evolve over time as the CCI scales across the Commonwealth and new cybersecurity challenges emerge. It is expected that CCI NoVA Node partners will endeavor to collaborate on research initiatives that fall under these strategic focus areas and initiatives in order to build multi-institution capability.

Research initiatives undertaken by the NoVA Node partners in FY20 include:

- Transportation and network cybersecurity by building an open, in-lab, in-field experimental system, including a fleet of deployable vehicles to investigate problems introduced by autonomous vehicle communications, as well as the impact of 5G on their security.
- Secure 5G wireless communications by conducting comprehensive research to understand the security challenges and benefits of 5G wireless communications technologies.
- Critical infrastructure protection using adversarial learning and moving target defenses by building a large-scale defense collaboration lab where multiple universities and industry partners can experiment with advanced malware to increase network resiliency and secure communications.
- Fast, automatic, and accurate code-based attack attribution through deep learning, allowing cyber defenders to respond better by helping them trace cyber attackers against critical US infrastructure more quickly and accurately.
- Cyber disaster resilience by establishing a novel and dynamic multi- phase assessment framework, capable of modeling and quantifying the strength of cyber infrastructures, including human vulnerabilities during an extreme disruption.
- Training the next generation of cybersecurity experts by developing scalable training modules and experiential learning opportunities for students as a core component of all CCI NoVA Node research endeavors.

Additionally, the NoVA Node is working to uplift cybersecurity research infrastructure by:

- Developing 5G-enabled testbeds;
- Providing the external community with access to research expertise across the node through the CCI NoVA Node website; and
- Standing up the CCI Northern Virginia Node Living Cyber Innovation Lab.

The CCI Northern Virginia Node Cyber Living Innovation Lab will be housed on Mason's Arlington Campus. Adjacent to Mason's new Institute for Digital InnovAtion (IDIA), the lab will include approximately 4,000 square feet of dedicated space for cybersecurity research, training, and experiential learning. The Living Innovation Lab will include robotic platforms to evaluate 5G performance and security vulnerabilities. It will study the impact of 5G on industry, IoT or Industry 4.0, and smart manufacturing, as well as the vulnerability of the supporting power grid. The lab will include autonomous vehicle sensor study, 5G performance, and security vulnerability. These platforms will support Lidar, radar, stereo, and night-vision cameras that will be deployed on the NoVA Node's fleet of vehicles that simulate autonomous driving. The NoVA Node's Cyber Living Innovation Lab will be a nexus of CCI partner activity, a place for convening, experimentation, training and data sharing among the NoVA Node partner institutions.

The Cyber Living Innovation Lab will enable research as well as hands on experiential learning and will be open to all NoVA Node partners. An adjacent training facility will enable instruction of NoVA Node partners on the use of experimental equipment, including fleet of vehicles, radar, Lidar and stereo and night vision cameras, sensors, data collection, data analytics and experimental design. Office space for NoVA Node faculty, other partner visitors and graduate student researchers to remain in residence for variable periods will be included. This facility will also enable instruction of cohorts of community college students and undergraduates incorporating hands on experiential exercises to elucidate classroom instruction on security of CPS, 5G, transportation networks, manufacturing, and power. The Lab is scheduled to be ready for operation by January 2021.

The testbeds and labs developed under these CCI initiatives will be shared resources serving the NoVA Node and the broader CCI Network.

Innovation

The CCI NoVA Node seeks to accelerate cyber startup creation and technology commercialization through a number of strategies including identification of critical challenges from public and private sector to inform startups in the region, leverage resources, such as CCI grants, Virginia Small Business Financing Authority (VSBFA), Small Business Innovation Research (SBIR), Small Business Development Center (SBDC), Small Business Technology Transfer (STTR) to provide seed funding for new cyber technologies; scale existing programs and resources such as Innovation Commercialization Assistance Program (ICAP) and I Corp-style programs to expand impact; and incentivize university faculty to advance technology to commercialization.

The CCI NoVA Node also seeks to develop the next generation of cyber entrepreneurs by serving as a clearinghouse of student opportunities to gain experience with entrepreneurship programs in universities and in partnership with business leaders, and mentors with experience in lean startup who are willing to counsel and support students. The NoVA Node's Website will serve as a clearinghouse to consolidate information, resources and opportunities.

Finally, the CCI NoVA Node seeks to develop an ecosystem for collaborative, commercialized cybersecurity research and development in Northern Virginia. The CCI NoVA Node seeks 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 R&D opportunities in the region.

Workforce Development

The NoVA Node seeks to grow workforce-ready cybersecurity and cyberphysical system security talent to meet today's demands and tomorrow's economy. The NoVA Node's strategy to achieve this goal is to provide experiential learning opportunities to students (defined broadly) to enable them to apply knowledge, skills and abilities acquired in classroom to real-world cyber challenges. Experiential learning opportunities should span needs of entire student cycle. For example, middle/high school students basic computing and soft skills are reinforced, college/university level students practice specific cyber knowledge, skills and abilities, and experienced workforce reinforce advanced and emerging practices. In addition to experiential learning opportunities, the NoVA node seeks to develop initiatives that encourage students' selection of cyber and cyber related education/training pathways (defined broadly), reduce the cost of cyber education and training and time to degree completion, and in the long term, enable scale of successful initiatives.

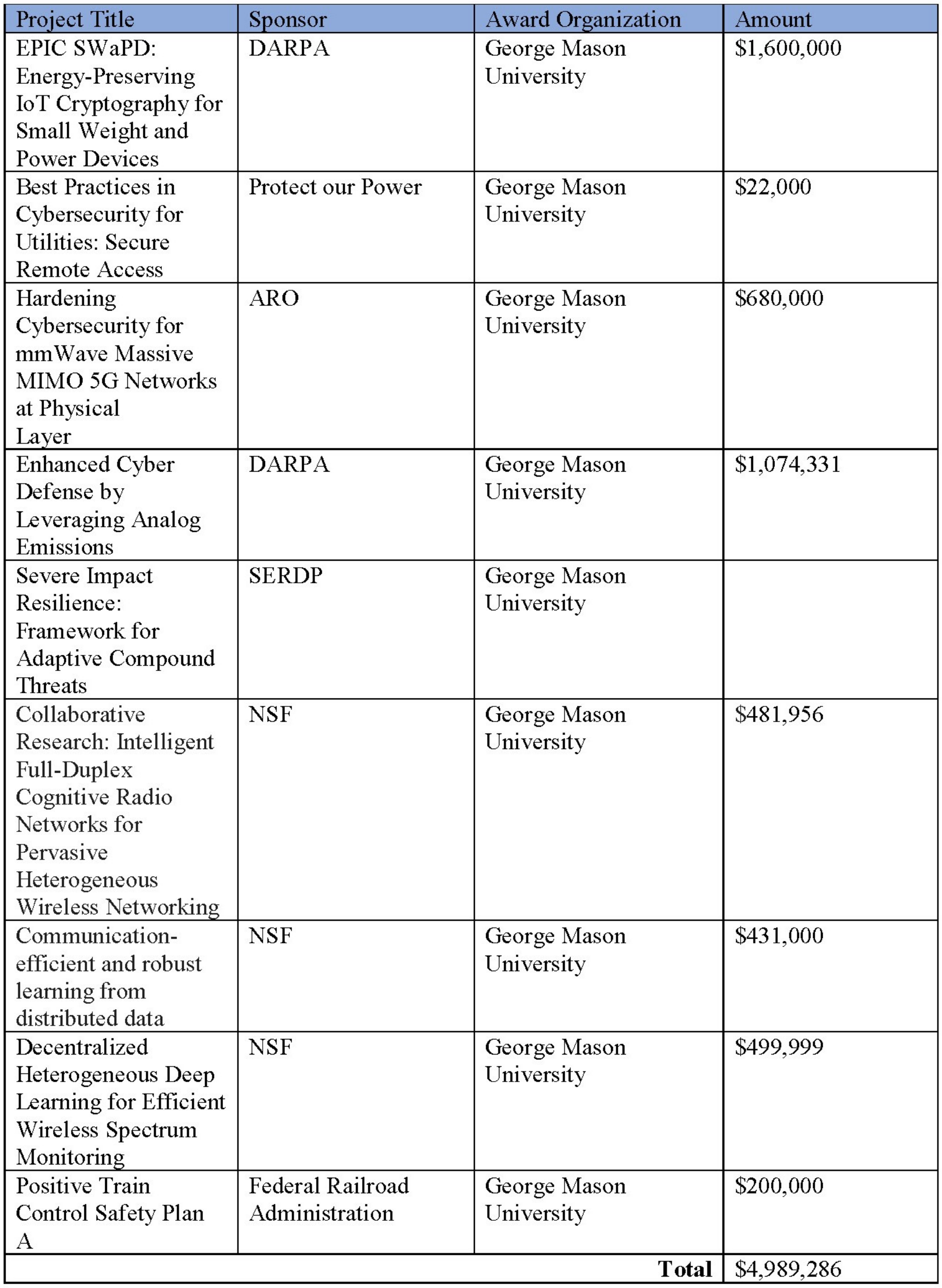
2.2.2 Report on the Seven Requirements as per Item 135, Chapter 1289, HB30

External Research Grants attracted to support the work of CCI

The CCI NoVA Node has drawn nearly $5M to support CCI-related research. In addition, the CCI NoVA Node has approximately an additional $6M of proposals pending with agencies including NSF, ARO, National Spectrum Consortium (NSC), Federal Railroad Administration, Department of Energy (DoE), and National Institute of Standards and Technology (NIST) (Figure 2.15).

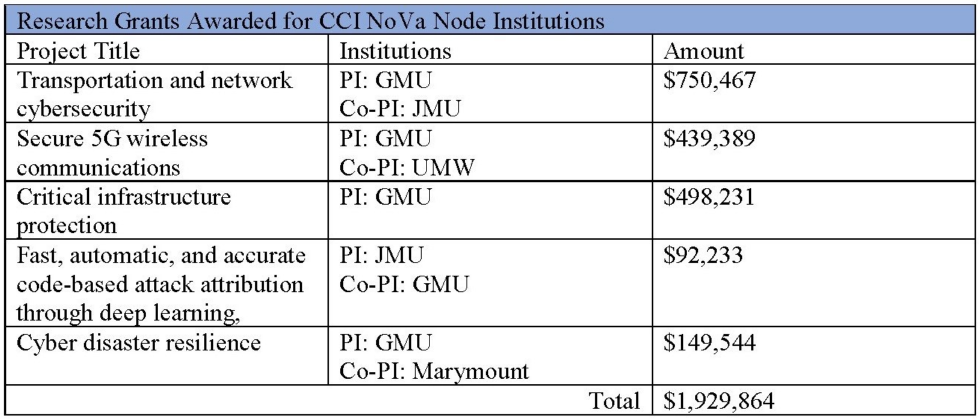
Research Grants awarded from the funds contained in HB30

Research awards supported by HB30 are nearly $2M for CCI NoVA Node institutions (Figure 2.16).



Project Title	Sponsor	Award Organization	Amount
EPIC SWaPD: Energy-Preserving IoT Cryptography for Small Weight and Power Devices	DARPA	George Mason University	$1,600,000
Best Practices in Cybersecurity for Utilities: Secure Remote Access	Protect our Power	George Mason University	$22,000
Hardening Cybersecurity for mmWave Massive MIMO 5G Networks at Physical Layer	ARO	George Mason University	$680,000
Enhanced Cyber Defense by Leveraging Analog Emissions	DARPA	George Mason University	$1,074,331
Severe Impact Resilience: Framework for Adaptive Compound Threats	SERDP	George Mason University	
Collaborative Research: Intelligent Full-Duplex Cognitive Radio Networks for Pervasive Heterogeneous Wireless Networking	NSF	George Mason University	$481,956
Communication-efficient and robust learning from distributed data	NSF	George Mason University	$431,000
Decentralized Heterogeneous Deep Learning for Efficient Wireless Spectrum Monitoring	NSF	George Mason University	$499,999
Positive Train Control Safety Plan A	Federal Railroad Administration	George Mason University	$200,000
		Total	$4,989,286

Figure 2.15: Grant proposals awarded to support CCI research.



Research Grants Awarded for CCI NoVa Node Institutions		
Project Title	Institutions	Amount
Transportation and network cybersecurity	PI: GMU Co-PI: JMU	$750,467
Secure 5G wireless communications	PI: GMU Co-PI: UMW	$439,389
Critical infrastructure protection	PI: GMU	$498,231
Fast, automatic, and accurate code-based attack attribution through deep learning,	PI: JMU Co-PI: GMU	$92,233
Cyber disaster resilience	PI: GMU Co-PI: Marymount	$149,544
	Total	$1,929,864

Figure 2.16: Research awards for CCI NoVA Node institutions supported by HB30.

Research Faculty Recruited

While the CCI NoVA Node did not use CCI resources to recruit new faculty in FY20, eight PhD students have been recruited and are supported in part with CCI NoVA Node funds. These doctoral candidates are actively contributing to the body of published literature, and cybersecurity R&D in the NoVA Node. They are future faculty, entrepreneurs or senior engineers preparing to have an impact in the cybersecurity ecosystem in northern Virginia.

Innovation and Entrepreneurship

To meet the CCI goal to accelerate cyber startup creation and technology commercialization, the NoVA Node partners have been engaged in a number of initiatives to support cybersecurity innovation, commercialization, and new ventures in the Commonwealth, making Virginia the best place to start a business in advanced cybersecurity technologies. In FY20 the NoVA Node has:

1. Conducted a request for proposals for Cyber Advanced Translational Development Grants (CATDG) to help teams speed the transition of research outcomes to the marketplace, paying for resources and personnel to test products and obtain initial market feedback. The winning teams were selected through a competitive process and evaluated by an external team of experts in innovation. The promising winning teams/products are:

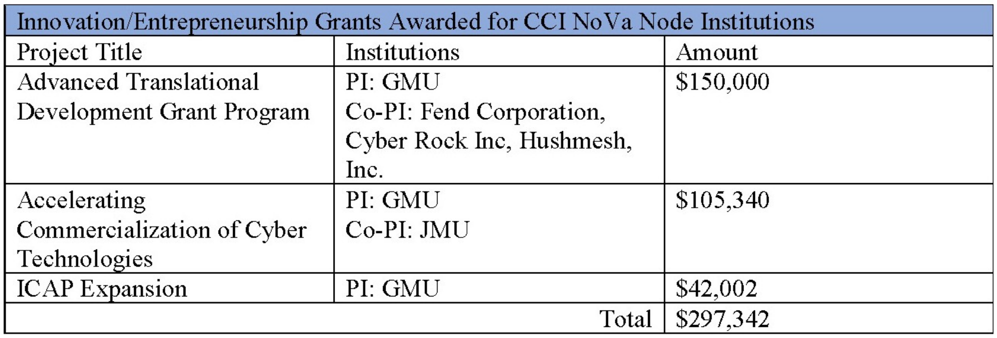
    - Fend Corporation: "Physically-Enforced Security for Vehicle Telematics";
    - CyberRock Inc.: "Transparent Immunization of Microsoft Windows Applications"; and
    - Hushmesh, Inc: "Decentralized cryptographic security for everyone".

    Awards totaling $150,000 were made in July 2020.

2. NoVA Node partners have also been working to accelerate the commercialization of cybersecurity technology by educating internal stakeholders about market strategies and facilitating regional technology showcases, and subsequently enhancing technology transfer and intellectual property commercialization from the region's research centers and institutions. The NoVA Node hosted a kickoff mixer event in January 2020 bringing faculty from across the Node and beyond together with subject matter experts from the Central Intelligence Agency (CIA) to discuss the CIA's most pressing cyber and big data challenges.

3. In FY20, the NoVA node supported the expansion of the ICAP, which guides startups through their early phases, helping them grow and engage investors. In May 2020, ICAP Launched a 100-Level virtual ICAP cohort. After two state-wide calls for potential partners with an emphasis on cyber – 85 people attended webinar training from over 70 organizations. Five cyber-related teams signed up for the July cohort. A 200-Level program was developed for the fall 2020 focusing on identifying early sales.

The innovation and entrepreneurship grants awarded by the CCI NoVA Node in FY20 are summarized in Figure 2.17.



Innovation/Entrepreneurship Grants Awarded for CCI NoVa Node Institutions		
Project Title	Institutions	Amount
Advanced Translational Development Grant Program	PI: GMU Co-PI: Fend Corporation, Cyber Rock Inc, Hushmesh, Inc.	$150,000
Accelerating Commercialization of Cyber Technologies	PI: GMU Co-PI: JMU	$105,340
ICAP Expansion	PI: GMU	$42,002
	Total	$297,342

Figure 2.17: Innovation/entrepreneurship grants awarded for CCI NoVA Node institutions.

Workforce Development

In FY20, to address the CCI goal to develop workforce-ready cybersecurity and cyberphysical system security talent to meet today's demands and tomorrow's economy, NoVA Node partners worked to:

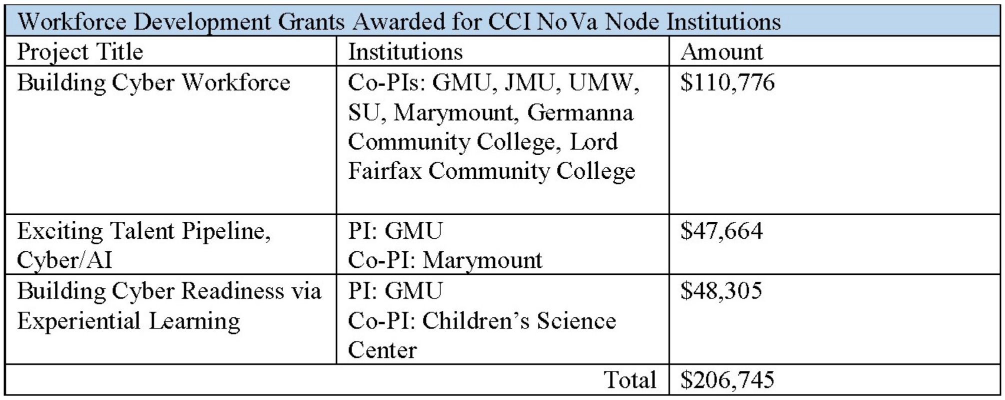
1. Build an active and strong cyber workforce by enhancing and aligning existing curricula of our academic partners with industry-identified skills to create pathways that bridge the gap between education and jobs. More than 120 industry and government partners provided responses to a survey to understand the skills, knowledge, and abilities (SKA) most needed in the cybersecurity realm. The NoVA Node academic institutions are working to map these SKA to academic programs and experiential learning opportunities

2. Develop the talent pipeline into the next cybersecurity workforce by designing experiences for Virginia students that provide the opportunity to learn about the role of artificial intelligence in cybersecurity. The cybersecurity workplace is changing as automated techniques are beginning to replace many of the technician jobs in the field. It is important that high school students understand these automated techniques, especially AI, as they increasingly apply to tomorrow's workplace, including cybersecurity. A cyber camp is designed to offer Virginia high school students the opportunity to learn about AI and its increasingly important role in our nation. The syllabus and activities developed will be made available to all schools in the Northern Virginia CCI node area, through a two-day orientation session and extensive dissemination of the resources. It will be a 5-day camp for 24 students (2 sets of 12 students each due to social distancing). Recruitment will focus on diversity, including female participation. The objective of the program is to prepare camp objectives, lesson plans and hands-on exercises for a week-long camp that could be offered throughout the Northern Virginia CCI node network, that will run as a pilot, primarily with Arlington Public Schools. Training modules will then be shared with teachers in a subsequent workshop to advance the tech transfer of cyber security lesson plans to secondary education classrooms.

3. Increase cyber readiness in students by offering internships in cybersecurity firms to prepare students for careers in cybersecurity. This initiative seeks to prepare and pair high school students with summer internships with cybersecurity firms. One barrier to integrating young people into a professional environment is their ability to communicate, conduct themselves in a professional setting, and work in teams. Corporate partners identify "soft skills" as a vital piece of education that is often missing in the academic and professional training programs and classes currently available. High School students may apply for positions with cyber firms and, if accepted, enter into a two-week professional development program with the Children's Science Center, followed by eight weeks of professional internship experience with a NoVA Node industry partner. The outcome will be a robust, paid experiential learning opportunity for a high school student that provides a foundation in professional skills and cybersecurity skills, positioning them well for entry into a 2 or 4 year program in cybersecurity at an institution of higher education and subsequently, a career in cybersecurity. This pilot program will accept 20 public school students in summer 2021. Although originally scheduled to be executed in Summer 2020, the internship program was postponed until Summer 2021 due to the ongoing COVID-19 pandemic.

4. Connect the workforce with high-demand cybersecurity opportunities through CCI-NoVaNode.org, a clearinghouse of information about training, internships, apprenticeships, and full-time employment opportunities

The workforce development awards made by the CCI NoVA Node in FY20 are summarized in Figure 2.18.



Workforce Development Grants Awarded for CCI NoVa Node Institutions		
Project Title	Institutions	Amount
Building Cyber Workforce	Co-PIs: GMU, JMU, UMW, SU, Marymount, Germanna Community College, Lord Fairfax Community College	$110,776
Exciting Talent Pipeline, Cyber/AI	PI: GMU Co-PI: Marymount	$47,664
Building Cyber Readiness via Experiential Learning	PI: GMU Co-PI: Children's Science Center	$48,305
	Total	$206,745

Figure 2.18: Workforce development awards for CCI NoVA Node institutions supported by HB30.

Collaborative partnerships and projects

Secure Transportation Networks

The CCI NoVA Node is deploying a 5G testbed dedicated to supporting secure transportation networks, led by CCI fellow Dr. Duminda Wijesekera at GMU. The research agenda was previously described in Section 2.1.2. The 5G testbed to date consists of the following:

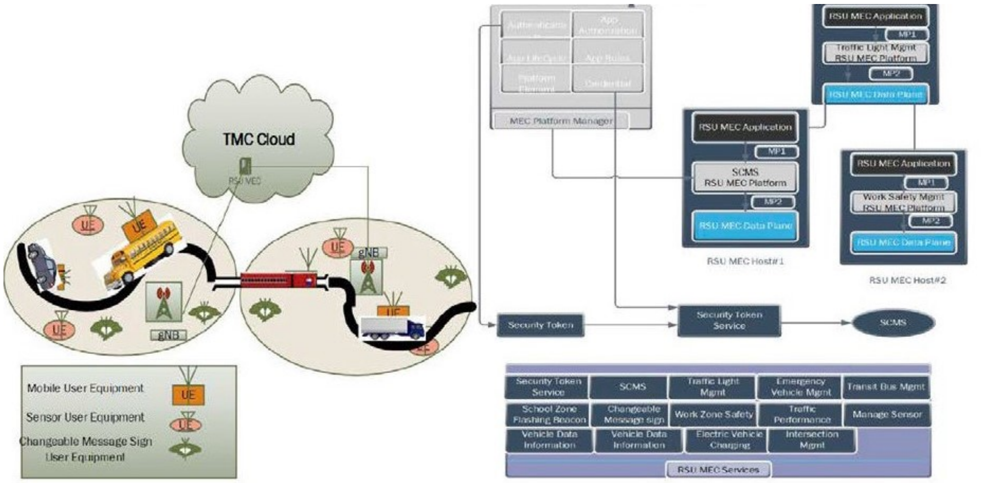
- 5G RAN, 5G core and a MEC system for experimentation on cyber security and specialized use cases such as CV2X and 5G for the Power Grid (5GPG).
- Three vehicles (Toyota Corolla, Honda Civic and Toyota Prius) equipped to Comma.ai software, color and infrared cameras, Lidars and radars.
- Driver simulation system suitable for in-lab experimentation.

- A programmable signal control system, and professional grade dual (infrared and cameras) integrated with the system for intersection management.

Some key accomplishments and ongoing initiatives to date include:

Developing MEC for CV2X and 5GPG

Dr. Wijesekera's team is in the process of developing mobile edge servers that connect to 5G radios for enabling multiple applications such as: connected vehicles; controlling power relays and synchrophasers (5GPG); smart building and cities that facilitate power transfer and dissemination; and industrial automation. The usage scenarios and internal MEC design are illustrated in Figure 2.19.



(Left) Usage Scenarios & Infrastructure (Right) Internal MEC Design

Figure 2.19: Usage scenarios and internal MEC design.

Simulating Autonomous Vehicles in Mixed Traffic

Dr. Wijesekera's team developed a driver simulator that drives on actual roads (Mason's Fairfax Campus) with 3-dimensional terrain, surface friction and lighting (daylight, night, dawn, dust and facing construction lights). Unlike most commercial simulators, this simulator can have multiple drivers driving on the same road network with autonomous vehicles. The team has developed an extended Simuation of Urban Mobility (SUMO) large-scale simulator integrated with a pseudonym certificate system to ensure the anonymity and un-linkability of emitted Basic Safety messages. The simulator supports Dedicated Short Range Communications (DSRC), IEEE 802.11p, and 5G CV2X transmission systems to develop realistic vehicular simulations, road geometries, traffic loads and experimenting the limitations on the number of vehicles that can be accommodated on CV2X systems without undue packets delays and sustainable packet drops. After four months of overhauling of the system, the system successfully runs on Mason's Argo cluster.

Multi-sensor Fusion for Vehicular Navigation

Dr. Wijesekera's team has developed a deep reinforcement learning system that can fuse multiple data streams (color cameras, infrared, Lidar and radar), even with moderate differences in time stamps for the individual streams (due to device clock drifts) and viewpoint differences. The same system can also categorize when one stream fails to detect obstacles and use the knowledge gained from one stream to teach the other without hand sampling. This also allows us to qualify the conditions under which individual sensors fail and quantify the failure rates that are paramount in providing assurances in terms of success probabilities under varying operational conditions.

Pedestrian Basic Safety Messages

This work has resulted in Basic Safety Message formats, including detection capabilities for pedestrian detection. The objective of the partly developed Pedestrian Basic Safety Message (P-BSM) is to allow a way for vehicles to be notified of potential pedestrian intrusions onto vehicles pathways and: (i) in case of autonomous vehicles, enrich the driving automation to take notice; (ii) in case of human driven cars to warn the driver. This work directly extends the dual focus camera based-pedestrian crossing being installed in Fairfax (e.g. one in front of the court house) and Arlington counties. The preliminary system has been successful because:

- The system employs deep learning systems (sparse and, dense optical flow and parse optical flow to determine pedestrian and vehicular flows) to detect potential pedestrian intrusions including jaywalkers and pedestrian walking at zebra crossings.
- The infrastructure provided under this grant allows us to use professional equipment to experiment. Preliminary detection photographs are shown in Figure 2.20.

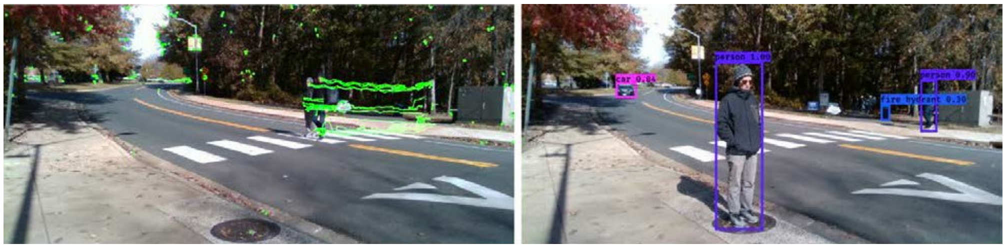


Figure 2.20: Pedestrian Basic Safety Messages.

Classifying User Behavior and Distractions from Drivers' Faces and Eye Movement

Research to classify driver behavior uses in-vehicle sensors (stereo and Infrared cameras) to detect driver distractions and estimate driver attention. Dr. Wijesekera's team is working to determine the conditions that create distractions for individual drivers and suggest automated responses to be taken by a vehicle. This work is illustrated in Figure 2.21.

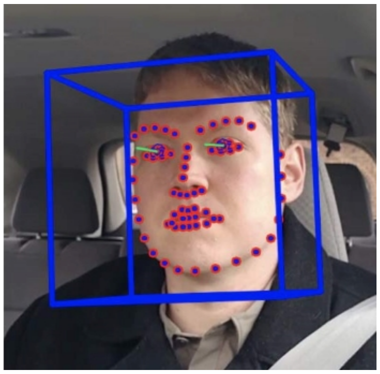


Figure 2.21: Classifying user behavior and distractions from drivers' faces and eye movement.

Attacks Modeling for CPS Using Systems Theory

Dr. Wijesekera's team continues to study Cyber-Physical-Chemical attacks on controllers of Lithium-iron battery controllers. His team has several batteries on hand and extracted and are in the process of reverse engineering the controllers.

5G Network Building

Dr. Wijesekera is leading a team to build the radio access network and the mobile edge computing system for CV2X systems.

Cyber Forensics

Dr. Wijesekera's team is working to develop a framework and algorithms for integrating data analytics and evidence-graph technologies to create a unified evidence collection capability in digital forensics examinations of mobile edge servers using deep learning.

Secure 5G Wireless Communications

The potential security benefits brought by 5G technologies, as well as new security threat against these new technologies, have not been well understood. In this initiative, 5G wireless communication security is being investigated in the following topics: 5G device authentication, robust 5G physical layer key generation, efficient pilot contamination attack detection and mitigation, eavesdropping risk control for 5G wireless network, secure 5G wireless communications under mobility, and testbed development.

Some key accomplishments and ongoing initiatives to date include:

5G Device Authentication and Identification

One of the interesting features of the beam pattern in mmWave Multiple Input Multiple Output (MIMO) is that the beam patterns' SNR shape is relatively stable for an individual device. This means that the transmitter's beam patterns do not change drastically over time. Different patterns show different SNR versus angle curves, while the same patterns present high correlations, even over a long measuring time interval.

To date, the team proposed a unique physical layer feature in IEEE 802.11ad networks, i.e., the SNR trace obtained at the receiver in the SLS process, to achieve efficient physical-layer spoofing attack detection. Experiments were conducted using off-the-shelf 802.11ad devices, Talon AD7200s and MG360, to evaluate the performance of the proposed scheme, obtaining detection accuracy up to 98%.

Robust 5G Physical Layer Key Generation

Physical layer key generation is a new key agreement mechanism, in which wireless devices measure highly correlated wireless channel characteristics (e.g., channel state information or received signal strengths) and use them as shared random sources to generate a shared key. In theory, in a rich multi-path scattering environment, a passive attacker who is more than a half-wavelength away from the legitimate users will obtain uncorrelated channel measurements, and thus cannot infer useful information about the generated key. Different from the traditional Diffie-Hellman key exchange protocol, the physical layer key generation mechanisms do not require expensive computation and have the potential to achieve information-theoretic security. Therefore, they are very appealing to many wireless IoT application scenarios with resource constrained devices.

Instead of using conventional CSI to generate the shared secret key between Alice and Bob, Dr. Kai Zeng's team at GMU proposed to utilize new channel characteristics – virtual Angle of Arrival (AoA) and Angle of Departure (AoD) – to generate the key. In the key generation process, Alice and Bob send sounding signals to each other within the channel coherence time to measure the virtual AoAs and AoDs. Then Alice and Bob quantize the channel characteristics and conduct information reconciliation and privacy amplification to generate the shared secret key.

According to the preliminary results, Dr. Zeng's team's process can achieve a very low bit disagreement ratio even at low SNR. This is a very promising preliminary result that supports the advantage of using virtual channel AoAs and AoDs as the new channel characteristics for key generation.

Efficient Pilot Contamination Attack Detection and Countermeasures

NOMA has been recognized as one of the key enabling technologies for fifth generation mobile networks. Via non-orthogonal resource allocation, NOMA can improve spectral efficiency and achieve massive connectivity with low transmission latency and signaling cost. However, NOMA is vulnerable to Pilot Contamination Attack (PCA), in which an attacker can send the same pilot signals as that of legitimate users. In the channel training phase, the PCA attacker can inject the same pilot as the legitimate user's to control the channel estimation result and affect the precoding process. If there are not any countermeasures, the attacker not only can degrade the signal reception at the legitimate receiver, but also can cause confidential information leakage in the communication system.

Dr. Zeng's team has proposed to exploit a unique characteristic in 5G wireless communication to counter pilot contamination attack in NOMA. In 5G communication networks, mmWave possesses high propagation loss and directionality which is highly sensitive to legitimate users' positions. Supported by massive MIMO, mmWave virtual channel, a representation of geometry channel model, will exhibit sparsity that can be used to distinguish pilot contamination attack from normal communication states in NOMA.

Based on the virtual channel representation, Dr. Zeng's team has established two effective pilot contamination attack detection schemes tackling static and dynamic environments, respectively. Simulation results show that the proposed detection scheme can reach a high detection accuracy.

Eavesdropping Risk Control for 5G Communications

While investigations in this are are still in a very early stage, Dr. Zeng's team is working on the development of a cross-layer security risk control framework to quantify the security risk introduced by packet eavesdropping at the physical layer with consideration of the discrepancies of message/packet-sensitivity, encryption-strength, and mutual trust between users at upper layers. Given a network profile of users, applications, and encryption algorithms and protocols (e.g., SSL, SSH, RSA, AES, DES, RC4, SHA3) utilized at each layer (application, transport, network, and Medium Access Control (MAC)) for each flow, Dr. Zeng's team will quantify the risk level of each individual packet and accumulated risk of multiple packets. The developed risk assessment models for wireless networks will integrate the user mutual trust factor, which thus will enable a context-aware security risk control at the physical layer for 5G wireless communications.

Secure 5G Wireless Communications with Mobility

In many application scenarios of wireless networks, mobility is intrinsic, e.g., civilian cellular users or connected cars moving in the city, soldiers and vehicles running in the battlefield, and cellular-connected UAVs delivering goods or performing surveillance tasks. Although the impact of mobility on network performance (e.g., throughput), communication quality (e.g., Bit Error Rate (BER) and outage probability), and physical layer security have been studied, very limited progress has been made so far in the study of spectrum efficiency and security of NOMA communications in 5G mobile networks.

Dr. Zeng's team is focused on the impact of mobility on the NOMA system and is studying the secrecy performance with combinations of two typical random mobility models: RWP and RD. A general analytical framework to numerically calculate the average secrecy rates of NOMA mobile users under steady state has been developed. By comparing secrecy performance of mobile users with static users, Dr. Zeng's team has confirmed that RWP mobile users can achieve higher average secrecy rates than the users with other mobility combinations. Based on their findings to date, Dr. Zeng's team has proposed a threshold power allocation strategy to improve the sum average secrecy rate of NOMA mobile users' communication.

Protecting Critical Infrastructure

Modern critical infrastructures have begun to transition from fully analog architectures towards hybrid ecosystems that incorporate a myriad of heterogeneous digital devices supporting physical interactions. Despite their value, the galloping integration of digital elements such as the Programmable Logic Controllers (PLCs) into these monolithic systems has exposed them to a new range of threats. Well-known incidents against critical infrastructures include the Stuxnet malware, which targeted the PLCs of a nuclear fuel enrichment facility in Iran, as well as the cyber-attack against the Supervisory Control and Data Acquisition (SCADA) systems of the Ukrainian power grid. Such incidents attest to the fact that not only critical infrastructures are on the scope of attackers, but also that these infrastructures remain to a large extent unprepared and vulnerable. To demonstrate the defense capabilities, Dr. Daniel Barbará's team at GMU is building a large-scale defense collaboration lab where multiple universities and industry partners can simulate and experiment with advanced malware that can cause network attacks and benchmark new defense strategies that are based on systems that support adversarial learning utilizing recent advances in AI and machine learning algorithms. The goal is to make these defenses capable of withstanding the challenges present in real industrial and infrastructure installations.

In order to achieve that, his team have researched and developed unsupervised techniques that can detect attacks not previously seen before (zero-day attacks) by analyzing involuntary emissions (which makes counterattacks very difficult). The team is busy finding solutions to real problems such as the presence of environmental noise and interference among the PLCs.

The lab may also be leveraged for training exercises exposing both recent advances in attacking capabilities and defenses to both students and industry practitioners. While many studies are evaluating protecting the 5G infrastructure operations, utilizing the 5G bandwidth in tandem with existing network services is the focus in this work. In addition to the work for Dr. Barbará's team, Dr. Eric Osterweil's team at GMU aims to increase the network resiliency and secure communications between critical infrastructure elements when they are attacked by sophisticated adversaries with access to state sponsored attack capabilities.

Specifically, Dr. Osterweil's team is employing enhancements to Named Data Networking (NDN) to orchestrate application and network level defenses that can be pushed to the network edge. The advantage in this approach is that this will help remediate Distributed Denial of Service (DDoS) attacks at their origins, before they have a chance to accrete and become overwhelming. In addition, Dr. Barbara's team is investigating the application of NDN to implement Moving Target Defense (MTD). This line of work capitalizes on flow parity that exists in NDN but does not require fixed control paths through the network. In the NDN architecture, data can be originated from any location, and sources can thereby move without disrupting ongoing network flows. The team is exploring how the bandwidth and deployment size increases that 5G technologies are ushering in will enable NDN-enhanced MTD solutions to fundamentally address shortfalls in current DDoS mitigation. They are also investigating necessary security and privacy protections that will need to be developed for dependent 5G technologies. Specifically, as orchestration and defenses are distributed increasingly broadly across 5G settings, the scale of securing and identifying end-systems will dominate deployment considerations. To address this, Dr. Osterweil's team is investigating using the DNS-based Authentication of Named Entities (DANE) protocol suite to allow end-point systems' security presences to scale with the expected 5G deployment sizes.

This project aims to continue the researchers' efforts of integrating the predictive power of AI and Machine Learning (ML) techniques with mature signal processing methods and lead to the development of novel and effective defenses.

Cyber Disaster Resilience: Assessment Framework for Cyber Impacts During Natural Disasters

Policymakers have attempted to reduce the impacts associated with threats by anticipating the unexpected; however, it is easy to under-analyze the complexities of risk, especially the relatively new category of risks from cyber threats. Natural disasters provide rich opportunities for cyberthreats to exploit already stressed infrastructure and social systems, creating a compounding effect. Policymakers require tools to handle effects of cyberattacks on information, physical, and social systems that can adapt as circumstances change. This project fosters community resilience against adaptive, compound threats that combine cyber attacks with natural disasters by developing: (1) metrics to assess the effects of communications infrastructure failures; (2) models to evaluate compound risk analysis and recovery; and (3) methods to enhance resilience against cyber deception and manipulation. This project also aims to establish how post-disturbance organizational learning can increase resilience by inoculating communities through institutionalized lessons learned and changed behaviors. The project team will apply insights from this analysis to evaluate educational initiatives that can assist humanitarian assistance and disaster response efforts, and to develop policy recommendations to support community resilience in the face of complex threats. Given recent events and the need to choose a focus area for the initial research, the decision was made to focus on the healthcare sector, and specifically the compounding effects of cyberattacks to the healthcare system in the midst of a disaster such as an earthquake, a hurricane, or a pandemic such as COVID-19. Models of hospital operations developed to study resilience are being augmented to incorporate the effects of cyberattacks.

Some key accomplishments and ongoing initiatives to date include:

- Dr. Kathryn Laskey's team at GMU has developed a method to enhance resilience against post-disaster social engineering using an open-sourced framework for annotating web data for disinformation. The framework was used to annotate 200+ websites comprising 1500+ sentences as misinformation, fact, or opinion. The framework will next be employed in training a machine learning algorithm to identify disinformation and misinformation.
- Dr. Laskey's team has developed metrics to assess effects of infrastructure failures and specifically evaluated cyberattacks on hospitals and their effects, with a focus on cyberattacks that disrupt hospital operations and affect patient care. Additionally, Dr. Laskey's team developed cyber-attack scenarios and integrated preliminary denial-of-service attack model in a hospital/pandemic mathematical model. The team defined metrics for evaluating hospital performance. Additional work will incorporate multiple types of cyberattacks, study the compounding effects of cyberattacks combined with other demand surge scenarios, examine strategies for improving resilience, and incorporate differential healthcare outcomes for marginalized populations.

Cyber Attack Attribution

In cyber security, attack attribution aims to either find the geographic location of a target hacker behind a cyberattack or determine whether an attack is conducted by a known hacker group (for example Advanced Persistent Threat 28, a Russian cyber espionage group). Tracing an attacker's real IP address can be extremely difficult, as a sophisticated hacker may break into multiple computers in different countries first, to minimize his/her traces on these zombie computers, and then use them as stepping stones to attack the real target. Tracing such an attack will often lead the investigators to the zombies' IP addresses, not that of the real hacker. Dr. Steve Wang's research team at JMU is using deep neural networks-based machine learning methods to analyze computer code that a hacker has left behind on zombie machines. By leveraging modern-day computational power and successful deep learning algorithms and tools, this project will achieve fast, automatic, and accurate code-based attack attribution. This approach differs from the traditional human-centric approach in its high-degree automation, from initial feature discovery to final attack attribution/classification. The project is organized around three attack scenarios, where the attack code is in the form of C/C++ source code, shell script, and binary executable respectively. In each case, appropriate deep machine learning methods are being investigated and their effectiveness for attack attribution is being evaluated.

Correlated economic outcomes (jobs and new business formation)

CCI NoVA Node ICAP Expansion in Cyber Security

The Virginia Small Business Development Center Innovation Commercialization Assistance Program (ICAP) delivers lean startup training and advising to early-stage, Virginia-based technology companies.

The CCI ICAP effort launched a 100-Level virtual ICAP cohort in May 2020. This program was conducted virtually due to COVID-19. Four companies applied for the program, three joined and all three completed the program, and each was a NoVA team. ICAP connected with the over 175 CCI NoVA Node contacts to announce the Program and held two state-wide calls for potential partners with an emphasis on cyber – 85 people attended from over 70 organizations. Five cyber-related teams signed up for the July 2020 cohort, two of which were as a result of using the CCI contact list. Development of a 200-Level program has started for the fall, focusing on identifying early sales. This program will also be delivered virtually due to COVID-19. It should be noted that ICAP works with early-stage companies and follow-on results and impact come about slowly, about 12, 24, or even 36 months later.

The ICAP teaching team spent a total of 58 hours with all three cyber teams leading up to and through the introductory course, including seven office hour meetings for each team as part of the introductory course. Each team received a follow-up action item list to discuss next steps and plans for future advising meeting. Each team will continue to work with their adjunct for as long as needed for their specific venture.

CCI Cyber Advanced Transitional Research Development Grant (CATRDG) Funding

The objective of the CCI NoVA Node CATRDG program was to support an idea from its concept through development and commercialization resulting in a minimal viable product or a commercial product ready for the end users. The CCI NoVA Node CATRDG program supports the commercialization of a cybersecurity technology or process and was awarded on a competitive basis to entrepreneurs with emerging technologies and faculty partners from public institutions of higher education within the NoVA Node. Mason's Office of Technology Transfer (ott.gmu.edu), on behalf of the CCI NoVA Node, facilitated pairing the teams of faculty researchers and local companies to speed the translation of academic cybersecurity innovations to the marketplace.

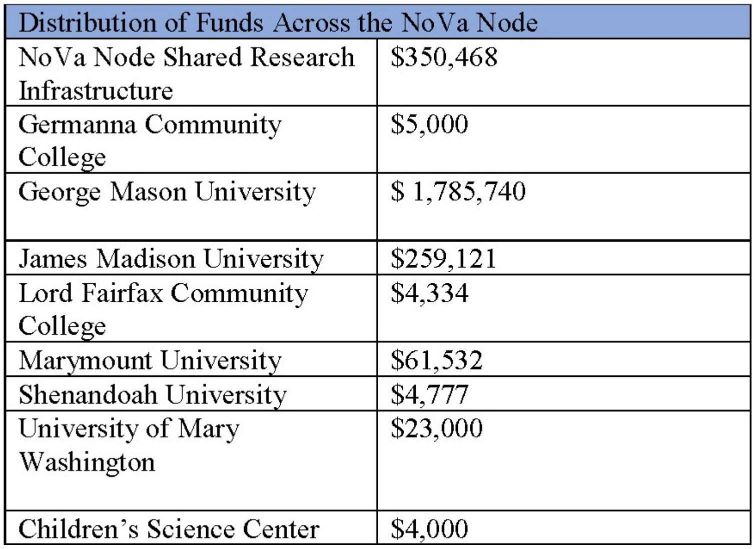
The winning teams and their products are as follows:

- CyberRock, Inc. (www.cyberrockinc.com): "Transparent immunization of Microsoft Windows applications". CyberRock, Inc. is developing and delivering the following cyber defense capabilities: 1) immunization-based cyber-defense systems to provide true real-time protection of mission-critical systems and networks from previously unknown cyberattacks; 2) Real-time and automated cyberattack attribution capability that can reliably identify and track encrypted and anonymized traffic across the internet.
- Fend Corporation (https://www.fend.tech): "Physically-enforced security for vehicle telematics". Fend protects America's critical infrastructure from cyberattacks using physics-based, one-way data flows. Fend's data diode products allow utility operators, building owners, and other managers to gain operational insight into equipment performance, such as control systems, chillers, pumps, and substations, without providing an adversary any physical path to infiltrate these networks. Paired with the power of predictive analytics in the cloud, Fend enables increased efficiency and resilience.

- Hushmesh, Inc (www.hushmesh.com): “Decentralized cryptographic security for everyone”. Hushmesh solves digital trust and privacy by wrapping cryptographic identity, authentication, and data security in a user experience that anyone can use called meshing in. Meshing in is a secure and convenient replacement for the outdated login process. It works universally across all use cases, devices, industries, markets, and geographies, both online and in the physical world. It eliminates usernames, passwords, two-factor authentication, account security questions, and password resets. As a result, it also eliminates phishing, social engineering, and identity theft and fraud.

Geographic distribution of awards from the funds contained in HB30

Figure 2.22 summarizes the distribution of resources across the institutions in the region. GMU is the only R1 research institution in the NoVA Node and therefore carried the research enterprise for the Node, in collaboration with the other institutions of higher education. Based on the robust engagement with the partners of the NoVA Node, a detailed strategic plan was developed in advance of the NoVA Node’s call for proposals to support the tenets of the strategic plan. All research grants support a component for tech transfer, in particular to community college faculty and students to support teaching and training on equipment and technology.



Distribution of Funds Across the NoVa Node	
NoVa Node Shared Research Infrastructure	$350,468
Germanna Community College	$5,000
George Mason University	$ 1,785,740
James Madison University	$259,121
Lord Fairfax Community College	$4,334
Marymount University	$61,532
Shenandoah University	$4,777
University of Mary Washington	$23,000
Children’s Science Center	$4,000

Figure 2.22: Distribution of funds across the NoVA Node.

2.2.3 Additional Programs, Projects, Accomplishments

The CCI NoVA Node has developed a website to serve as a regional resource and communicate about the CCI NoVA Node with the internal and external community. This includes a web-based clearinghouse portal for cyber internships, apprenticeships and full-time employment opportunities, as well as training and education opportunities (Figure 2.23). The CCI NoVA Node website also provides a clearinghouse for cyber security employment and training opportunities especially curated for veterans (Figure 2.24).

The CCI NoVA Node website also provides training and educational resources for teachers (Figure 2.25) and additional training resources for cyber practitioners (Figure 2.26).

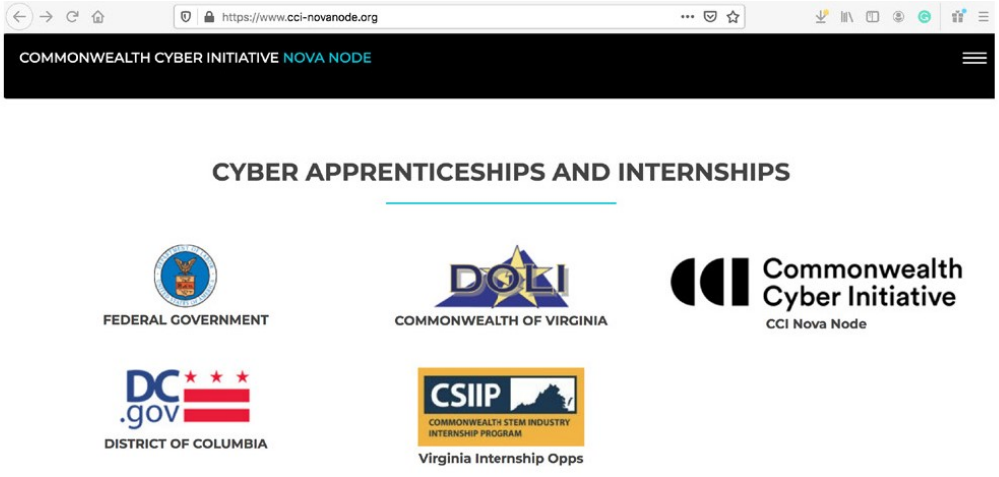

https://www.cci-novanode.org
COMMONWEALTH CYBER INITIATIVE NOVA NODE
CYBER APPRENTICESHIPS AND INTERNSHIPS
FEDERAL GOVERNMENT
DOLI
COMMONWEALTH OF VIRGINIA
Commonwealth Cyber Initiative
CCI Nova Node
DC.gov
DISTRICT OF COLUMBIA
CSIIP
COMMONWEALTH STEM INDUSTRY INTERNSHIP PROGRAM
Virginia Internship Opps

Figure 2.23: Cyber apprenticeships and internships.

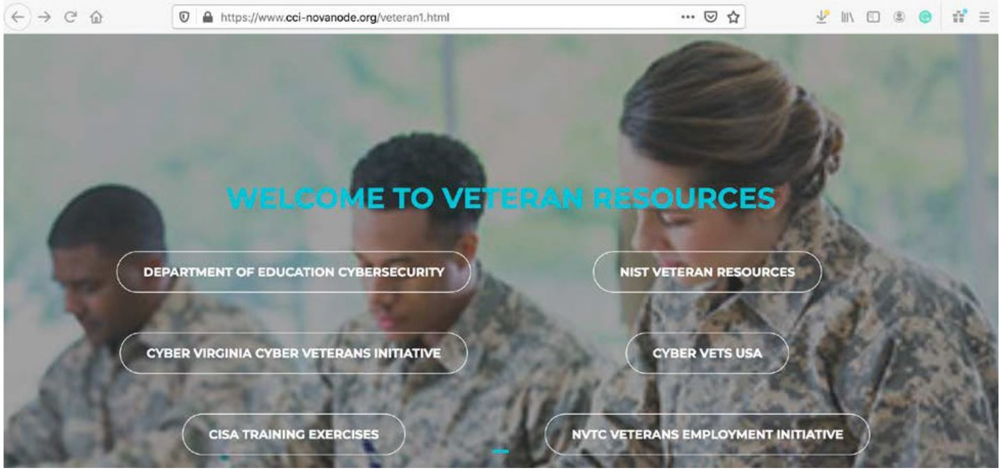

https://www.cci-novanode.org/veteran1.html
WELCOME TO VETERAN RESOURCES
DEPARTMENT OF EDUCATION CYBERSECURITY
NIST VETERAN RESOURCES
CYBER VIRGINIA CYBER VETERANS INITIATIVE
CYBER VETS USA
CISA TRAINING EXERCISES
NVTC VETERANS EMPLOYMENT INITIATIVE

Figure 2.24: The NoVA Node website is a valuable resource for veterans.

2.3 CCI Central Virginia Node

2.3.1 Role of the CCI Central Virginia Node

The two core research areas of the CeVA Node are: smart city and connected community development; and smart health and the impact of connected devices.

At UVA, CCI efforts are coordinated by UVA Engineering Associate Dean for Research Susan Barker, Associate Dean for Academic Affairs Prof. N Scott Barker, and Link Lab Program Director Travis Hite, as well as a steering committee of faculty to advise the CCI research investments. The faculty steering committee includes Profs. Peter Beling, Jack Davidson, Barry Johnson, John (Jack) Stankovic, and Yixin Sun. Direct staff support comes from the Office of Research Development, as well as the UVA Engineering Graduate office and Engineering Career Development office. CCI-related work touches many groups at UVA, but has concentrations in the Link Lab, the Center for Engineering in Medicine, and the Cyber Innovation and Society Group.

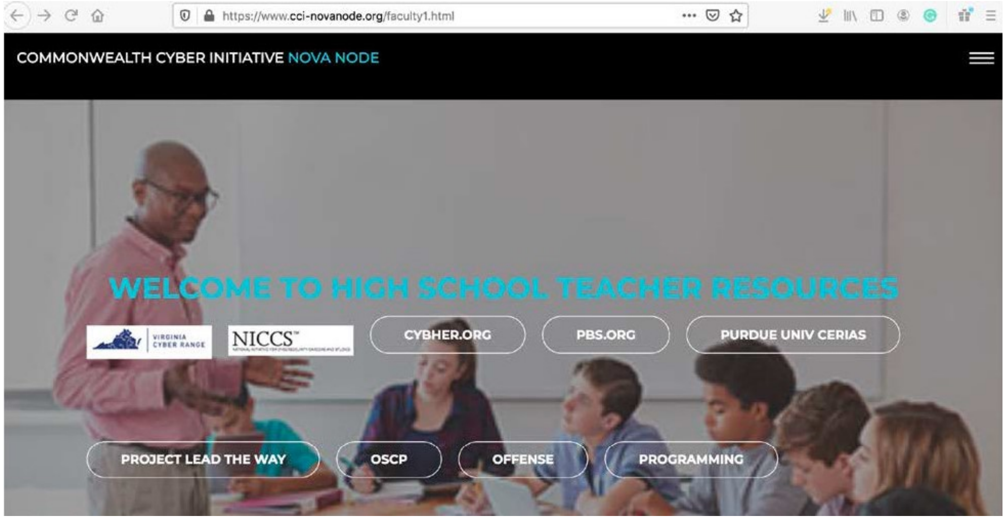

https://www.cci-novanode.org/faculty1.html
COMMONWEALTH CYBER INITIATIVE NOVA NODE
WELCOME TO HIGH SCHOOL TEACHER RESOURCES
VIRGINIA CYBER RANGE
NICCS
CYBHER.ORG
PBS.ORG
PURDUE UNIV CERIAS
PROJECT LEAD THE WAY
OSCP
OFFENSE
PROGRAMMING

Figure 2.25: The NoVA Node website is a training and educational resource for teachers.

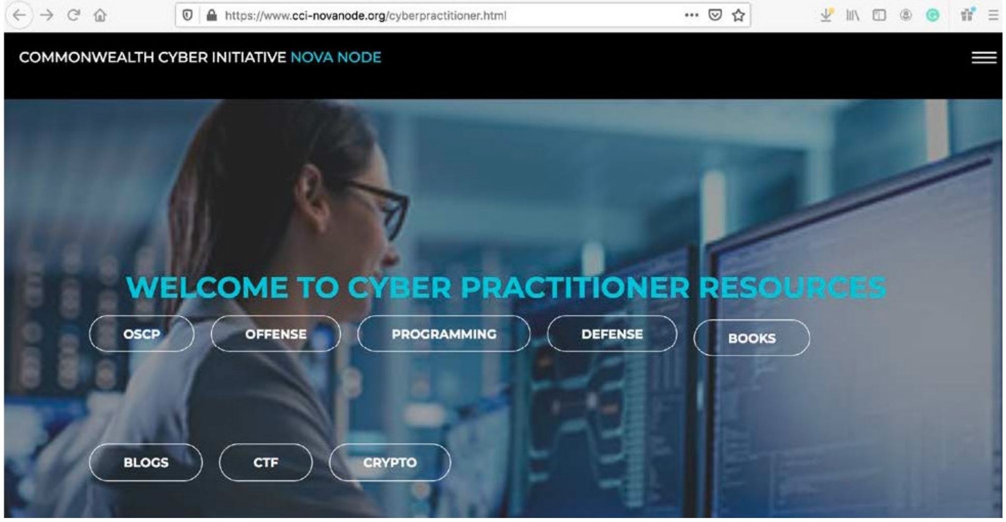

https://www.cci-novanode.org/cyberpractitioner.html
COMMONWEALTH CYBER INITIATIVE NOVA NODE
WELCOME TO CYBER PRACTITIONER RESOURCES
OSCP
OFFENSE
PROGRAMMING
DEFENSE
BOOKS
BLOGS
CTF
CRYPTO

Figure 2.26: The NoVA Node website provides additional training resources for cyber practitioners.

Governance and Partnerships

Higher education institutions in the Central VA Node include: Virginia Commonwealth University, University of Virginia, Virginia State University, Virginia Union University, Longwood University, Piedmont Virginia Community College, John Tyler Community College, and J Sergeant Reynolds Community College.

The Central VA Node leadership team is comprised of:

- Dr. Erdem Topsakal, Chair and Professor, Department of Electrical and Computer Engineering, College of Engineering, VCU (Node Executive Director);
- Susan L.R. Barker, Associate Dean of Research, UVA (Node Cochair);
- Gregory Triplett, Senior Associate Dean for Academic Affairs, VCU (Node Co-Chair).

The CeVA node has also formed a Leadership Council and Technical Advisory Board. Members include:

Erdem Topsakal (VCU), Susan Barker (UVA), Michael Straightiff (UVA), Peter Beiling (UVA), Gregory Triplett (VCU), Milos Malic (VCU), Sherif Abdelwahed (VCU), John Leonard (VCU), Paul Rocheleau (VCU), Krys Cios (VCU), Travis Hyte (UVA), Scott Barker (UVA), Bobby Keener (VDE), Kenn Spedden (AI Research), Robert Powell (NASA), Helen Cauthen (CVPED), Donald Palm (VSU), Nibir Dhar (Night Vision), and Michael Mancini (VCU).

Business Partners include: Bank of America, Capital One, Amazon Web Services, Inc., Booz Allen Hamilton, CoStar Group, Dominion Energy, IBM, Fannie Mae, Micron, Leidos, Rockwell, MITRE, Northrop Grumman, SRC, Willow Tree, Battelle Energy Alliance.

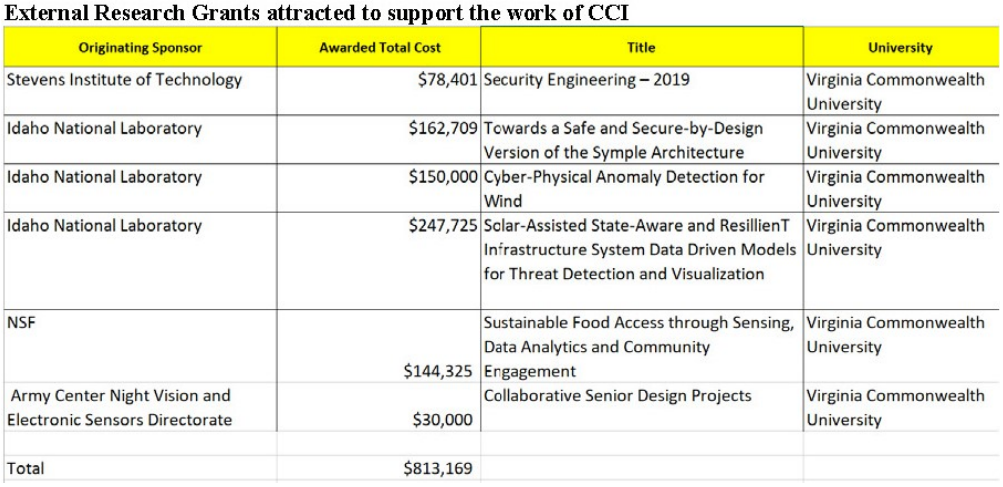
Additional partners include:

- Government: NASA, DoD, Virginia Department of Education, Idaho National Laboratory, Oak Ridge National Laboratory, DoE;
- Economic Development: Virginia Cybersecurity Partnership, Central Virginia Partnership for Economic Development.
- Non-profits: International Science and Technology, Smart Cville.

2.3.2 Report on the Seven Requirements as per Item 135, Chapter 1289, HB30

External Research Grants attracted to support the work of CCI

The CeVA Node attracted $813K in external research grants at VCU to support the work of CCI (detailed list of research grants in Figure 2.27). An additional $9.9M in external funding was attracted at UVA to support the work of CCI (see the list of research grants in Figures 2.28 to 2.31). The total external research funding in the CeVA Node in FY20 was $10.7M.



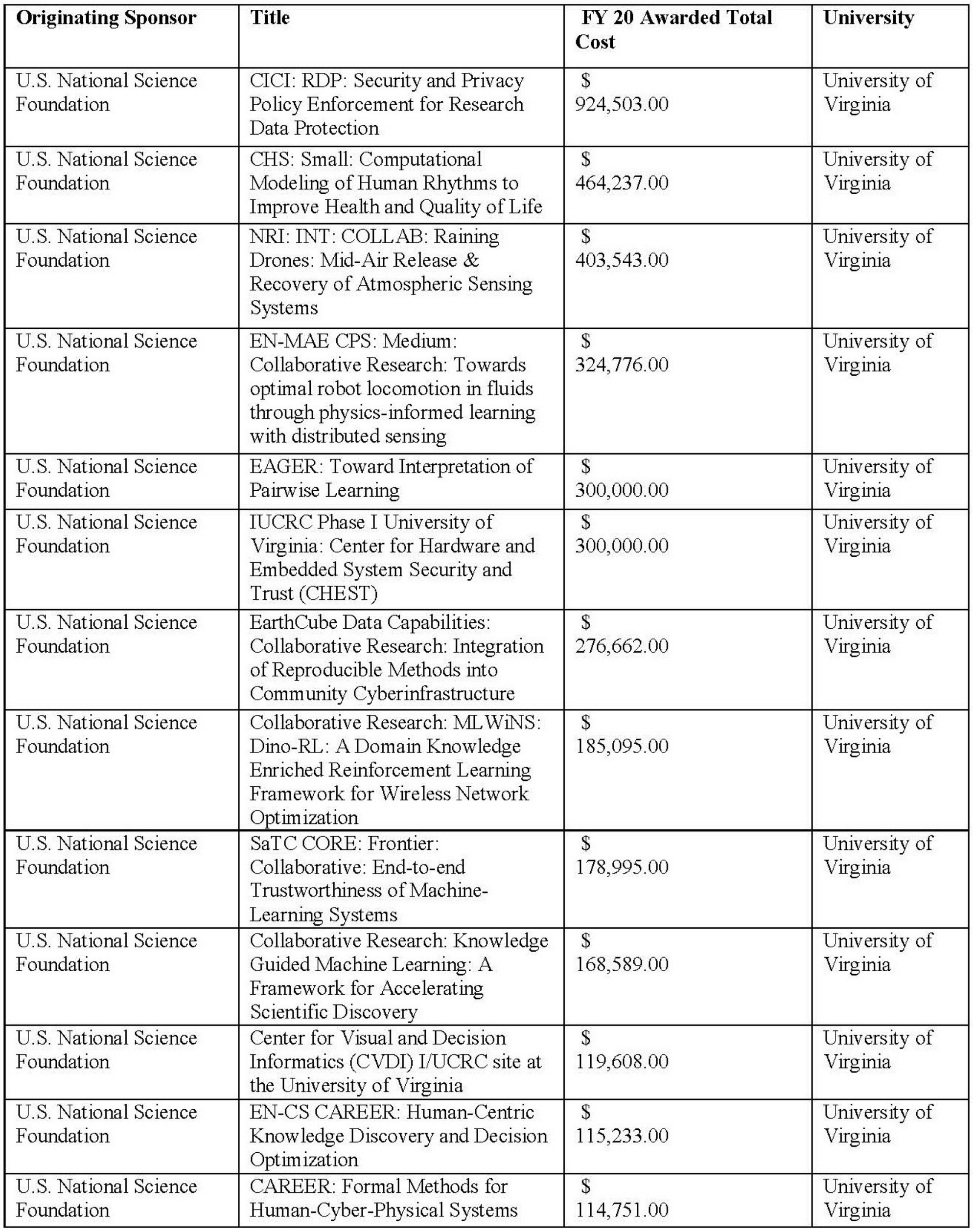
External Research Grants attracted to support the work of CCI

Originating Sponsor	Awarded Total Cost	Title	University
Stevens Institute of Technology	$78,401	Security Engineering – 2019	Virginia Commonwealth University
Idaho National Laboratory	$162,709	Towards a Safe and Secure-by-Design Version of the Symple Architecture	Virginia Commonwealth University
Idaho National Laboratory	$150,000	Cyber-Physical Anomaly Detection for Wind	Virginia Commonwealth University
Idaho National Laboratory	$247,725	Solar-Assisted State-Aware and ResillienT Infrastructure System Data Driven Models for Threat Detection and Visualization	Virginia Commonwealth University
NSF	$144,325	Sustainable Food Access through Sensing, Data Analytics and Community Engagement	Virginia Commonwealth University
Army Center Night Vision and Electronic Sensors Directorate	$30,000	Collaborative Senior Design Projects	Virginia Commonwealth University
Total	$813,169		

Figure 2.27: FY20 external research grants attracted to support the work of CCI.

Research Grants awarded from the funds contained in HB30

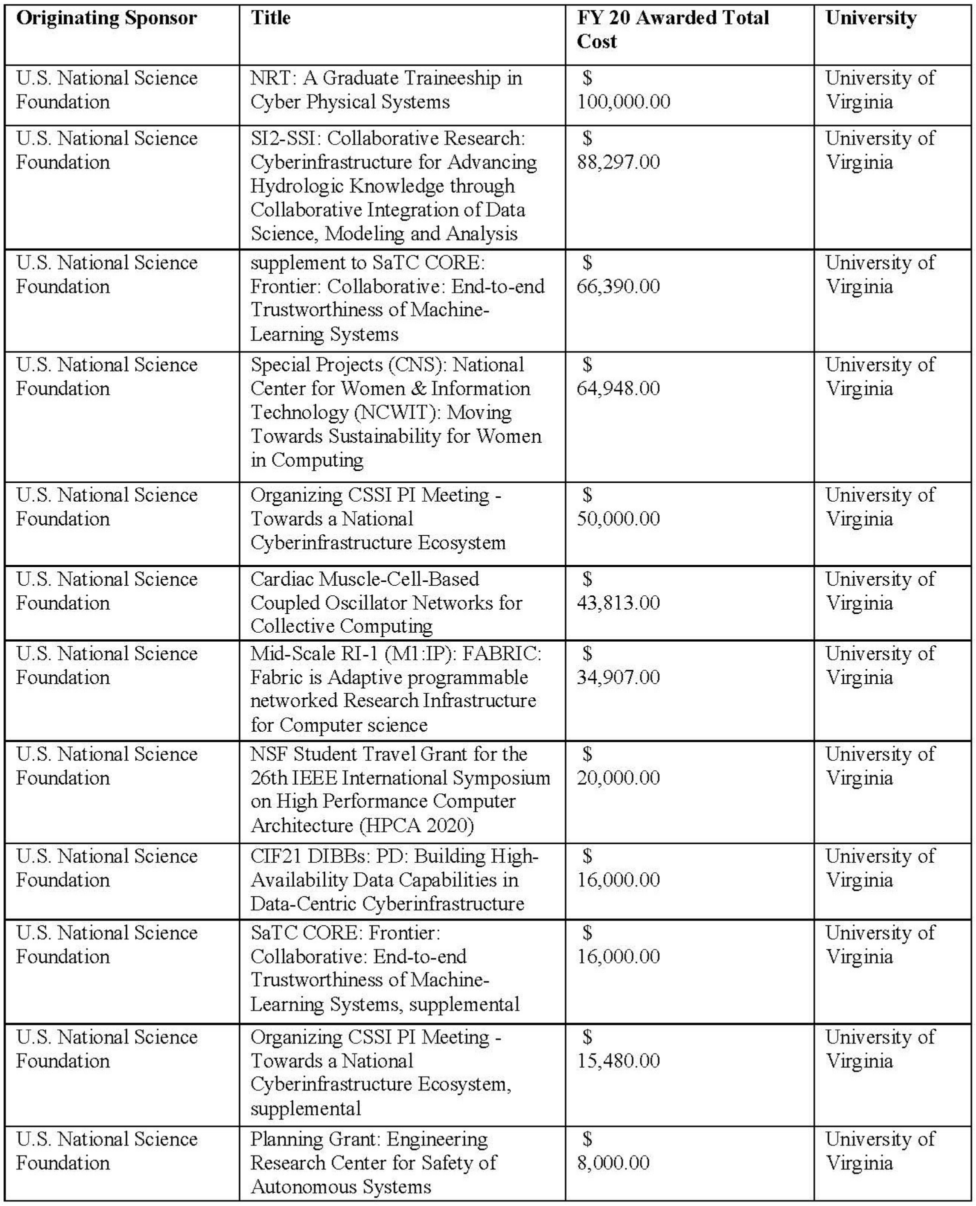
UVA Engineering provided cost shared FY20 resources for research efforts impacting the mission of CCI. UVA Engineering awarded internal grants to promote new research ideas, support proposal development,



Originating Sponsor	Title	FY 20 Awarded Total Cost	University
U.S. National Science Foundation	CICI: RDP: Security and Privacy Policy Enforcement for Research Data Protection	$ 924,503.00	University of Virginia
U.S. National Science Foundation	CHS: Small: Computational Modeling of Human Rhythms to Improve Health and Quality of Life	$ 464,237.00	University of Virginia
U.S. National Science Foundation	NRI: INT: COLLAB: Raining Drones: Mid-Air Release & Recovery of Atmospheric Sensing Systems	$ 403,543.00	University of Virginia
U.S. National Science Foundation	EN-MAE CPS: Medium: Collaborative Research: Towards optimal robot locomotion in fluids through physics-informed learning with distributed sensing	$ 324,776.00	University of Virginia
U.S. National Science Foundation	EAGER: Toward Interpretation of Pairwise Learning	$ 300,000.00	University of Virginia
U.S. National Science Foundation	IUCRC Phase I University of Virginia: Center for Hardware and Embedded System Security and Trust (CHEST)	$ 300,000.00	University of Virginia
U.S. National Science Foundation	EarthCube Data Capabilities: Collaborative Research: Integration of Reproducible Methods into Community Cyberinfrastructure	$ 276,662.00	University of Virginia
U.S. National Science Foundation	Collaborative Research: MLWiNS: Dino-RL: A Domain Knowledge Enriched Reinforcement Learning Framework for Wireless Network Optimization	$ 185,095.00	University of Virginia
U.S. National Science Foundation	SaTC CORE: Frontier: Collaborative: End-to-end Trustworthiness of Machine-Learning Systems	$ 178,995.00	University of Virginia
U.S. National Science Foundation	Collaborative Research: Knowledge Guided Machine Learning: A Framework for Accelerating Scientific Discovery	$ 168,589.00	University of Virginia
U.S. National Science Foundation	Center for Visual and Decision Informatics (CVDI) I/UCRC site at the University of Virginia	$ 119,608.00	University of Virginia
U.S. National Science Foundation	EN-CS CAREER: Human-Centric Knowledge Discovery and Decision Optimization	$ 115,233.00	University of Virginia
U.S. National Science Foundation	CAREER: Formal Methods for Human-Cyber-Physical Systems	$ 114,751.00	University of Virginia

Figure 2.28: FY20 UVA engineering sponsored funding topically related to CCI (list 1 of 4).

and bridge efforts between research and implementation in the areas of cyber-physical systems, machine learning, and related technologies. Example topics included smart watch technologies to improve hand hygiene practices, autonomous bridge inspection, privacy-preserving machine learning, and improved decision making for safety-critical intelligent cognitive assistants. In addition, via the Center for Engineering in Medicine, UVA funded research projects pairing professionals from Engineering and the School of Medicine including CCI relevant projects such as mobile sensing related to kidney disease, and robotic surgery training. Outcomes from these projects are being leveraged toward external funding and expanded efforts in FY21.



Originating Sponsor	Title	FY 20 Awarded Total Cost	University
U.S. National Science Foundation	NRT: A Graduate Traineeship in Cyber Physical Systems	$ 100,000.00	University of Virginia
U.S. National Science Foundation	SI2-SSI: Collaborative Research: Cyberinfrastructure for Advancing Hydrologic Knowledge through Collaborative Integration of Data Science, Modeling and Analysis	$ 88,297.00	University of Virginia
U.S. National Science Foundation	supplement to SaTC CORE: Frontier: Collaborative: End-to-end Trustworthiness of Machine-Learning Systems	$ 66,390.00	University of Virginia
U.S. National Science Foundation	Special Projects (CNS): National Center for Women & Information Technology (NCWIT): Moving Towards Sustainability for Women in Computing	$ 64,948.00	University of Virginia
U.S. National Science Foundation	Organizing CSSI PI Meeting - Towards a National Cyberinfrastructure Ecosystem	$ 50,000.00	University of Virginia
U.S. National Science Foundation	Cardiac Muscle-Cell-Based Coupled Oscillator Networks for Collective Computing	$ 43,813.00	University of Virginia
U.S. National Science Foundation	Mid-Scale RI-1 (M1:IP): FABRIC: Fabric is Adaptive programmable networked Research Infrastructure for Computer science	$ 34,907.00	University of Virginia
U.S. National Science Foundation	NSF Student Travel Grant for the 26th IEEE International Symposium on High Performance Computer Architecture (HPCA 2020)	$ 20,000.00	University of Virginia
U.S. National Science Foundation	CIF21 DIBBs: PD: Building High-Availability Data Capabilities in Data-Centric Cyberinfrastructure	$ 16,000.00	University of Virginia
U.S. National Science Foundation	SaTC CORE: Frontier: Collaborative: End-to-end Trustworthiness of Machine-Learning Systems, supplemental	$ 16,000.00	University of Virginia
U.S. National Science Foundation	Organizing CSSI PI Meeting - Towards a National Cyberinfrastructure Ecosystem, supplemental	$ 15,480.00	University of Virginia
U.S. National Science Foundation	Planning Grant: Engineering Research Center for Safety of Autonomous Systems	$ 8,000.00	University of Virginia

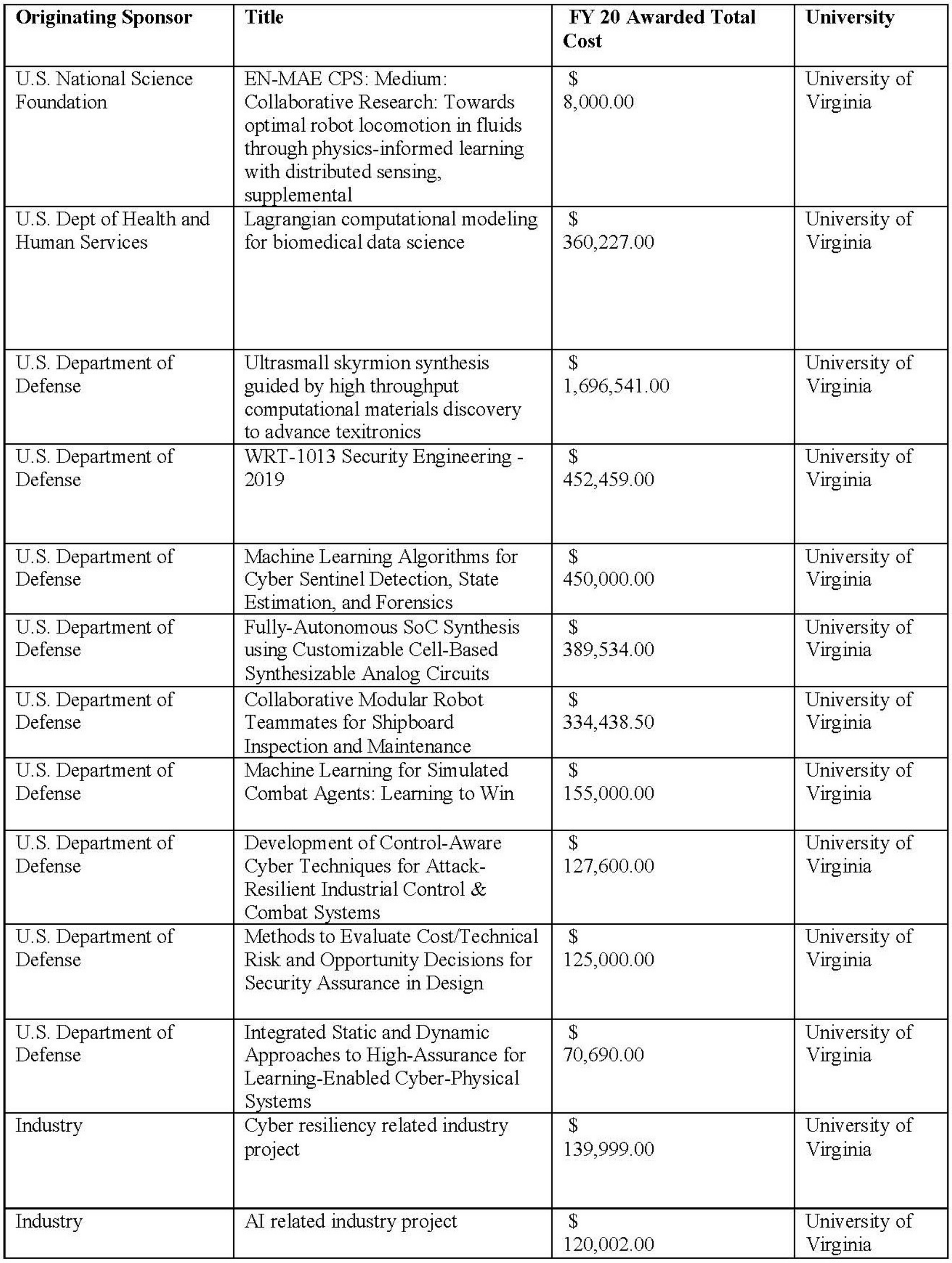
Figure 2.29: FY20 UVA engineering sponsored funding topically related to CCI (list 2 of 4).

Research Faculty Recruited

UVA recruited a number of new faculty in FY20 in the CCI research focus areas. These are listed in Figure 2.32.

Results of Entrepreneurship and Workforce programming

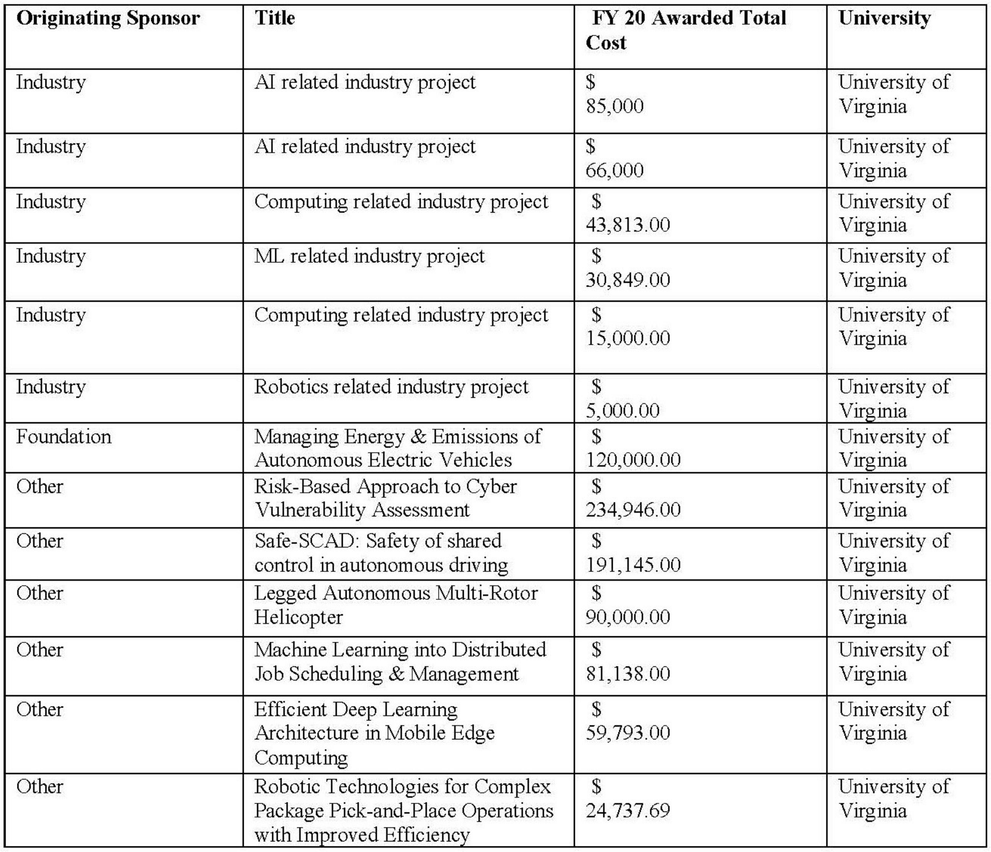
Among the entrepreneurship and workforce programming activities that involve the CCI CeVA Node researchers were:



Originating Sponsor	Title	FY 20 Awarded Total Cost	University
U.S. National Science Foundation	EN-MAE CPS: Medium: Collaborative Research: Towards optimal robot locomotion in fluids through physics-informed learning with distributed sensing, supplemental	$ 8,000.00	University of Virginia
U.S. Dept of Health and Human Services	Lagrangian computational modeling for biomedical data science	$ 360,227.00	University of Virginia
U.S. Department of Defense	Ultrasmall skyrmion synthesis guided by high throughput computational materials discovery to advance texitronics	$ 1,696,541.00	University of Virginia
U.S. Department of Defense	WRT-1013 Security Engineering - 2019	$ 452,459.00	University of Virginia
U.S. Department of Defense	Machine Learning Algorithms for Cyber Sentinel Detection, State Estimation, and Forensics	$ 450,000.00	University of Virginia
U.S. Department of Defense	Fully-Autonomous SoC Synthesis using Customizable Cell-Based Synthesizable Analog Circuits	$ 389,534.00	University of Virginia
U.S. Department of Defense	Collaborative Modular Robot Teammates for Shipboard Inspection and Maintenance	$ 334,438.50	University of Virginia
U.S. Department of Defense	Machine Learning for Simulated Combat Agents: Learning to Win	$ 155,000.00	University of Virginia
U.S. Department of Defense	Development of Control-Aware Cyber Techniques for Attack-Resilient Industrial Control & Combat Systems	$ 127,600.00	University of Virginia
U.S. Department of Defense	Methods to Evaluate Cost/Technical Risk and Opportunity Decisions for Security Assurance in Design	$ 125,000.00	University of Virginia
U.S. Department of Defense	Integrated Static and Dynamic Approaches to High-Assurance for Learning-Enabled Cyber-Physical Systems	$ 70,690.00	University of Virginia
Industry	Cyber resiliency related industry project	$ 139,999.00	University of Virginia
Industry	AI related industry project	$ 120,002.00	University of Virginia

Figure 2.30: FY20 UVA Engineering sponsored funding topically related to CCI (list 3 of 4).

- SustainLab VIP team – This Vertically Integrated Projects (VIP) team has operated continuously since Spring 2017 and has involved students from Biology, Art, and Engineering. Projects have included design and construction of green walls at VCU and at Lakeside Elementary School, construction of instrumentation and data collection for Urban Heat Island study, construction and deployment of air quality sensors, and design and construction of urban agriculture systems.
- Medical Device Development and Prototyping - This VIP team has been active since 2016 and accommodates 12-20 undergraduate and graduate students each year. The projects include design and development of wireless medical telemetry devices and sensors. The main focus is in implantable systems.



Originating Sponsor	Title	FY 20 Awarded Total Cost	University
Industry	AI related industry project	$ 85,000	University of Virginia
Industry	AI related industry project	$ 66,000	University of Virginia
Industry	Computing related industry project	$ 43,813.00	University of Virginia
Industry	ML related industry project	$ 30,849.00	University of Virginia
Industry	Computing related industry project	$ 15,000.00	University of Virginia
Industry	Robotics related industry project	$ 5,000.00	University of Virginia
Foundation	Managing Energy & Emissions of Autonomous Electric Vehicles	$ 120,000.00	University of Virginia
Other	Risk-Based Approach to Cyber Vulnerability Assessment	$ 234,946.00	University of Virginia
Other	Safe-SCAD: Safety of shared control in autonomous driving	$ 191,145.00	University of Virginia
Other	Legged Autonomous Multi-Rotor Helicopter	$ 90,000.00	University of Virginia
Other	Machine Learning into Distributed Job Scheduling & Management	$ 81,138.00	University of Virginia
Other	Efficient Deep Learning Architecture in Mobile Edge Computing	$ 59,793.00	University of Virginia
Other	Robotic Technologies for Complex Package Pick-and-Place Operations with Improved Efficiency	$ 24,737.69	University of Virginia

Figure 2.31: FY20 UVA Engineering sponsored funding topically related to CCI (list 4 of 4).

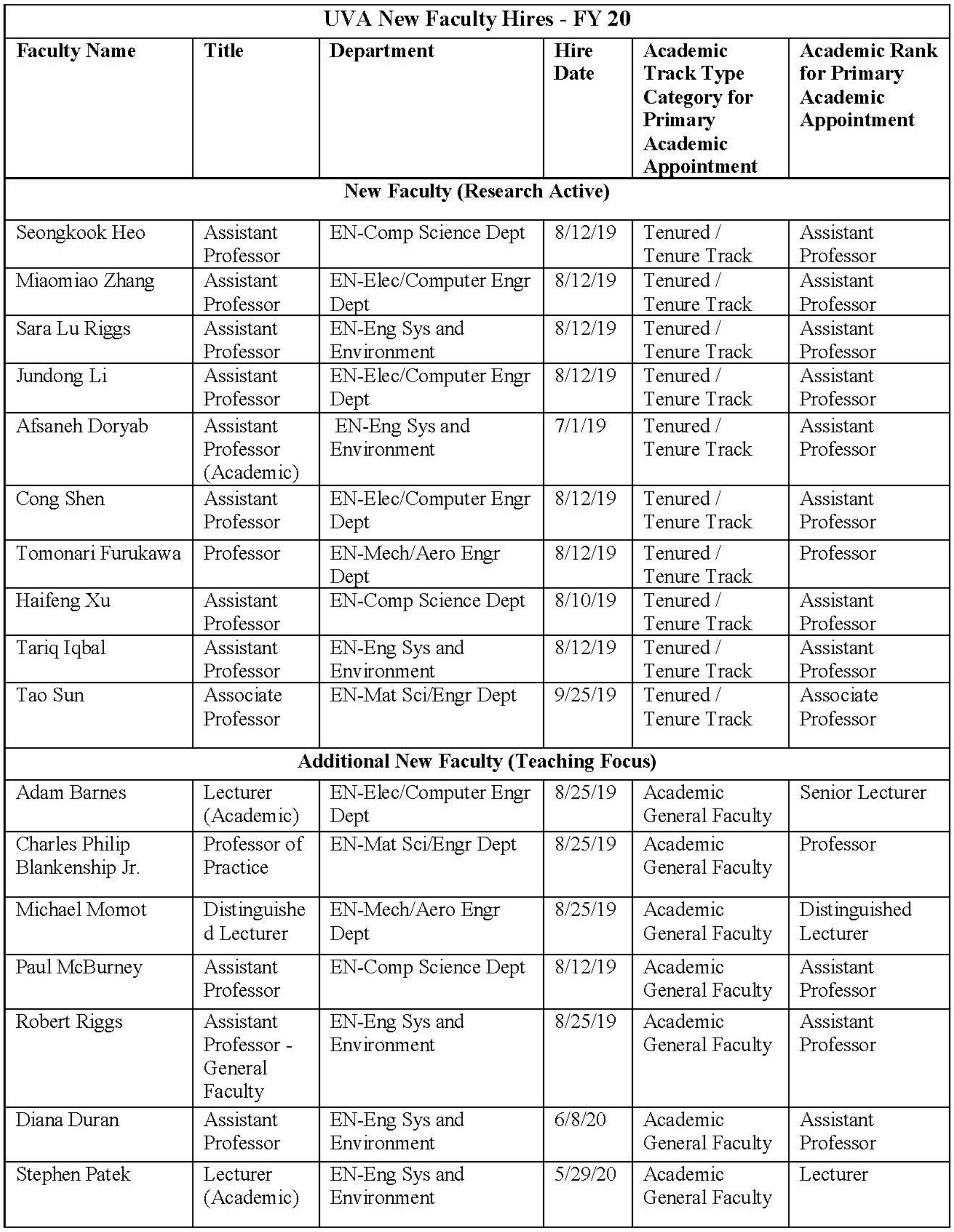
- Training in the Integration of Cyber Physical Systems and Security: A CeVA Node team recently was awarded a grant for experiential learning from the CCI Hub. The main objectives for this proposed CPS experiential learning program under the CCI are: to package three newly developed UVA CPS classes for dissemination to other CCI colleges and universities; to develop and package hands-on labs for each of these classes; to identify the first group of schools to use one of more of the class and lab materials and support transferring the materials to them; and to support undergraduate underrepresented minorities as summer interns.

Engineering Career Development

The UVA Engineering Career Development office expanded in FY20, hiring a new full-time position focused on 1:1 student advising and organizing workshops on important topics in the tech industry. These include "What the Tech?" (a panel of UVA alumni in tech), a "Getting Started with GitHub" workshop, and technical interviewing workshops. For the 2020 Academic Year, this position completed over 230 student appointments. This position was also the co-lead for a new class series titled "Careers in Computing" that is geared towards first and second year students at UVA with an interest in computing majors and careers.

Over a 6-week period, UVA Engineering hosted employers to share with students about different career options in computing, and answer students' questions about computing careers. These efforts will continue and be expanded for FY21.

The UVA Engineering Career Development office piloted a new program called "Skilled" to help students practice their technical interviewing skills. Funding provided by the office enabled students to conduct



UVA New Faculty Hires - FY 20					
Faculty Name	**Title**	**Department**	**Hire Date**	**Academic Track Type Category for Primary Academic Appointment**	**Academic Rank for Primary Academic Appointment**
New Faculty (Research Active)					
Seongkook Heo	Assistant Professor	EN-Comp Science Dept	8/12/19	Tenured / Tenure Track	Assistant Professor
Miaomiao Zhang	Assistant Professor	EN-Elec/Computer Engr Dept	8/12/19	Tenured / Tenure Track	Assistant Professor
Sara Lu Riggs	Assistant Professor	EN-Eng Sys and Environment	8/12/19	Tenured / Tenure Track	Assistant Professor
Jundong Li	Assistant Professor	EN-Elec/Computer Engr Dept	8/12/19	Tenured / Tenure Track	Assistant Professor
Afsaneh Doryab	Assistant Professor (Academic)	EN-Eng Sys and Environment	7/1/19	Tenured / Tenure Track	Assistant Professor
Cong Shen	Assistant Professor	EN-Elec/Computer Engr Dept	8/12/19	Tenured / Tenure Track	Assistant Professor
Tomonari Furukawa	Professor	EN-Mech/Aero Engr Dept	8/12/19	Tenured / Tenure Track	Professor
Haifeng Xu	Assistant Professor	EN-Comp Science Dept	8/10/19	Tenured / Tenure Track	Assistant Professor
Tariq Iqbal	Assistant Professor	EN-Eng Sys and Environment	8/12/19	Tenured / Tenure Track	Assistant Professor
Tao Sun	Associate Professor	EN-Mat Sci/Engr Dept	9/25/19	Tenured / Tenure Track	Associate Professor
Additional New Faculty (Teaching Focus)					
Adam Barnes	Lecturer (Academic)	EN-Elec/Computer Engr Dept	8/25/19	Academic General Faculty	Senior Lecturer
Charles Philip Blankenship Jr.	Professor of Practice	EN-Mat Sci/Engr Dept	8/25/19	Academic General Faculty	Professor
Michael Momot	Distinguishe d Lecturer	EN-Mech/Aero Engr Dept	8/25/19	Academic General Faculty	Distinguished Lecturer
Paul McBurney	Assistant Professor	EN-Comp Science Dept	8/12/19	Academic General Faculty	Assistant Professor
Robert Riggs	Assistant Professor - General Faculty	EN-Eng Sys and Environment	8/25/19	Academic General Faculty	Assistant Professor
Diana Duran	Assistant Professor	EN-Eng Sys and Environment	6/8/20	Academic General Faculty	Assistant Professor
Stephen Patek	Lecturer (Academic)	EN-Eng Sys and Environment	5/29/20	Academic General Faculty	Lecturer

Figure 2.32: UVA new faculty hires.

technical interviews virtually with a tech: https://www.skilledinc.com. This tool will continue to be piloted to students in FY21.

Corporate Engagement and Collaboration

There continues to be a tremendous amount of interest from companies in interacting with and recruiting UVA Engineering CCI related students. UVA won the National Collegiate Cyber Defense Competition for the third year in a row. This has helped create additional buzz around our students and generated new partners. The annual student-led hackathon moved to being fully virtual which enabled participation to grow to 800+ students. UVA Engineering corporate partners play an important role mentoring student projects over the weekend-long hackathon event. Additionally, UVA's annual Tech Night Takeover event attracted 30+ tech companies, helping 200+ students with technical interviewing ahead of the career fair.

As UVA Engineering looks to broaden the interaction between industry and students, expanding the partnership programs with our corporate partners has been an increased focus. UVA Engineering added five new corporate partners. Having these partnerships on board facilitates research engagement, and helps support development activities for students as well as increased internship and full-time recruitment options with companies, especially those local to Virginia. Growth of corporate engagement will continue to be a focus for FY21.

Collaborative partnerships and projects

Development of Robust Materials for Nanoscale Security

Security features, used to authenticate bank notes, passports, identity cards, legal documents, have become an indispensable part of our society, to an extent where the market for security features is estimated to reach $25 billion by 2026. Amongst the several methods available, watermarks and holograms are the most widely used form of security feature, primarily due to their low manufacturing cost but at the expense of easy reproducibility. While for most applications this security would suffice, certain areas, such as legal documents and identity cards, could benefit from more secure security features.

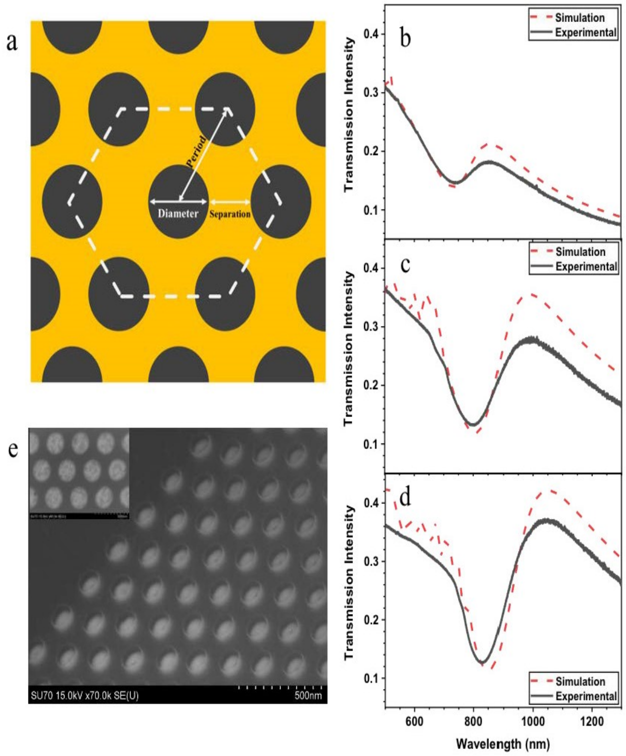
Figure 2.33: Titanium nitride thin films grown on sapphire.

Nanophotonics offers an opportunity to accomplish this. In particular, when a metal is patterned on the nanoscale it can produce a range of colors that are different from its normal appearance. This is a promising technique for high-security systems, as an exact reproduction of the nanoscale pattern is almost impossible due to the random variations inherent in nanoscale growth and fabrication. Moreover, it would require multi-million-dollar fabrication tools and facilities in combination with precise material growth methods and nanofabrication processes. Despite benefits, practical applications are limited largely by the cost and robustness of the typical materials used - silver, gold or aluminum. Here we seek to alleviate this issue, realizing a scalable, low cost, and industrially friendly fabrication process for robust metals.

We have focused on titanium nitride (TiN), a promising alternative material providing exceptional durability. With a young's modulus of up to 400 GPa (5 times that of silver), and a 9 on the Moh's hardness scale (0 to 10, while silver is 2.5), which denotes the scratch resistance of a material, TiN is an attractive choice for security devices on heavily handled objects such as bills, labels identity cards and legal documents. However, high quality TiN has usually been grown via sputtering at temperatures exceeding $650°C$, which renders the process incompatible with most standard lithographic processes. Through this work we have optimized an atomic layer deposition process capable of producing thin films with nanometer accuracy over inch-square areas. Our process has produced a material that is the highest performing TiN film in literature using ALD (see Figure 2.33), and is achieved at deposition temperatures half of previous techniques. Together this allows a low-cost, scalable, and practical approach to realizing robust metallic security devices. This work was published as: D. Fomra et al., "Plasmonic Titanium Nitride via Atomic Layer Deposition: A Low-Temperature Route," J. Appl. Phys., vol. 127, no. 10, pp. 1–16, Mar. 2020.

Plasmonic Color for Robust Covert Security Stamps

Making use of the leading TiN films already developed, preliminary work to realize the first security stamp has begun. In particular, simulations and designs of the necessary nanoscale pattern required to produce a range of colors has been completed (see Figure 2.34) including initial fabrication runs and test data. The resulting nanohole array exhibits polarization independent and angle insensitive (+/- 10) plasmonic colors in the visible and short-wave infrared spectral region, accessible by inexpensive Si based charge coupled device detectors (Figure 2.34 b, c, d and e). More importantly though, the TiN nanohole array exhibits vastly improved durability and scratch resistance, demonstrating promise for use in security applications such as identity cards and legal documents.



(a) Schematic of the nanhole array, (b), (c) and (d) Simulated and experimentally measured transmission spectra of three representative structures with a radius of 75 nm, 125 nm, 150 nm and separation between the holes of 200 nm with EOT peaks positioned at 800 nm, 1000 nm and 1050 nm, respectively, (e) SEM image of the nanohole array.

Figure 2.34: Nanohole array and transmission spectra of three representative structures.

Vertically Integrated Projects: Telecommunications Team

Teaching efforts have also expanded through the help of CCI over the last year. During the 2019-2020 academic year, a new sub-team to the Optics and Photonics VIP team was created, focused on the development of a high-speed test bench for nanoscale secure and integrated telecommunications systems. As a key economic area in the state of Virginia, growth of the workforce for telecommunications and data centers is critical over the next several decades. This team is gaining invaluable hands-on experience learning the foundational principles of modern optical communications networks, data centers, and the areas in need of research advancement. Specifically, the team is working to research, design, and build from scratch a cutting-edge test bench that blends programming of integrated systems, high-frequency RF (¿40 GHz signals), fiber optics, and integrated nanophotonics into a single project. Their goal is to realize a custom system capable of interrogating nanophotonic devices measuring key metrics of their performance such as bit-error-rate, modulation depth, energy consumption, and more. Undergraduate students participating in the team are working side-by-side with PhD students to complete the project and currently represent students from sophomore to senior in standing.

In addition to pursuing continued research endeavors, through the CCI program we have an opportunity to continue to grow the program in nanophotonics and optical materials for secure devices and systems. Through this we have begun the process of hiring a Research Scientist to aid in the expansion of our research efforts and externally funded programs, train students and guide experimental efforts in the lab, as well as continue the development and expansion of our lab space at VCU. More than 15 applications were received for the position and we are in the final stages of negotiations with the candidate. Furthermore, through the help of CCI the optical lab space at VCU has been expanded to include a hybrid research/teaching space enabling us to continue to develop and improve our high school, undergraduate and graduate programs in optics. Specifically, this includes planned development of a hands-on experimental optics course as well as the addition of new laboratory components to numerous classes in the VCU curriculum. Moreover, the expansion provides a dedicated space for the VCU Optics and Photonics VIP team to perform tackle their research projects in laser characterization systems, acoustic metamaterials, and high-speed telecommunications.

Multi-monitor Runtime Verification in support of Smart Cities

This work started out as partially funded by EPRI. We have begun to move it in the direction of more open applications such as smart cities, autonomous vehicles, and avionics. There is a need for monitoring city states in real-time to ensure safety and performance requirements. If a requirement violation is detected by the monitor, the smart infrastructure service providers can take actions to change the evolving problems, such as improving traffic performance, rejecting unsafe actions, sending alarms to first responders, etc. The key challenges of developing such a monitor include how to use an expressive, machine-understandable language to specify smart city requirements, and how to efficiently monitor requirements that may involve multiple sensor data streams. We have been developing a multi-monitor framework based on TeSSla - streaming metric temporal logic developed by University of Luebeck. The key challenges to date are examining the expressiveness of TeSSla to capture unusual smart city performance and safety requirements. These requirements are not only based on logic and time, but spatial properties too. Example, “there should be no more than 30% traffic congestion on roads in the northeast direction of short pump at 11am”. The second issue is implementation of these monitors: they should be synthesizable directly from the language into C or VHDL.

CYBOK - A Cyber Body of Knowledge vulnerability assessment tool

To manage cyber risk, we must start assessing security threats as early as possible in a system’s lifecycle and then throughout with the use of models. We advocate the use of system models to support life cycle development. Such models should be augmented to be a living artifact of security considerations in addition to design choices, but often they do not consider any security information. The main problem this work addresses is how to design tools that find relevant attack vectors on a system when the only available description is design documents. This is particularly difficult because a large number of security tools used in the industry are assuming a realized system. CYBOK is a tool that associates NIST/MITRE cyber vulnerability and attack pattern databases to models of a system captured in SysML. In doing so, we can provide early feedback on the cyber security posture of a system before substantial design investment in the system. The tool is publicly available and can be licensed from VCU.

Attacker Modeling

Characterizing attacker behavior with respect to Cyber-Physical Systems is important to assuring the security posture and resilience of these systems. Classical cyber vulnerability assessment approaches rely on the knowledge and experience of cyber-security experts to conduct security analyses and can be inconsistent where the experts’ knowledge and experience are lacking. This work has built a exible attacker modeling framework that aids in the security analysis process by simulating a diverse set of attacker behaviors to predict attack progression and provide consistent system vulnerability analysis. The model proposes an expanded architecture of vulnerability databases to maximize its effectiveness and consistency in detecting

CPS vulnerabilities while being compatible with existing vulnerability databases.

Urban Heat Island Consortium

This study focused in measuring location-based surface temperatures to identify temperature variations across the city of Richmond associated with differences in the built environment. Partners include: Science Museum of Virginia, Groundwork RVA, University of Richmond, Portland State University.

Richmond OpenAir Project

This ongoing project has a goal of deploying a city-wide network of air quality sensors for continuous monitoring of air quality in the Richmond metropolitan area through construction, calibration, and deployment of sensors. Work on this project has been support by a grant from VCU Service Learning and a grant to the Science Museum of Virginia from the Institute of Museum and Library Sciences. Partners include: Science Museum of Virginia, University of Richmond, Virginia Union University, Virginia Department of Environmental Quality.

Urban Agriculture/Food Systems

Partners for this project include: BeautifulRVA, Virginia Department of Health, University of Virginia (The Equity Center), Fairfield Middle School, The Market at 25th Street, VCU Health Hub, Chesterfield County. The project includes three strands:

1. Food production – This ongoing project focuses on the design, construction, and scaling of local production of vegetables. Systems are designed, constructed, and used to grow a variety of healthy produce (microgreens, leafy greens, tomatoes, carrots, etc). Proposals have been submitted to the VCU REAL Challenge Initiative and the Southern Region Sustainable Agriculture Research and Education Program.
2. Land Evaluation and Site Assessment (LESA) – This ongoing project uses Geographic Information System (GIS) layers to suggest suitable locations for urban green space and urban agriculture. Proposal is in preparation to the USDA Office of Urban Agriculture.
3. The Role of Smart Technology in Improving Sustainable Food System - The goal is to investigate the role of the latest technologies/techniques available in the world in improving sustainable food system management. Some research activities related to this item include: new technologies for food delivery/transportation; new techniques for food waste management; smart farming/smart agriculture using smart technologies for collecting data; machine learning applications for optimal growing conditions and maximizing desired features; new techniques (for production, distribution, transportation, waste reduction, storage, etc.) with less environmental impact.

Smart health and the impact of connected devices enabling active and engaged patient users and expanding healthcare

Our work in smart health is currently aimed at developing in-body and on-body sensor systems for monitoring health and well-being. We are designing mechanically flexible, conformable biosensors that can be used at biointerfaces to measure various biomarkers relevant to human health. These include physical parameters such as temperature and biochemical targets such as glucose (diabetes patients) and ascorbate (sepsis patients). Of current interest is the integration of wireless telemetry (e.g. printed antennas or Radio Frequency Identification (RFID)) in the sensor systems for remote monitoring and telemedicine. Material and system design in support of this aim is focused on issues of sustainability and the use of bioderived and biodegradable materials for device fabrication.

Testbed Development

Two testbeds are currently under development at the CCI CeVA Node as described below. Both testbeds will be up and running in the spring of 2021.

- Smart City 5G-IoT Testbed (CyberWorld): A smart city is, in simplest terms, a coordinated implementation of IoT technology and data analytics in an urban environment to improve the health, safety, and quality of life for inhabitants. This is possible through innovative applications of many technologies that are currently in widespread use. The smart city lab focuses on the utilization of model-based control and machine learning to achieve efficient management of complex, smart, and autonomous systems. To accomplish this, the proposed testbed is designed as practical implementation of current research around smart buildings, intelligent control systems, autonomous vehicles, and other areas critical to urban living. Designed for future expansion, the modular design is composed of multiple city blocks with buildings designated for purposes such as offices, homes, manufacturing, and parking. These model buildings are created to be integrated with sensors and actuators to mimic true-to-life smart buildings. Operating these buildings are intelligent controllers that will learn the optimal conditions of the building and its residents in order to improve resource utilization, security, and comfort. Usage of intelligent controllers and machine learning allows for flexibility of location and building design without sacrificing customization options. Between these buildings are roads for scale-model autonomous vehicles that will navigate the city based on on-board sensors. An intelligent, adaptable traffic control system will be used to direct autonomous vehicles based on dynamically collected data on city conditions. In order to improve the robustness of the testing environment, a motion capture system is implemented to track all components of the smart city testbed. This system is used to replicate GPS coordinates for autonomous vehicle navigation.

  Figure 2.35 shows the initial design drawing of the CyberWorld modules. CyberWorld is composed of modular tiles that will house individual buildings such as businesses, schools, factories, highways, parks, railways etc. The CyberWorld will allow the research in autonomous infrastructures and vehicles using 5G/IoT technologies. VCU will also develop several new classes utilizing this new facility and offer it to the entire Commonwealth.

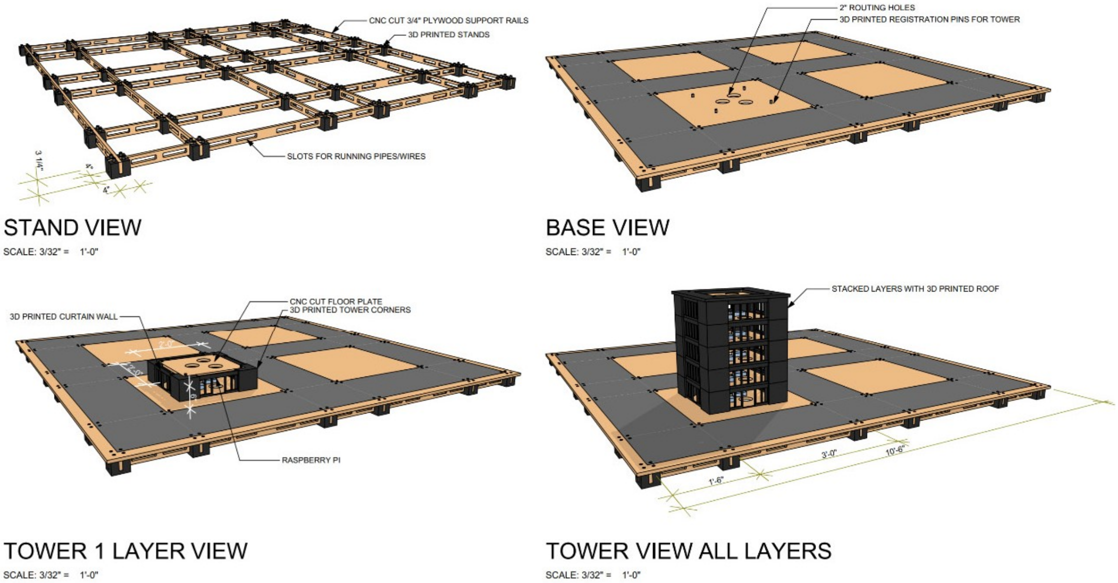


Figure 2.35: Initial design drawing of CyberWorld modules.

- Medical Device Security Testbed: The medical device security testbed covers two aspects of medical device security; patient point of care devices, and important at home medical devices. The testbed is designed so that a connected hospital room environment can be penetration tested on a network with specialized tools for discovering and analyzing protocols. A home connected healthcare environment has been designed in a similar fashion. The devices have been selected out of devices that may either critically impact patient care, cause harm, or substantially interfere with patient monitoring and diagnostics. This lab will be set up so that testing on these systems can be run remotely, allowing for many academic contributors to help secure our medical infrastructure.

As described above, UVA has invested cost-shared funds for research efforts impacting the mission of CCI. These efforts span Smart and Connected Health, Smart Cities, and Autonomous Systems focus areas, and include AI/ML and 5G research. The UVA LinkLab serves as a key access point, facilitating a breadth of collaborative partnerships. More details are available from https://engineering.virginia.edu/link-lab. As noted above, UVA received external funding for more than 50 new CCI-related projects in FY20, bringing in more the $10M in new CCI-related funding, adding to a portfolio of ongoing projects. Outcomes from these projects are being leveraged toward additional external funding and expanded efforts in FY21.

Correlated economic outcomes (jobs and new business formation)

The UVA Licensing and Ventures Group has hired multiple new Entrepreneurs in Residence tasked with scouting the UVA research landscape for promising new technologies. One of these new positions is specifically CCI related, focused on IoT, cybersecurity, and autonomy technology areas. In FY21, we will continue to leverage this position to promote tech transition.

UVA Licensing and Ventures Group Entrepreneur in Residence Mike Raker, focusing on CCI-related technologies shared:

> I see tremendous growth and potential in cyber physical systems which could have a profound impact on Virginia's economy. Initiatives like CCI are critical to realizing that potential. As an entrepreneur I see CCI as being critical to not only innovations in trust and security, but also in ensuring that other game changing innovations can be fully realized. Innovations from UVA in areas like smart health, autonomous systems, and smart cities have the potential to make the world a better and safer place while also lifting Virginia's economy, but innovations in these areas will never realize their potential without strong support from CPS. In that regard, I applaud the CCI efforts to create an ecosystem where all of these parts have a better opportunity to thrive and improve the lives of Virginians and people around the world.

In FY20, the UVA Weldon Cooper Center hired the first community liaison position that will pilot community and local leader engagement efforts to develop an understanding of how CCI related technologies can help improve local governance. This initiative's goals are to engage community leaders and stakeholders to facilitate understanding of these technologies which will help build a potential customer base for regional companies that drive technology integration in their communities. This pilot project will be completed in FY21.

In an effort to expand the CCI network, UVA partnered with local government, industry and community partners to form the Center for Civic Innovation, a project of the larger Smart Cville initiative. The Center focuses on Civic Technology & Smart Cities, Civic Engagement & Civic Innovation, and Data for the Public Good. The Center for Civic Innovation facilitated engagement, including a series of events led by the UVA LinkLab, to facilitate dialog and conversation on the use of technology and data for promoting civic innovation. COVID-19 related shutdowns shifted some planned events to later dates and impacted in-person interactions, but this partnership will continue to be leveraged in FY21.

Geographic distribution of awards from the funds contained in HB30

CeVA Node funds in FY20 were disbursed to the University of Virginia, Virginia State University, and Virginia Commonwealth University.

2.3.3 Additional Programs, Projects, Accomplishments

UVA has identified two strategic research programs for FY21:

- UVA Smart Health - The Smart Health initiative will develop means of voice-based cognitive assistance for health and wellness at a distance, as applied to traditional telehealth visits as well as remote health and wellness scenarios resulting from COVID-19. Not only is this topic important to support Virginia's rural communities needing increased access to the best healthcare possible, it is now increasingly important throughout all communities coping with change in our patterns of life. This program will address central issues of: (1) security, assurance, and trust, (2) cognitive assistant development utilizing natural language processing techniques and, (3) novel sensing and data processing capabilities.
- UVA Smart Cities - While much attention has been paid to smart city solutions for large cities, small cities and rural communities must also be included in the smart cities revolution. This project will focus on flood identification, characterization, and management as needed at a street/intersection level. This hyper-local prediction and control capability would support the decisions of officials in charge of issuing evacuation orders; allocating equipment and other resources; and managing catchments, pipes, and other flood-control infrastructure. This program will address central issues of: (1) system hardware and design, (2) modeling and simulation and, (3) system integration, interface, and robust secure communication.

2.4 CCI Coastal Virginia Node

2.4.1 Role of the CCI Coastal Virginia Node

CoVA CCI is southeastern Virginia's engine for research, innovation, and commercialization of next-generation cybersecurity technologies particularly in the areas of CPSS, 5G, and AI in maritime, defense, and transportation business sectors.

The CoVA vision is to secure the nation's critical infrastructure and strengthen Virginia's economy through the commercialization of findings from cutting-edge cybersecurity research focused on the maritime, defense, and transportation industries.

CoVA has four goals: build world leading CPSS capabilities; accelerate cyber startup creation and technology commercialization; grow workforce-ready cybersecurity and cyber physical system security talent to meet today's demands and tomorrow's economy; and build a collaborative network.

CoVA CCI created a network of over 80 faculty and researchers representing the region's universities and community colleges. These educational partners include Christopher Newport University, Norfolk State University, ODU, William & Mary, Regent University, East Coast Polytechnic Institute (ECPI) University, Eastern Shore Community College, Paul D. Camp Community College, Tidewater Community College, Thomas Nelson Community College. CoVA CCI is also partnering with private industry and government agencies including the US Navy, Huntington Ingalls Shipbuilding, CISCO, KBRWyle, Sentara Healthcare, G2Ops, 360IT, MI Technical Solutions to name a few. The CoVA CCI partners are depicted in Figure 2.36.

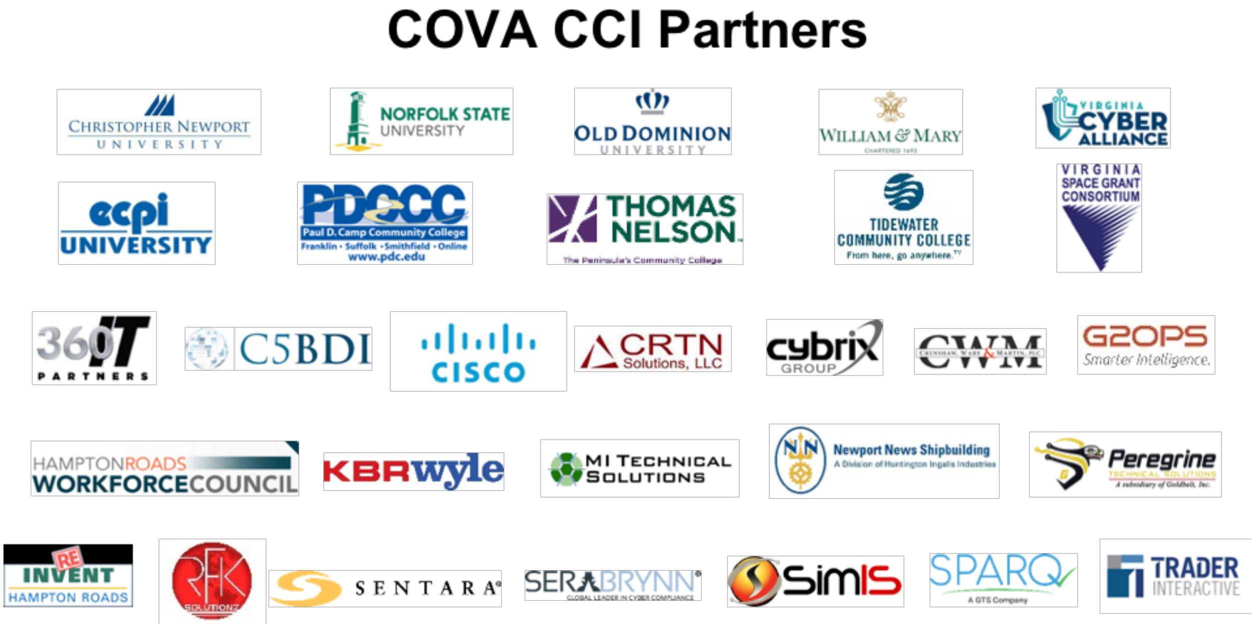


Figure 2.36: The CoVA CCI partners.

CoVA CCI has developed and launched multiple programs, including cybersecurity research and commercialization, creation of the Cyber Innovation Park, assisting students with internships, undergraduate research and other experiential opportunities, and business outreach.

2.4.2 Report on the Seven Requirements as per Item 135, Chapter 1289, HB30

Since first receiving notification of certification as CCI's southeastern node in December 2019, the Coastal Virginia Center for Cyber Innovation (CoVA CCI) has been actively engaged in accomplishing designated goals and objectives. In the past year, CoVA CCI has accomplished the following:

External Research Grants attracted to support the work of CCI

The CoVA CCI External Partnership Committee is designed to extend the reach of the CoVA CCI and increase the strength of its partnerships. The committee has the following main objectives:

- Develop a community of practice among industry and educational partners.
- Enhance articulation agreements and transfer pathways to include prior learning experiences and credentials identified of importance for employment and align with higher education curriculum.
- Develop a strategic outreach focused on both academic coursework and certificate credentialing, open houses, conferences, and academic and career advising/counseling networking events.
- Collaborate with the other CCI committees to support state and local projects.

The committee highlights include: it facilitated the Cyber Speaker Series; it evaluated cyber security certifications; it developed new and enhanced transfer pathways and educational agreements; it facilitated workshops for faculty and academic advisors and coordinated meeting/networking events.

CoVA CCI is actively working with multiple researchers and partners to pursue external research projects and grants.

From the period of July 2019 through June 2020 over $8.6M are currently active in 22 different cybersecurity grants, detailed in Figure 2.37. Research proposals have also been submitted to an additional 14 projects representing over $16M in potential funds.

Research Grants awarded from the funds contained in HB30

Research Projects

Five research projects have been awarded a total of $679,429 in COVA CCI node funding (Figure 2.38). These projects are:

- Leveraging AI and Machine Learning to Develop New CPSS and Workforce Development Solutions. Old Dominion University and Civilian Cyber, $150,000.
- Trust, Interoperability and Inclusion: A Framework for Creating Cyber-Trust in Connected Homes. William & Mary and Old Dominion University, $150,000.
- Encouraging Positive Changes in Cyber Hygiene Behaviors and Knowledge in the Department of Defense. Old Dominion University and MI Technical Solutions, $86,709.
- Securing IoT Devices through Power Side Channel Auditing and Privacy Preserved Convolutional Neural Networks. William & Mary and Old Dominion University. $150,000.
- Explore Privacy-Preserving in Deep Image Retrieval Systems. Old Dominion University, William & Mary, and Hampton University, $142,720.

Curricula Development

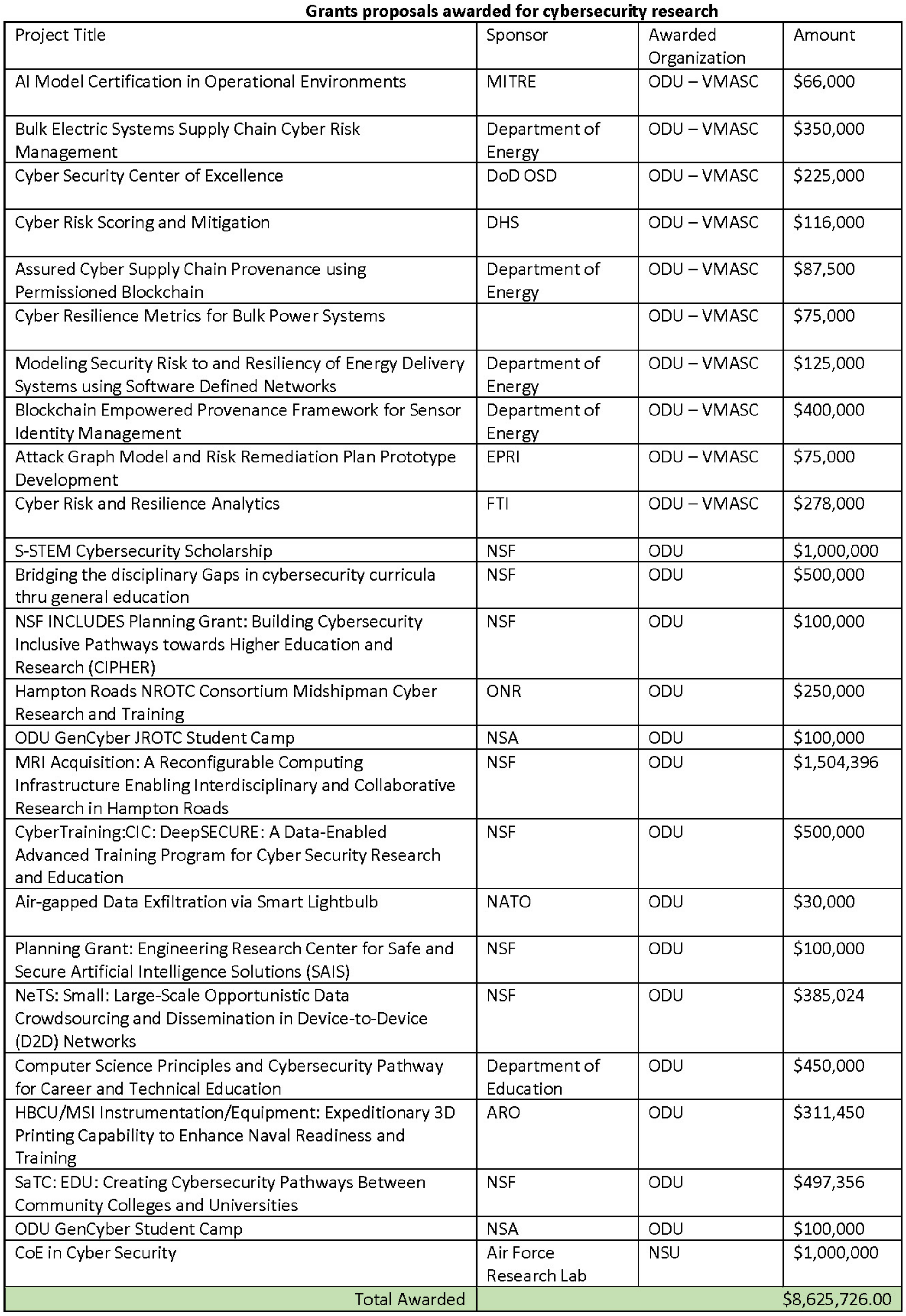
CoVA CCI has also allotted a total of $75,000 in funds to support in the creation of cybersecurity curricula that fills identified gaps and provides additional curricula to the Virginia Cyber Range. Three projects were initially funded for a total of $30,000. Two awards were given to Old Dominion University and one to William & Mary. Each project is awarded $10,000 (Figure 2.39).

- Cybersecurity practices for local governments and small to medium sized businesses. Submitted by Fred Lederer on behalf of William and Mary.
- Revision of ODU CYSE-600, Introduction to Cyber Security Principles. Submitted by Daniel W. Henkel, Old Dominion University.
- Course development for implementing blockchain applications for information security. Submitted by Harris Wu, Old Dominion University.

Virginia Space Grant Consortium

CoVA CCI is providing funding to the Virginia Space Grant Consortium to support the Internship program, Undergraduate Cybersecurity Research Program, and the INNOVATE Cyber Challenge. A total of $145,000 has been transferred to the VSGC to support these programs (Figure 2.40).

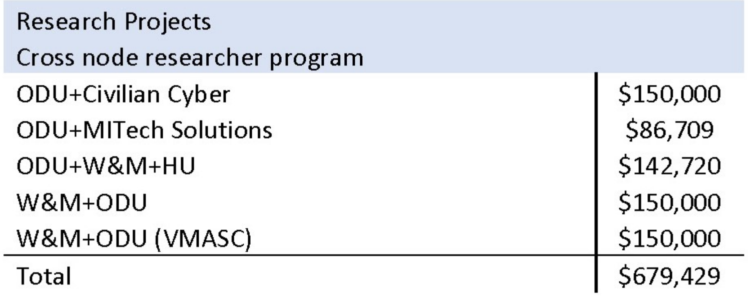
Graduate Student Experiential Learning Program



Grants proposals awarded for cybersecurity research

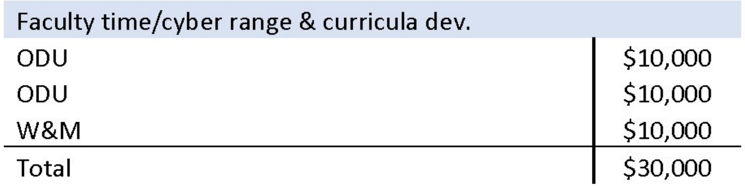
Project Title	Sponsor	Awarded Organization	Amount
AI Model Certification in Operational Environments	MITRE	ODU – VMASC	$66,000
Bulk Electric Systems Supply Chain Cyber Risk Management	Department of Energy	ODU – VMASC	$350,000
Cyber Security Center of Excellence	DoD OSD	ODU – VMASC	$225,000
Cyber Risk Scoring and Mitigation	DHS	ODU – VMASC	$116,000
Assured Cyber Supply Chain Provenance using Permissioned Blockchain	Department of Energy	ODU – VMASC	$87,500
Cyber Resilience Metrics for Bulk Power Systems		ODU – VMASC	$75,000
Modeling Security Risk to and Resiliency of Energy Delivery Systems using Software Defined Networks	Department of Energy	ODU – VMASC	$125,000
Blockchain Empowered Provenance Framework for Sensor Identity Management	Department of Energy	ODU – VMASC	$400,000
Attack Graph Model and Risk Remediation Plan Prototype Development	EPRI	ODU – VMASC	$75,000
Cyber Risk and Resilience Analytics	FTI	ODU – VMASC	$278,000
S-STEM Cybersecurity Scholarship	NSF	ODU	$1,000,000
Bridging the disciplinary Gaps in cybersecurity curricula thru general education	NSF	ODU	$500,000
NSF INCLUDES Planning Grant: Building Cybersecurity Inclusive Pathways towards Higher Education and Research (CIPHER)	NSF	ODU	$100,000
Hampton Roads NROTC Consortium Midshipman Cyber Research and Training	ONR	ODU	$250,000
ODU GenCyber JROTC Student Camp	NSA	ODU	$100,000
MRI Acquisition: A Reconfigurable Computing Infrastructure Enabling Interdisciplinary and Collaborative Research in Hampton Roads	NSF	ODU	$1,504,396
CyberTraining:CIC: DeepSECURE: A Data-Enabled Advanced Training Program for Cyber Security Research and Education	NSF	ODU	$500,000
Air-gapped Data Exfiltration via Smart Lightbulb	NATO	ODU	$30,000
Planning Grant: Engineering Research Center for Safe and Secure Artificial Intelligence Solutions (SAIS)	NSF	ODU	$100,000
NeTS: Small: Large-Scale Opportunistic Data Crowdsourcing and Dissemination in Device-to-Device (D2D) Networks	NSF	ODU	$385,024
Computer Science Principles and Cybersecurity Pathway for Career and Technical Education	Department of Education	ODU	$450,000
HBCU/MSI Instrumentation/Equipment: Expeditionary 3D Printing Capability to Enhance Naval Readiness and Training	ARO	ODU	$311,450
SaTC: EDU: Creating Cybersecurity Pathways Between Community Colleges and Universities	NSF	ODU	$497,356
ODU GenCyber Student Camp	NSA	ODU	$100,000
CoE in Cyber Security	Air Force Research Lab	NSU	$1,000,000
Total Awarded			$8,625,726.00

Figure 2.37: Grant proposals awarded for cybersecurity research.



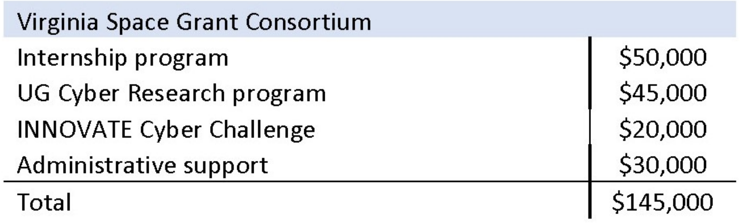
Research Projects Cross node researcher program	
ODU+Civilian Cyber	$150,000
ODU+MITech Solutions	$86,709
ODU+W&M+HU	$142,720
W&M+ODU	$150,000
W&M+ODU (VMASC)	$150,000
Total	$679,429

Figure 2.38: Cross Node Researcher Program.



Faculty time/cyber range & curricula dev.	
ODU	$10,000
ODU	$10,000
W&M	$10,000
Total	$30,000

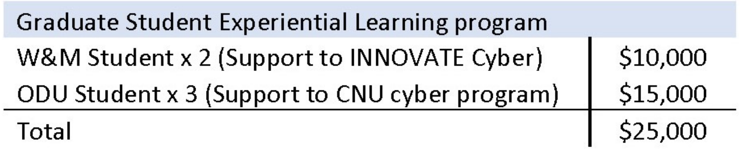
Figure 2.39: Curricula development.



Virginia Space Grant Consortium	
Internship program	$50,000
UG Cyber Research program	$45,000
INNOVATE Cyber Challenge	$20,000
Administrative support	$30,000
Total	$145,000

Figure 2.40: Virginia Space Grant Consortium.

CoVA CCI has allotted $100,000 to support graduate student experiential learning. This program allows graduate students to work with community colleges and universities within the region. Each student is awarded $5,000 for their work and a total of $25,000 has been provided for the first round of this program. Students from CNU, ODU, and W&M provided support to students from Tidewater Community College, Paul D. Camp Community College, Christopher Newport University, Norfolk State University, and Old Dominion University (Figure 2.41).



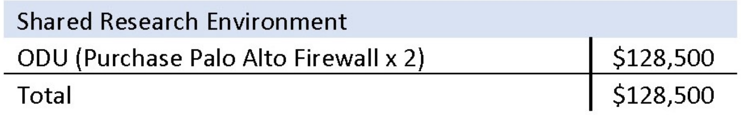
Graduate Student Experiential Learning program	
W&M Student x 2 (Support to INNOVATE Cyber)	$10,000
ODU Student x 3 (Support to CNU cyber program)	$15,000
Total	$25,000

Figure 2.41: Graduate Student Experiential Learning Program.

Shared Research Environment

CoVA CCI has allotted $600,000 in funds to support the development of a shared research environment (known as COVA Share). This environment will allow research to be conducted securely across node. A total of $128,500 has been spent on this project to date. The remaining funds will be executed within the next 4 months (Figure 2.42).

CoVA CCI released a request for proposals for curricula development for the Cyber Range and coursework



Shared Research Environment	
ODU (Purchase Palo Alto Firewall x 2)	$128,500
Total	$128,500

Figure 2.42: Shared Research Environment

.

in January 2020. This request for proposals asked for proposals from faculty that identified gaps in existing curricula and strategies to fill those gaps. In March 2020, CoVA CCI selected three proposals and awarded $10,000 to each faculty member to develop and refine cybersecurity curriculum that will be shared statewide. Curricula topics include:

- Cybersecurity practices for local governments and small to medium sized businesses. Submitted by Fred Lederer on behalf of William and Mary.
- Revision of ODU CYSE-600, Introduction to Cyber Security Principles. Submitted by Daniel W. Henkel, Old Dominion University.
- Course development for implementing blockchain applications for information security. Submitted by Harris Wu, Old Dominion University.

Research Faculty Recruited

COVA CCI is funding a regional cluster hire of five research scientists. These scientists will conduct research in cybersecurity related projects supporting the goals of CCI.

- Dr. Tan Le, Old Dominion University (Virginia Modeling, Analysis & Simulation Center);
- Dr. Rui Ning, Old Dominion University (Center for Cybersecurity Education and Research);
- Dr. Daniel Shin, W&M;
- Dr. Yan Lu, Old Dominion University (Virginia Modeling, Analysis & Simulation Center) – Hired as a match using university funds;
- Dr. Moeti Masiane, Norfolk State University.

CoVA CCI is funding Graduate Research Assistants (GRAs) to work on cross-node research projects supported by Christopher Newport University, Norfolk State University, Old Dominion University, and William & Mary. These GRAs will assist with the five research projects that were awarded in May 2020.

Results of Entrepreneurship and Workforce programming

Research experience is critical to cybersecurity education and workforce development, preparing students with the capacity to analyze real-world cyberattacks and combat new vulnerabilities. A program developed by the CoVA Node leverages the strength of research-extensive institutions to support active research participation by undergraduate students in the area of cybersecurity. Students will have opportunities to explore a variety of cutting-edge research topics, including but not limited to: Blockchain Security, Cyber Law and Policies, Human Behavior Security, Online Scams, Mobile Protection, Secure Digital Printing, Secure Internet of Things, Secure Machine Learning, Social Engineering, and Wireless Security. The selected students participate in one of the two sessions: Session 1 (04/13/2020 - 07/31/2020) and Session 2 (08/29/2020 -

12/19/2020). Each session offers a 16-week research program where a participant will work on a research project under the guidance of a faculty member and each selected student will receive a stipend of $2,500 to support her/his research and training. The call-for-participation was announced on February 13, 2020, and 39 students applied, with 18 selected to participate in the program. Selection criteria included students' academic achievements, awards, cybersecurity experience, geographic boundaries, personal attributes, and equity criteria.

The INNOVATE Cyber Challenge program aims to help students develop work skills while they resolve important issues faced by local business and industry. Students worked within a team to identify a challenge or issue related to cybersecurity. Using the design thinking approach to problem-solving, students are empowered to express their ideas, think creatively, and research within a high-impact team environment to identify solutions. Design thinking focuses on creating innovators – a human-centered method for creative action that leans heavily on empathy, observation, interviewing, and brainstorming. The selected students received an award package that includes a $1,000 project stipend, resources needed to produce and showcase a pitch, and a toolkit to help participants continue to innovate beyond this experience. A total of 24 undergraduate students were selected from Old Dominion University, Christopher Newport University, ECPI, Norfolk State University, William & Mary, and Tidewater Community College participated in this 9-week program from March 1, 2020 through May 12, 2020. Students were divided into five teams. Each team was tasked with developing a final cyber-related product or solution to a challenge suggested by business and institutional partners. Project topics included Disrupting Financial Incentives, High School Cybersecurity, Preventing Data Breaches, CVC Student Association, and Communicating "What Is Cybersecurity." A virtual showcase was held on May 12, 2020 for the students to pitch their solutions to a diverse group of faculty, administrators, and business contacts. Several of the teams will advance their ideas by creating business models with support from the ODU Entrepreneurial Center.

CoVA CCI is partnering with the Virginia Space Grant Consortium (VSGC) to manage the Cybersecurity Internship Program using their Commonwealth STEM Industry Program (CSIIP). VSGC will leverage CSIIP to build and improve on the relationships with employers across the Commonwealth to develop internship and experiential learning opportunities. VSGC will place 40 interns during the first two years of CoVA CCI. As of the end of May, VSGC received over 60 applications for internships and is the process of reviewing the applicants and finding placements.

CoVA CCI is supporting graduate assistants (GA) with experiential learning opportunities by supporting our community college partners. These GAs will work with the community college faculty member to assist in mentoring and supporting their cybersecurity class. CoVA CCI has placed three GRAs with Christopher Newport and one with Paul D. Camp Community College. Two GAs from William & Mary were also hired to support the INNOVATE Cyber Challenge to assist and mentor the student teams as they developed their projects.

The Virginia Space Grant Consortium developed a project to expand their internship placement across the state with their Experiential Learning through the Commonwealth STEM Industry Internship Program (CSIIP) in Support of the Commonwealth Cyber Initiative. This project will provide 34 paid internships across the state using CSIIP. CSIIP was established to support workforce development and research initiatives in the Commonwealth by providing students pursuing a STEM major at Virginia institutions of higher education with meaningful experiential learning opportunities through internships with Virginia-based companies. CSIIP services are free of charge to companies, schools and students. CSIIP provides year-round placements with maximum flexibility for part or full-time experiences. The length of the internship may vary based on company needs and student availability. A typical summer session will be 10-12 weeks full-time and a part-time academic semester is typically up to 20 hours per week for 16 weeks. Students will be paid a fair wage. CSIIP requires a minimum stipend/salary of $10 per hour; however, CCI-related disciplines typically are higher paid. CSIIP has a strong existing infrastructure and best practice process for recruiting and placing internships statewide and is well poised to build and sustain internship placements statewide in CCI disciplines.

Collaborative partnerships and projects

CoVA CCI is also investing in a shared collaborative research computing environment, known as COVA SHARE, to support the growing cybersecurity programs, academic and research collaboration opportunities, and industry partnerships. Guided by CoVA CCI researchers, the computing center and network investment will support the CoVA CCI and enable communication to the Hub and other Nodes. The environment will lay a foundation to support 5G testbed data collection, secure storage and transfer between connected Node members and to the CCI Hub for analysis and other collaboration. It will provide access to a flexibly designed computing environment via connectivity improvements between ODU and William & Mary, and between ODU and Norfolk State University for potential collaborative efforts involving secure transfer of data between schools or secure remote access to physical or virtual hosts.

A team of researchers from W&M was awarded funding from the CCI Hub for their project to expand upon their research of data poisoning for convolutional neural networks designed to estimate information from satellite imagery, using road quality and condition as a case study. They will extend and expand these activities to include (a) a broader range of geographies around additional institutions of higher education in Virginia, to better take into account the effects of scene variations as we move from urban and suburban to semi-rural and rural areas, and (b) research into data poisoning (an issue of increasing importance given the looming threats of cyber vandalism, and cyberwarfare at large) in the context of satellite imagery and deep learning. These activities will be conducted as a part of a partnership with intelligence community and industry partners who are interested in both (a) understanding the minimum modifications necessary to 'trick' existing deep learning technology into believing a rough road might be smooth, or a smooth road rough, and (b) if there are network architectures resilient to poisoned datasets. The proposed work pursues three different classes of objectives: (1) experiential learning objectives, (2) applied research objectives, and (3) project objectives.

Correlated economic outcomes (jobs and new business formation)

A Cyber Innovation Park is being developed on the ODU campus. This $2M capital investment includes over 11,000 square foot space for housing a data center, multiple research labs, teaching labs and classrooms, meeting space, faculty offices, and a student cyber incubator. Part of the space will be reconfigurable to support cybersecurity events such as cybersecurity competitions and workshops. The Cyber Innovation Park is anticipated to be made available in spring 2021. It will become home to not only ODU's cybersecurity program but also CoVA CCI, supporting various cybersecurity research, innovation, commercialization, and talent development efforts.

CoVA CCI maintains strong partnerships with industry and is working with these partners on several initiatives. Below are several testimonials from these partners on the value added by supporting CoVA CCI.

Chris Shenefiel, Cisco, provides the following testimony:

> The collaboration with CoVA CCI has been very helpful for industry partners in serving to share innovation, best practices. It has also given industry the opportunity to educate Virginia cybersecurity students, guide curricula and to contribute to research focus areas beyond our normal spheres of collaboration. I believe CoVA CCI will have positive impact on the future of cybersecurity in the Commonwealth through partnerships, innovation, and collaboration that would not have happened otherwise.

Tracey Gregorio, CEO, G2OPS, puts it as follows:

> Working with the Coastal Virginia Center for Cyber Innovation has opened the door for numerous opportunities, new employees and interns. I very much appreciate the open dialogue we are

> fostering between researchers, industry leaders, and the workforce. Based on the success to date, I anticipate that CoVA CCI will have a significant impact in our region and CCI will shape the future of cyber in the Commonwealth.

Leigh Armistead, President, Peregrine Technical Solutions, says:

> I would like to write about the value of the Coastal Virginia Center for Cyber Innovation and the Commonwealth Cyber Initiative (CCI). As a robust small business, Peregrine Technical Solutions, LLC, is a thought leader within the cybersecurity industrial control systems (ICS) and the Internet of Things (IoT), supporting many federal and commercial customers... We are based in Hampton Roads and have been very closely associated with Old Dominion University for the last five years through a number of cyber research/industry initiatives to include Hampton Roads Cyber (HRCyber) as well as a board member with the Virginia Cyber Alliance. I also served on the committee that produced the CCI Blueprint, and I have been very impressed with the remarkable growth of this latest iteration, with its diverse and large parallel working groups. ODU, as the regional leader, has brought in a number of local industry leaders to provide ongoing feedback to the overall effort, and it shows in the products developed to date. In addition, the close communications between researchers and businesses, along with the vision and future plans for CCI, will undoubtedly result in a number of significant economic benefits for the Commonwealth in general. I look forward to continuing to participate in the effort as a small business thought leader.

Bobby Kenner, CEO, CivilianCyber, highlights his support:

> We have been highly impressed by the Coastal Virginia Center for Cyber Innovation and truly appreciate their support as we work to automate and scale the cybersecurity workforce pipeline. CoVA CCI has provided invaluable thought leadership as well as interactive facilitation between researchers and leaders in the public and private sectors. One outcome for us has been a collaboration with the Virginia Beach EDA to collect feedback from over thirty regional public and private organizational leaders. The result will be an industry-driven cybersecurity workforce needs assessment that will help us deliver an effective solution. Based on our interactions and positive results to date, I have no doubt that CoVA CCI is providing great benefit to the region and will continue to serve as a cyber leader throughout the Commonwealth.

Mike Ihrig, CEO, MI Technical Solutions, says:

> As MI Technical Solution has grown over the past decade and a half, we have found that we only do so with the help and constant assistance of organizations like Commonwealth Cyber Initiative (CCI). I believe that without their guidance and support, MI Technical Solutions would not have been selected as one of the Top Workplaces in Hampton Roads. I am writing today to express my full support for the CCI in the Commonwealth of Virginia, as I am sure they will continue to have a significant impact in our region, Virginia and the Country. The opened dialogue and the associated contacts developed through our relationship with CCI has provided MI Technical Solutions and in particular me, huge opportunities that I could not have found elsewhere. We here at MITS are looking forward to our continuing relationship and where it might take us as we shape the future.

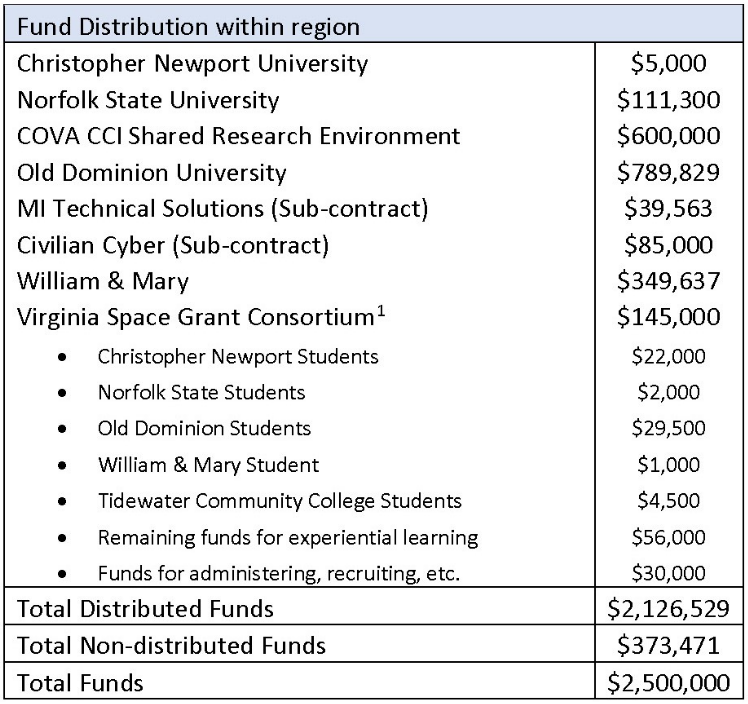
And last but not the least, here is Dan Bowden, Sentara:

> As Chief Information Security Officer for Sentara, I have worked closely with regional cybersecurity researchers and educators for nearly four years. The CCI efforts have ramped up our ability

to jointly produce research and products that will have an economic benefit. Most recently, Sentara's work with cybersecurity researchers affiliated with CoVA CCI has explored how to use Blockchain to enhance health care technology management, and increased care management efficiency. The long-term potential and impact of this research cannot be understated, and is continually growing.

Geographic distribution of awards from the funds contained in HB30

CoVA CCI has distributed funds to Christopher Newport University, Norfolk State University, Old Dominion University, Virginia Space Grant Consortium, and W&M. These funds are provided for research and innovation and talent pipeline projects and activities. Funding for cybersecurity research is also provided to MI Technical Solutions and Civilian Cyber for their work in partnership with researchers from Old Dominion University. CoVA CCI is also working with the regional community colleges and is provided support through the Graduate Student Experiential Program (Figure 2.43).



Fund Distribution within region	
Christopher Newport University	$5,000
Norfolk State University	$111,300
COVA CCI Shared Research Environment	$600,000
Old Dominion University	$789,829
MI Technical Solutions (Sub-contract)	$39,563
Civilian Cyber (Sub-contract)	$85,000
William & Mary	$349,637
Virginia Space Grant Consortium[1]	$145,000
• Christopher Newport Students	$22,000
• Norfolk State Students	$2,000
• Old Dominion Students	$29,500
• William & Mary Student	$1,000
• Tidewater Community College Students	$4,500
• Remaining funds for experiential learning	$56,000
• Funds for administering, recruiting, etc.	$30,000
Total Distributed Funds	$2,126,529
Total Non-distributed Funds	$373,471
Total Funds	$2,500,000

Figure 2.43: Fund distribution within the Coastal Region.

The non-distributed funds will be committed during the remainder of 2020 and into the spring/summer of 2021. The following activities will be supported during this timeframe.

- Graduate Student Experiential Learning (fall 2020). Eight graduate students will be hired at $5,000/student to support selected projects under the Experiential Learning Program for a total cost of $40,000.
- INNOVATE Cyber Challenge (Fall 2020). We will conduct our second INNOVATE Cyber Challenge in fall 2020 with 20 students from across the region. Total cost for the program is $27,000.
- Research Project Commercialization proposals (Fall 2020 through Summer 2021). A request for proposals was released in August 2020 to the PIs of the five cybersecurity research projects previously funded by CoVA CCI. This RFP will provide seed funds, totally $100,000, to support the commercialization efforts of the selected proposals. These funds are coming out of the Tech Transfer/patent cost program.

- Curriculum Development (Fall 2020). A request for proposals was released in August 2020 to faculty requesting proposals on the development of new cybersecurity curriculum. Each proposal will be supported with an award of $10,000 with a total budget of $55,000.
- The remaining funds, $151,471, will be disbursed in Spring 2021 to upgrade and extend to COVA Share environment and to support research and innovation initiatives demonstrating the most success.

2.4.3 Additional Programs, Projects, Accomplishments

The CCI Fellow program is aiming to build an ecosystem of shared cyber expertise and collaboration across the CCI Network and at the CCI Hub. Awarded Fellows will directly contribute to, or be responsible for creating, Hub-led research, education, or innovation programs in priority areas determined by Executive Director in consultation with the Leadership Council. Three CoVA CCI faculty were selected to join the CCI Fellows Inaugural Cohort, with a term from June 1, 2020 to May 30, 2022. The fellows are Dr. Hongyi Wu, Old Dominion University, Dr. Sachin Shetty, Old Dominion University, and Dr. Frank Hu, Norfolk State University.

CoVA CCI has allocated the majority of the budgeted funds for several successful initiatives. These include the Research and Innovation Research ($680,000 out of $775,000), INNOVATE Cybersecurity Challenge ($25,000), and Undergraduate Research (50,000). CoVA CCI is looking at realigning several budget lines to find additional funds to add to these initiatives. In addition, CoVA CCI is looking at additional revenue sources in the form of industry contributions to provide funding for the INNOVATE Cybersecurity Challenge.

2.5 CCI Southwest Virginia Node

2.5.1 Role of the CCI Southwest Virginia Node

The Southwest Virginia node of the CCI network (SWVA CCI) seeks to promote southwestern Virginia and the greater Commonwealth as leaders in cyber research, innovation and entrepreneurship, and workforce development.

SWVA CCI's mission encompasses the four goals of CCI. First, it seeks build world-leading Cyber Physical Systems Security (CPSS) research capabilities by promoting multi-institution, cross-sector programs for security of emerging technologies, developing programs applying advanced cyber technologies to node focus areas, and leveraging collaborations at the forefront of security in emerging technology and commercialization. Second, it aims to accelerate cyber startup creation and technology commercialization by enhancing cyber entrepreneur and internship programs and expediting development of commercialization ecosystem for cybersecurity. Third, it will grow workforce-ready cybersecurity and CPSS talent to meet today's demands and tomorrow's economy by providing support for cyber training for educators and practitioners and expanding experiential learning opportunities in cybersecurity. Fourth, it works to build a collaborative network by fostering ties with the hub and advancing synergies within node and across network

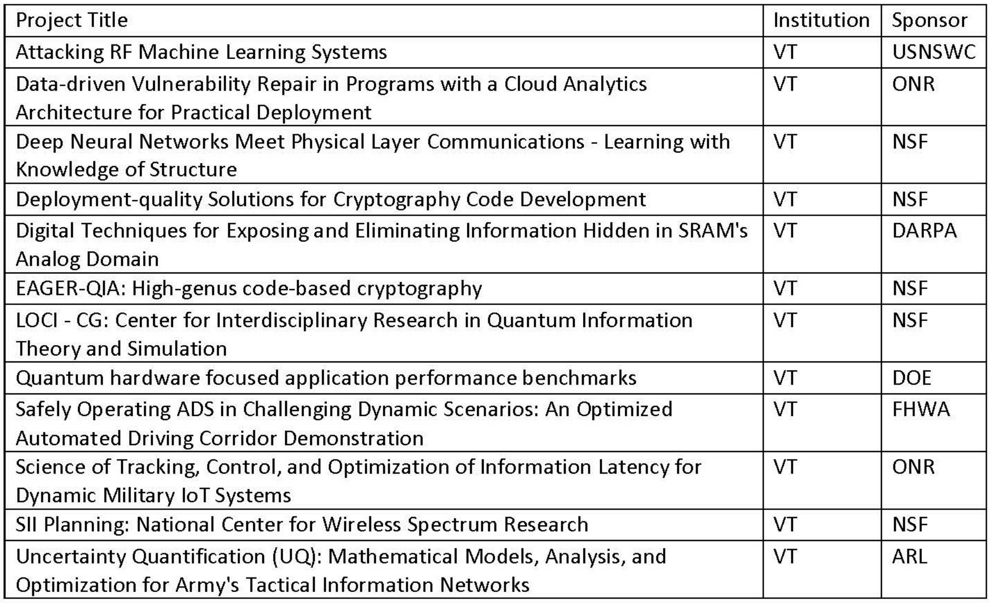
SWVA CCI consists of the academic institutions Radford University, University of Virginia's College at Wise (UVa-Wise), Liberty University and Virginia Polytechnic Institute and State University (Virginia Tech or VT) and their constituent business partners, along with the Virginia Cyber Range, Danville Community College, Mountain Empire Community College, New River Community College, Southwest Virginia Community College, Virginia Highlands Community College, Virginia Western Community College, Wytheville Community College, the New College Institute, and the Institute for Advanced Learning and Research. SWVA CCI builds on synergies between partners and leverages extensive research capabilities, industry partnerships, and excellence in education to secure the emerging 5G and future 6G wireless infrastructures for connected, intelligent, and autonomous applications ranging from transportation to power to unmanned platforms underwater, in air, and in space.

In its inaugural year, SWVA CCI launched a number of initiatives in accordance with its strategic plan which was submitted to and approved by VRIC in Fall 2019.

2.5.2 Report on the Seven Requirements as per Item 135, Chapter 1289, HB30

External Research Grants attracted to support the work of CCI

From June 2019, CCI SWVA engaged faculty have been active on externally sponsored projects awarded at amounts totalling more than $40M, a few of which are featured in Figure 2.44.



Project Title	Institution	Sponsor
Attacking RF Machine Learning Systems	VT	USNSWC
Data-driven Vulnerability Repair in Programs with a Cloud Analytics Architecture for Practical Deployment	VT	ONR
Deep Neural Networks Meet Physical Layer Communications - Learning with Knowledge of Structure	VT	NSF
Deployment-quality Solutions for Cryptography Code Development	VT	NSF
Digital Techniques for Exposing and Eliminating Information Hidden in SRAM's Analog Domain	VT	DARPA
EAGER-QIA: High-genus code-based cryptography	VT	NSF
LOCI - CG: Center for Interdisciplinary Research in Quantum Information Theory and Simulation	VT	NSF
Quantum hardware focused application performance benchmarks	VT	DOE
Safely Operating ADS in Challenging Dynamic Scenarios: An Optimized Automated Driving Corridor Demonstration	VT	FHWA
Science of Tracking, Control, and Optimization of Information Latency for Dynamic Military IoT Systems	VT	ONR
SII Planning: National Center for Wireless Spectrum Research	VT	NSF
Uncertainty Quantification (UQ): Mathematical Models, Analysis, and Optimization for Army's Tactical Information Networks	VT	ARL

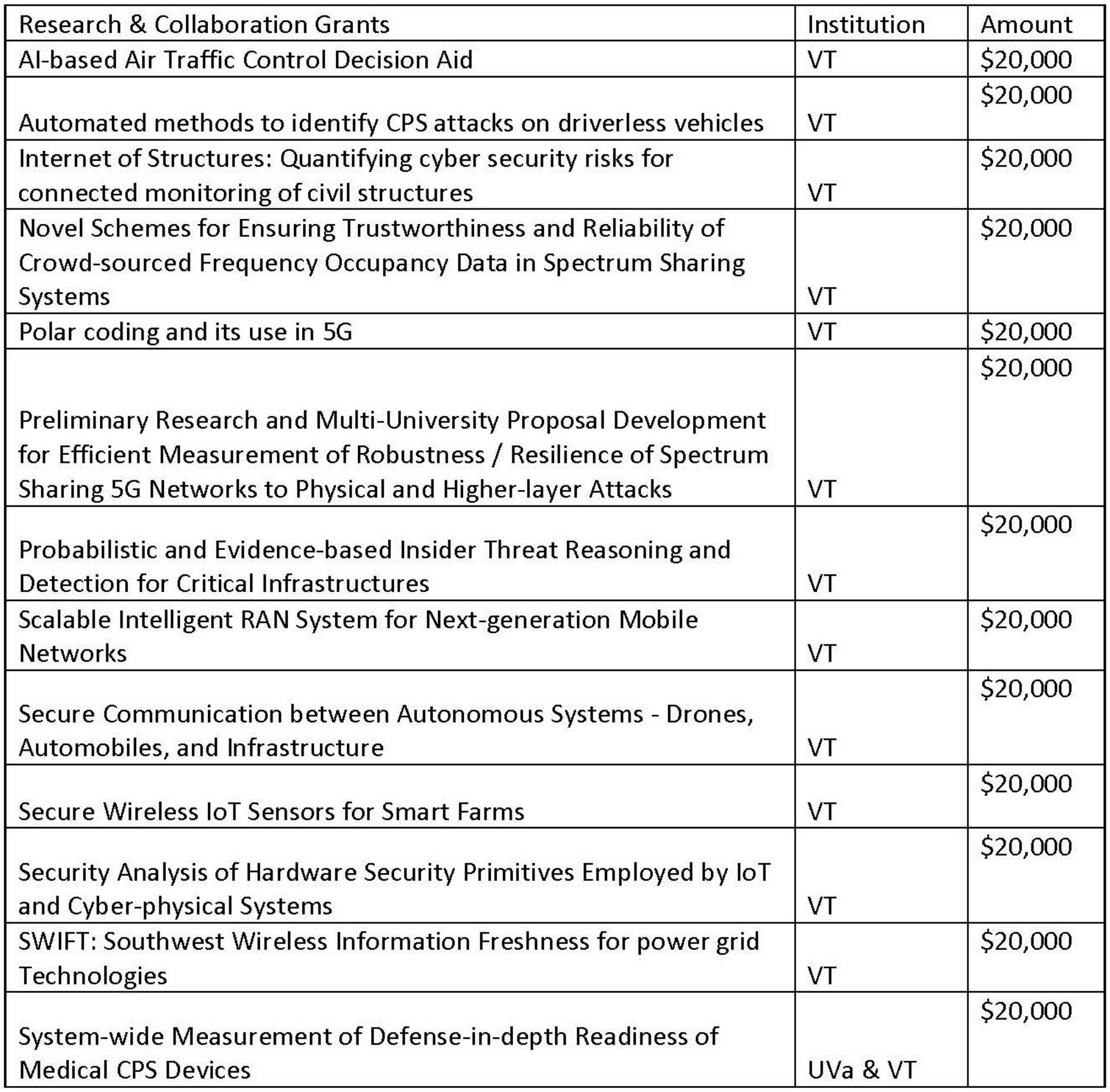
Figure 2.44: Selected externally sponsored projects supported by faculty engaged in SWVA CCI during FY20 and FY21.

Research Grants awarded from the funds contained in HB30

In support of building world-leading CPSS research capabilities, SWVA CCI focuses research efforts on secure CPS to fully harness the power of 5G and node application domains which include automotive, power systems, manufacturing, autonomous vehicles, and agriculture, and offer the potential to discover, demonstrate, and commercialize technological solutions that will enable the next industrial revolution. FY20 saw the commencement of several node-led research initiatives.

Research and Collaboration Grants awarded by SWVA CCI allow researchers to build a collaborative network throughout Virginia and beyond, accelerating commercialization as well as increasing external funding and scholarly output. These grants promote the work of researchers to encourage collaboration; ramp up to engage in the key node research areas; and facilitate other CPSS research leaning toward commercialization. Access to shared equipment via such projects is another way in which research will be strengthened through the node and network.

Figure 2.45 summarizes SWVA CCI Research and Collaboration Grants awarded in FY20. Project details follow. In most cases, each project was funded in the amount of $10,000 in FY20, with the balance to be allocated in FY21.



Research & Collaboration Grants	Institution	Amount
AI-based Air Traffic Control Decision Aid	VT	$20,000
Automated methods to identify CPS attacks on driverless vehicles	VT	$20,000
Internet of Structures: Quantifying cyber security risks for connected monitoring of civil structures	VT	$20,000
Novel Schemes for Ensuring Trustworthiness and Reliability of Crowd-sourced Frequency Occupancy Data in Spectrum Sharing Systems	VT	$20,000
Polar coding and its use in 5G	VT	$20,000
Preliminary Research and Multi-University Proposal Development for Efficient Measurement of Robustness / Resilience of Spectrum Sharing 5G Networks to Physical and Higher-layer Attacks	VT	$20,000
Probabilistic and Evidence-based Insider Threat Reasoning and Detection for Critical Infrastructures	VT	$20,000
Scalable Intelligent RAN System for Next-generation Mobile Networks	VT	$20,000
Secure Communication between Autonomous Systems - Drones, Automobiles, and Infrastructure	VT	$20,000
Secure Wireless IoT Sensors for Smart Farms	VT	$20,000
Security Analysis of Hardware Security Primitives Employed by IoT and Cyber-physical Systems	VT	$20,000
SWIFT: Southwest Wireless Information Freshness for power grid Technologies	VT	$20,000
System-wide Measurement of Defense-in-depth Readiness of Medical CPS Devices	UVa & VT	$20,000

Figure 2.45: Research and Collaboration Grants Awarded in FY20.

AI-assisted Air Traffic Control (ATC) Decision Aid (AADA)

AADA is a decision aid for air traffic controllers meant to improve aircraft routing upon arrival/departure and alleviate stress on human controllers by highlighting areas of risk. Additionally, components of the system support ground control routing of planes on the tarmac, a likely earlier adopter of AI. At a high level, this system includes three components: AI Engine, Human Machine Interface (HMI), Security Engine. As of January 2020, all aircraft are required to equip Automatic Dependent Surveillance-Broadcast (ADS-B) in order to fly in most controlled airspaces. ADS-B broadcasts data obtained from the aircraft's navigation system at a specified interval, providing situational awareness to both pilots and controller situational awareness to both pilots and controllers. The system, illustrated in Figure 2.46, will harness ADS-B signals as an input to the AI engine, and we will employ additional authentication or other security measures to ensure that the signal cannot be spoofed or manipulated. The decision aid is intended to act strictly as a supplemental tool for the human controller to inject helpful information into their normal process while not distracting the controller from their core duties. While the primary goal of this system is to improve safety at airports by reducing the potential for human error due to stress of fatigue, it would also allow us to review existing security protocols in ATC towers and associated CPS. Based on this review, additional security measures are required to safely enable the increased automation.

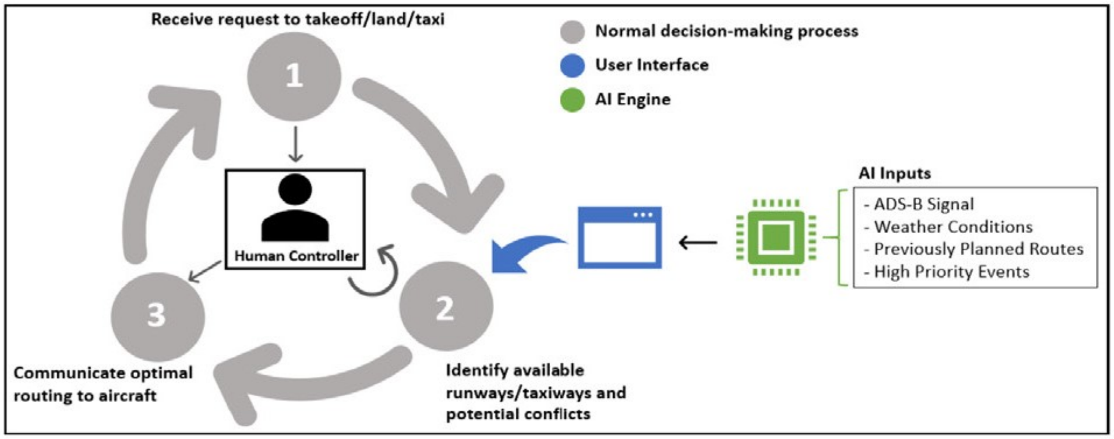

Receive request to takeoff/land/taxi
1
Human Controller
2
3
Communicate optimal routing to aircraft
Identify available runways/taxiways and potential conflicts
Normal decision-making process
User Interface
AI Engine
AI Inputs
- ADS-B Signal
- Weather Conditions
- Previously Planned Routes
- High Priority Events

Figure 2.46: System diagram of modified decision-making process with proposed decision aid for AI-assisted ATC.

Automated Methods to Identify CPS Attacks on Driverless Vehicles

CPSS is increasingly important in the fields of Autonomous and Automated Driving Technologies. Automating a CPS typically involves three robotic layers of sensing, planning, and acting. Computer algorithms are being used for each of these layers. Neural Networks (NNs) and deep learning (DL) are some of the algorithms within ML that can be found in the sensing layer. As an example, NVIDIA is a company promoting using NN for what is call an “end-to-end” solution in the autonomous driving field. End-to-end means the raw sensors inputs are fed into the NN which directly controls vehicle actuation (steering and throttle/brakes). Unfortunately, AI/ML are susceptible to cyber-attacks. Prototype automated vehicles, such as sedans, SUVs, trucks, and tractors, are increasingly relying their sensing on AI/ML. This project focuses on defending CPS in their decision-making from attack or deception, reduction of false alarms and cyber-attacks rates, and real-time situational awareness.

Internet of Structures: Quantifying Cyber Security Risks for Connected Monitoring of Civil Structures

Structural Health Monitoring (SHM), an active research field dedicated to the automation of civil infrastructure inspection. Although still far from achieving a fully connected network of structures, many civil structures are currently being monitored remotely, such as the Varina-Enon bridge near Richmond, VA. But what happens if the abnormal pattern is generated by a malicious, interfering device? Or if the interference occludes true damage patterns? If the data is hacked, would ambient vibrations due to traffic and pedestrians contain any information exploitable by a malicious entity? SHM systems are a new class of vulnerable CPS with unique concerns, illustrated by the above scenario. Their architecture, scale, context and use differ greatly from typical cyber-physical security targets, such as mobile phones, automobiles and wearable devices. This uniqueness requires a paradigm shift in how the security of these systems is approached, starting from the basic sensing strategies and algorithmic assumptions. As such, we propose the need for security strategies for the “Internet of Structures” (IoS), the network of connected buildings, bridges, dams, etc., that is the inevitable future of infrastructure inspection in smart cities.

This research envisions three primary threat models to SHM systems: fault injection which falsely triggers a system’s damage detection protocol and causes the operator (usually a local government agency) to investigate; spoofing a baseline sensor signal, thereby occluding a physical attack on a structure which causes critical damage without an alarm; and eavesdropping, a side-channel attack whereby information about occupants, occupancy patterns and traffic patterns is inferred from unconventional processing of sensor data. All of threats are focused on unique vulnerabilities at the sensor, algorithm, and raw data levels.

The research will leverage Goodwin Hall on VT's campus as a full-scale, CPS test bed. Goodwin Hall is an instrumented smart building, with a building-wide structural monitoring network composed of 225 accelerometers, the largest vibrations monitoring platform of any building in the world. The network enables continuous tracking of the structural behavior for the purposes of damage detection. It also enables observation of occupant behavior through structural vibrations induced by footsteps, door openings, and other actions. This data has been used to track occupant location and classify occupant information. The building is a research model for what future smart buildings could look like. It presents an opportunity to explore the limits of CPS cyber security at a large scale, with complete flexibility.

Novel Schemes for Ensuring Trustworthiness and Reliability of Crowd-sourced Frequency Occupancy Data in Spectrum Sharing Systems

The overarching goal of this research project is to design and evaluate coordinated spectrum sharing approaches for the CCI-funded Vehicular testbed being developed at Virginia Tech. This is important because the user capacity and data rates supported by currently allocated frequencies in the 5.9 GHz band for vehicular communications may not be sufficient, and additional frequency bands may need to be utilized via coordinated spectrum sharing. Specifically, we plan to develop and assess secure and reliable novel schemes to enhance spectrum sharing by exploiting crowd-sourced spectrum occupancy information. These approaches, illustrated in Figure 2.47 will consider both the trustworthiness of the users who provide this information and the accuracy with which they are able to measure spectrum occupancy. However, such crowd-sourced approach is susceptible to two threats. First, usefulness of data is limited by the receiver sensitivity of the contributing users' radio hardware. Second, malicious users could deliberately provide inaccurate data. This project proposes novel schemes that ensure the trustworthiness, reliability, and accuracy of crowdsourced spectrum occupancy data obtained from contributing users. Promising approaches include devising a hybrid scheme and applying the cell-division approach.

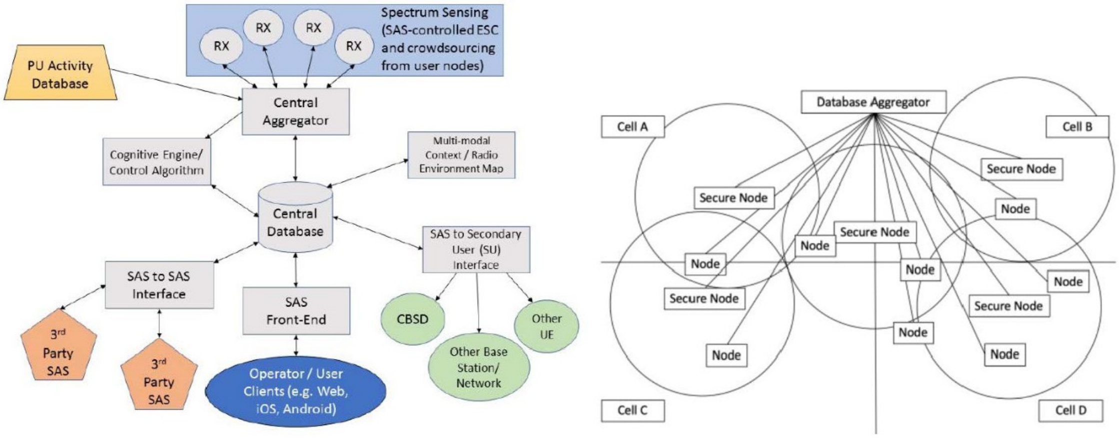


Figure 2.47: (a)An open source spectrum access sharing system under development by Wireless@VT allows radio nodes to be configured and controlled in a geographic area (b) An example scheme for ensuring trustworthiness of crowdsourced data

Polar Coding and Its Use in 5G

Polar coding supports 5G technology with a new communication paradigm introduced in 2009. Polar codes have already been of immense value as the source of error correction in 5G wireless infrastructure and they have shown great potential in a diverse range of applications. However, there are key elements in their construction that are still poorly understood at finite length, which is required for actual implementation.

The basic construction begins with a kernel matrix which decreases the error rate of some bits through the creation of synthetic channels, some of which are improved while others are degraded relative to the original channel. This polarizing effect is exaggerated by repeated tensoring to concentrate transmission errors into a few parity bits. Ultimately, some channels are near perfect (allowing nearly noiseless communication) while others must be discarded. This project aims to address issues arising from a disconnect between the theoretical construction of polar codes and their practical use and whose resolution stands to improve performance. In practical settings, errors are not randomly separated and can sometimes depend on prior bits in the codeword (a phenomenon known as intersymbol interference). Moreover, there is a need for flexible construction of kernel matrices for on-the-fly decisions about which channels should be discarded.

Probabilistic and Evidence-based Insider Threat Reasoning and Detection for Critical Infrastructures

Organizational insider threat detection has been a long-standing open problem, mainly due to excessive false alarms. For large organizations operating modern critical infrastructures (e.g., telecommunications, power and utilities, and transportations), the threat of insiders may cause serious operational disruption, besides data loss. This work aims to design and develop an accurate and easy-to-deploy solution for an organization to detect insider threat anomalies. Specifically, this project includes design and development of a probabilistic programming language-based insider threat reasoning and detection system. The system will provide the ability to sift through a huge amount of multi-dimensional data and logs and recognize outlier user activities by modeling and capturing uncertainties associated with human behaviors. Our approach will observe, learn, and detect abnormalities among interdependent events and user-actions within a learnable or customizable duration of time. Main features of the approach are high accuracy, plug-and-play deployment, and scalability. The novelty is in the probabilistic computational strategies for maximizing evidences and reducing false alarms, minimizing human guidance in training the detector, and the probabilistic programming language in the context of anomaly detection.

Scalable Intelligent RAN System for Next-generation Mobile Networks

The future generation mobile network is expected to support various types of services such as eMBB (enhanced Mobile Broadband), mMTC (massive Machine Type Communications), and URLLC (Ultra-Reliable and Low Latency Communications) and beyond, while at the same time fulfilling different QoS/QoE requirements. These requirements will be determined between the network operator and end-users with specifications of key performance indicators (KPIs), such as throughput, latency, connectivity, etc. As a service-based architecture, network slicing enables a diverse range of services to be accommodated in the same physical radio access network (RAN). To satisfy service requirements, the key is the placement of distributed RAN resources (e.g, spectrum, computation, memory resources etc.) that support dynamic customization of each slice. This proposal aims to architect a RAN-level intelligent system that dynamically predicts network progression and conducts network design strategies and auto-deployment within the network periodically through temporal data mining of the RAN behaviors. The proposed method observes the behavior of the network, translates the policy restrictions of service agreement, spectrum, and physical resources, and applies deep learning to optimize allocations of various RAN resources promptly. Comparing earlier network generations have been designed as general-purpose connectivity platforms with limited differentiation capabilities across use cases, 5G (and Next-G) intends to create an ecosystem for technical and business innovation involving vertical markets such as automotive, energy, healthcare, etc. Through abstracting the features of each scenario, our system adapts to meet the requirements from different fields and markets in an efficient way. The proposed transformative research will result in the following key technical innovations:

- An automated deep learning-based RAN framework that takes in input - the raw information from various 5G components, i.e., BS and Core, and requested QoS/QoE requirements by stakeholders, UEs and mobile virtual network operators (MVNO, defined as reseller for wireless communication services), and outputs in real-time
- A list of optimal 5G network design and deployment strategies that guarantees the QoS/QoE requirements for each UE and MVNO, under the dynamic and unpredictable wireless environment (channel conditions, interference, mobile UEs etc.). The proposed framework will be universal in the sense that

it will be auto adaptive to a given 5G wireless scenario (e.g., rural vs urban areas)

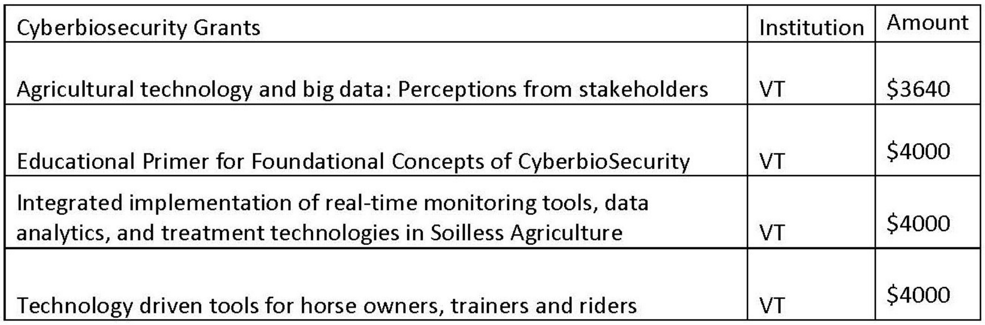
Security Analysis of Hardware Security Primitives Employed by IoT and Cyber-physical Systems

Underlying all cryptographic operations, whether they be encryption, integrity checks, or authentication, is a source of key material. Hardware is in a unique position to serve as a source of key material because, unlike software, it is influenced by chaos—both at manufacturing time and during operation. Research provides three hardware-level mechanisms for providing key material:

- Phase Locked Loops (PLLs)
- Ring Oscillators (ROs)
- Static Random-Access Memory (SRAM)

While it is clear is that the approach employed by commodity processors (i.e., PLLs) is ill-suited for ultra-low SWaP devices due to their reliance on special-purpose black-box hardware circuits that have a high latency and are high power, it is not clear what the landscape looks like between RO- and SRAM-based approaches. This is because research on RO- and SRAM-based hardware security primitives has bifurcated itself such that it ignores the other class of approach in their evaluation; this self-segregation holds for both defense and attack papers. The goal of this project is to examine the real-world trade-offs of the two most popular hardware security primitives suitable for ultra-low SWaP devices common to cyber-physical systems. The landscape analysis will include both defensive and attack constructions.

To support the growth of cyber-related agricultural applications, SWVA CCI has a separate call for Cyberbiosecurity Grants. Figure 2.48 summarizes SWVA CCI Cyberbiosecurity Grants awarded in FY20. Project details follow:



Cyberbiosecurity Grants	Institution	Amount
Agricultural technology and big data: Perceptions from stakeholders	VT	$3640
Educational Primer for Foundational Concepts of CyberbioSecurity	VT	$4000
Integrated implementation of real-time monitoring tools, data analytics, and treatment technologies in Soilless Agriculture	VT	$4000
Technology driven tools for horse owners, trainers and riders	VT	$4000

Figure 2.48: FY20 Cyberbiosecurity Grants.

Agricultural Technology and Big Data: Perceptions From Stakeholders

Agricultural technology and big data have revolutionized the food system. This large system creates millions of data points, populates the Internet of Things (IoT), and creates issues of cyberbiosecurity related to the big data that is generated. Stakeholder groups do not know what it means, what to do with it, how to manage it, or how to use it for communications with their stakeholder groups and consumers. Stakeholder groups in agriculture often miss out on opportunities to talk among each other, create a lexicon of words that all can agree on, and educate one another about the aspects they value, what they deem important, and how it can affect purchasing behavior or usage statistics. This project lies within these spaces, at the nexus of stakeholder groups, looking to create synergistic relationships in order to not only spread the land grant mission, but educate multiple stakeholder groups in the advancement of the agriculture industry. Using the

SmartFarm Innovation Network and partnering with community college and industry partners, this project analyzes the lens that stakeholder groups operate under related to cyberbiosecurity and big data.

An Educational Primer for Foundational Concepts of CyberbioSecurity – In Support of Empowering Agricultural Educators

Generally, small agricultural operations do not have the benefit of dedicated information technology support that is focused on maintenance of cybersecurity. This leaves our seed and plant/crop agribusinesses, animal breeding and production enterprises, food processing, and retail industries, and the associated supply chain vulnerable to cyber-attack as the weakest links within the food system. Our agriculture and food system needs a trained workforce at the interface of life sciences and biosecurity, physical systems, and cybersecurity: cyberbiosecurity. Agricultural education, in formal and non-formal contexts, is an essential component of the pipeline into agricultural careers, but cybersecurity is just emerging as a topic in these programs. Within rural communities, contextualizing cybersecurity within the agriculture and food system represents a unique opportunity to spark interest in the emerging field of cyberbiosecurity. A majority of the food production and agribusinesses that support the agricultural industry are situated in rural environments. 4-H and school agricultural programs in rural areas provide youth hands-on opportunity to explore STEM careers associated with this industry. However, existing programs integrating cybersecurity with life sciences applications are significantly lacking, limiting the potential for educators [university faculty, extension specialists and agents, middle school and high school educators] to enter into youth development in cyberbiosecurity. This project designs strategies and supporting materials for translating important concepts of relevance to cyberbiosecurity and overarching concepts of life science in the context of education, including: designing foundational documents that facilitate entry level concept understanding, language, and operational use; characterizing design elements needed for open educational resources. In particular, this project will develop an interdisciplinary primer describing the basic elements of the nascent cyberbiosecurity space. This will be accomplished by integrating terminology of relevance for biosecurity, cybersecurity, and cyber-physical security in context with life science, agriculture, and education and identifying and creating conceptual templates for Open Education Resources and FACT sheets targeted for middle school youth.

Integrated Implementation of Real-time Monitoring Tools, Data Analytics, and Treatment Technologies in Soilless Agriculture

Soilless agriculture based on large scale hydroponic systems has becoming increasingly popular because it is considered as environmentally friendly agriculture. Soilless agriculture has the potential for crop production all-year round in climate-conditioned facilities, less transportation costs, reduced land area and quality requirement, greater control of food safety and biosecurity, and substantially reduced inputs with respect to water supply, pesticides, herbicides, and fertilizers. Hydroponic systems therefore represent an ideal application context for Smart Agriculture that requires various cutting edge cyber-physical system technologies and data analytics services.

Integrated implementation of real-time monitoring tools, data analytics, and treatment technologies would clearly help improve timely decision on treatment and reuse of the exhausted hydroponic solutions at the end of a productive cycle. Ultimately, it would result in water and fertilizer savings, safer produce for human consumption, and less negative environmental impact on the affected water and soil resources. Seed funding is requested to work with the newly established Controlled Environment Agriculture Innovation Center in Danville to accomplish the following objectives: initiate research integrating real-time water monitoring tools, data analytics, and treatment technologies; establish collaborative experiential learning opportunities between the undergraduate students enrolled in Computer Science and Information Technology Program at Danville Community College and those major in Environmental Sciences at Virginia Tech, both institutions part of SWVA CCI; and facilitate connections and collaborations with private companies in SWVA.

Technology Driven Tools for Horse Owners, Trainers and Riders

Nutrient requirements of adult working horses are dated and poorly defined owing to an absence of metabolic data underlying performance measures. The Middleburg Agricultural Research and Extension (MARE) Center, located in the Northern Virginia technology corridor, is uniquely positioned to fill this void by developing new predictive models that couple workload with nutrient intake and metabolic outputs. Relying on inertial sensors and high-speed cameras, the big data phenotyping project will provide the basis for workload modeling efforts that define nutrient requirements for horses. The objective of the grant is to develop a smart app at the intersection of equine exercise and nutrition, provide experiential learning opportunities for engaged students, handle data captured with inertial sensors and high-speed cameras and transmitted to local and cloud storage devices for access by Blacksburg and MARE Center scientists for analysis. Additional benefits are continued partnership with the companies provides a solid foundation for development of commercial equine monitor, asynchronous learning opportunities that breach location and time barriers for students of all ages, and understanding the needs and expectations of the current student generation to accelerate design of appropriate on-line STEM learning modules.

Ultra-low and Multiscale Latency 5G

We aim to implement a private 5G cellular network to support research for secure CPS, thus providing a model that can be propagated throughout the CCI Network to create cellular networks for other nodes specifically designed with extra security and robustness and creating an even larger scale network that would attract partners across the base of Virginia technology companies and potential sponsors. This will enable the nodes to demonstrate the utility of the testbed, supported by skilled researchers who know how to use it, drawing local and distant industries to support their R&D efforts. The intellectual property resulting, such as new security approaches, mechanisms for rapid deployment and management, and specific network slices could become valuable to Virginia-based start-up companies. Low latency solutions are essential to the military who may seed commercial industries to restart U.S. manufacturing of wireless infrastructure.

5G Energy Slice and Securing the Power Grid

The US power grid is a critical infrastructure that still relies on a slow and inefficient supervisory control and data acquisition systems for monitoring, control, and operation. On top of the power infrastructure reside layers of information and communications technology that are interconnected with electric grids, constituting a large, complex cyber-physical system. As the power infrastructure has evolved into one with highly connected network environments, the use of firewalls has become a widely adopted access control method against intruders, but firewalls themselves do not guarantee cybersecurity. Consequently, the utility companies are now considering the transition from their current dedicated communication lines to 5G networks not only to address the above mentioned, but also to accommodate large numbers of devices and massive amounts of information within the Internet of Energy (IoE) concept. Moreover, the unrelenting progress in the power electronics field has been the primary reason for massive deployment of renewable energy resources over the past several decades, silently insinuating the necessity for serious revision of conventional practices in electricity production, distribution, and consumption at all levels – from portable electronics to power grid itself. It will not be long before all human energy needs are dominantly provided by electricity and delivered through the power electronics converters functioning as energy routers. Recent reports by the White House suggest that power grid outages cost the U.S. economy $18B to $33B annually. The U.S. utilities already spend between $1M to $10M annually on cybersecurity to meet the NERC (North American Electric Reliability Corporation) standards. However, due to the growing sophistication of computer hacking, there is an increasing need for technologies to secure the power grid. The legacy nature of both physical and cyber layers of the power system provides opportunities that we will pursue and challenges we will address. These include cybersecurity threats, high penetration of distributed and renewable energy systems, low inertia operation of the power system, advanced information and communication technologies as well as physical security issues including intrusions and sabotage and extreme weather events in which the rapidly expanding connectivity leaves the power system prone to cyberattacks. By building a modular testbed, with potential for expansion in future, we can assess the impact of cybersecurity threats and performance of their mitigation methods.

Transportation and Secure Communication between Autonomous Systems

Autonomous vehicles are expected to penetrate the marketplace in the next few years, yet studies have shown than hackers can cause harm to autonomous vehicle occupants, and have demonstrated the feasibility of attacking vulnerable automotive systems. Safety threats might be mitigated if one could quickly identify attacks, but it is not clear that traditional cybersecurity threat detection approaches are well-suited to connected and autonomous vehicles. Secure 5G communications may be the key to unlock the promise of autonomous transportation systems. Low-latency, security, and reliability are clearly necessary for the transportation sector, where lives and livelihoods are on the line. Other concerns with connected and autonomous include confidentiality (privacy of driver information and locations), integrity (of firmware and onboard data between sensors), and availability (risk of denial of service as attackers render a connected car non-responsive, even while driving). All of these add up to a large public safety risk and will hinder the adoption of the technology if breakthroughs are not made soon. There are several communications protocols used or planned today, the two most common are Digital Short Range Communications (DSRC) and Cellular Vehicle to Everything (C-V2X) which will run over 5G. Security is lacking across both protocols. We will test autonomous vehicle security through the 5G network, connecting with the 5G testbed and autonomous vehicle research facilities, allowing for remote testing capability that could simulate and perhaps actually perform end to end remote testing of autonomous vehicle security.

Cyberteam VIPs

SWVA CCI will provide a self-sustaining pipeline for many research and credentialing activities via undergraduate research engagement through the Vertically Integrated Pro-jects (VIP) model, creating the potential for a sustained involvement and cross-pollination of cybersecurity research; community college students will benefit from this enhanced learning experience; graduate students project experience will be supported as they engage in project work in the security of CPS; industry and education partnerships through shared research facilities; high growth in cyber skilled workforce through alignment of curriculum in its community college base and proliferation of hybrid/online certificate programs via shared resources; high-wage jobs through the growth of a targeted industry cluster.

Research Engagement Programs

Collaboration within the node and within the network is encouraged via Research and Collaboration Grants. This program allows researchers to build a collaborative network throughout Virginia and beyond, accelerating commercialization as well as scholarly output, with the support of the node. Dedicated resources are devoted to promoting the work of researchers to ramp up to engage in the key areas identified above or other CPSS research leaning toward commercialization. Access to shared equipment is another way in which research will be strengthened through the node and network.

Research Faculty Recruited

Given COVID-19 situation, researchers made temporary use of existing faculty as a stopgap measure in FY20. While FY20 supported a number of researchers, graduate students, and undergraduates, no new faculty were recruited during this time. Hiring of research faculty will take place in FY21.

Results of Entrepreneurship and Workforce Programming

SWVA CCI aims to encourage for budding entrepreneur via several coordinated efforts, including developing training modules and embedding participants so that they are generating research while participating in a mentorship program with an entrepreneurial focus. Thus, this entrepreneurial mindset is communicated to the team, via a train-the-trainer method.

Cyber Dashboard for Southwest Virginia

To increase cybersecurity-related new venture activity and bring increased visibility to cyber efforts in Southwest Virginia, SWVA CCI is partnering with the Valleys Innovation Council (VIC), a nonprofit organization launched in January 2018 to connect, communicate, and collaborate with regional stakeholders to support the region with a focus on the innovation economy. VIC is cultivating an ecosystem for high growth potential, technology-based start-ups. To this end, VIC is working to improve access to capital, develop mentorship and acceleration programming, and improve the awareness of technology sector job opportunities in the region so that growth companies can attract the talent needed to scale a company. Existing and Emerging Technology Industry Clusters relevant to the node have been identified through studies performed by the Virginia Tech's Office of Economic Development. These clusters offer critical mass and value chain partners that support virtuous cycles of growth and innovation, including blockchain applications, software applications and data analytics; advanced manufacturing; and transportation and autonomy. Equipped with this information and VIC's economic projections, the node targets particular opportunities for growth and leverage resources to attract attention the cyber expertise in the region and greater Commonwealth. The development of a Cyber Dashboard for Southwest Virginia is underway to showcase cyber opportunities in the region.

Startup Toolkit for Early Stage Potential Ventures

A startup toolkit that can be used for early-stage potential CCI ventures is under development. The toolkit is intended to provide a structured approach to new venture readiness. It leverages some concepts of a technology commercialization toolkit that currently under construction in VT's LICENSE LAUNCH organization. Students were engaged in the creation, including some with keen interest digital technology-based startups, providing early student exposure. The toolkit will serve as a launch point for those interested in commercialization, especially graduate students, postdoctoral researchers, and faculty as well as an upcoming FY21 cohort-style program.

Online (Cyber) Range Readiness and Reach

Online modules are being developed to increase accessibility to and applicability of the CyberRange for K-12 teachers and community college faculty. A platform prep to Cyber Range readiness will broaden participation at both the instructor and student levels by introducing the operating system utilized by the Virginia Cyber Range. Additional modules will be designed to support teachers in taking advantage of the more advanced Cyber Range materials, thus yielding increased student exposure throughout the Commonwealth. Module delivery will be asynchronous to give teachers maximum flexibility in the making full use of the Cyber Range.

Automotive Cybersecurity VIPs

Initiated in May 2020, researchers at the VT Hume Center established an undergraduate experiential learning team for Automotive Cybersecurity, following the Vertically Integrated Projects model used in other Hume projects. The core objective of that VIP model, illustrated in Figure 2.49, is to create a long-term research opportunity (5-10+ year projects) for students that serves as a thematic student pipelines where (1) students may engage in sustained research for a period of 3 years, (2) senior students assist in mentoring incoming students, and (3) feedback from project sponsors and recruiters is integrated into future project objectives. For the automotive cybersecurity team, an initial collection of 7 students were recruited for summer internships and given the charter of performing literature surveys to support future automotive cybersecurity sub-teams. Specific areas of focus included physical- and cyber-security pertaining to:

- Automotive infrastructure: Focuses include road side units, signal cabinets, roadside sensors / actuators, traffic signal pre-emption systems, and core networks to DOT systems.
- Use and implementation of cryptographic primitives in vehicles: Focuses include secure credential management system (SCMS) protocols for PKI certificates, cryptographic algorithms within ECUs, device authentication.
- Communications internal to a vehicle: Focuses include Controller Area Network (CAN) bus, Local Interconnect Network (LIN) bus, and connectivity via the On-Board Diagnostics (OBD) II port.

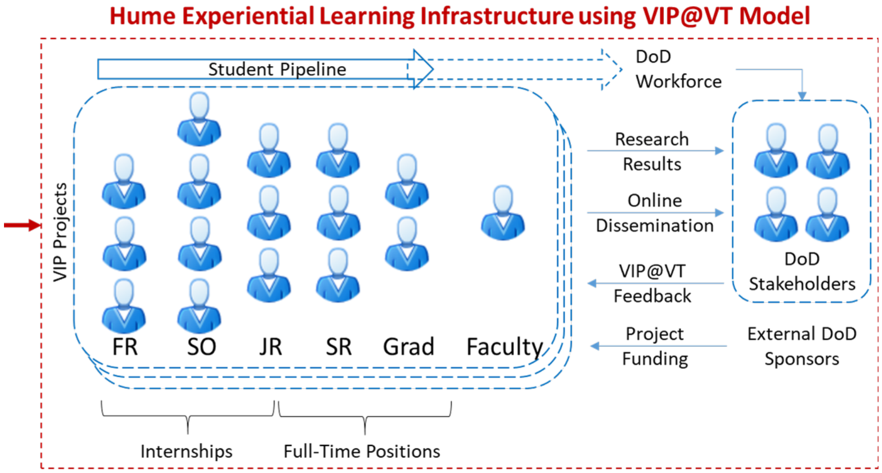


Figure 2.49: Hume Experiential Learning Infrastructure using VIP@VT Model

- Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications: Focuses include Dedicated Short-Range Communications (DSRC / 802.11p) and emerging standards for V2V/V2I projects.
- Application of quantum-based optimization algorithms: Focuses include routing optimization and operational optimizations within the vehicle, building upon industry sponsored projects.

In each of the project topic areas, students were tasked with generating an ‘annotated bibliography’ (300 total sources) that captures relevant sources and begins to synthesize the results into the foundation for future specific research efforts. Finally, towards the end of the summer, the entire team was tasked with identifying potential attacks on the vehicle OBDII port, developing a prioritized list of candidate attacks and verification methods that will be explored in FY21.

Collaborative Partnerships and Projects

SWVA CCI leverages node and network partnerships, research, and resources to enhance positive regional economic development through the acceleration of cyber startups and technology commercialization. This began in FY20.

Virginia Testbed for 5G Power Grid (5GPG)

The electric power system is a critical infrastructure. As a legacy system, both physical and cyber layers of the power system were designed without anticipation of the modern technologies and their associated opportunities and challenges, e.g., cybersecurity threats, high penetration of distributed and renewable energy systems, and advanced information and communication technologies. To advance the Commonwealth’s research capabilities and infrastructure for cyber-power system research, this project supports the creation of a modular testbed, with potential for expansion in the future, that can provide an environment for co-simulation, -emulation, and - experimentation of both physical and cyber aspects of the power system. This testbed will leverage existing facilities and equipment available at Virginia Tech’s Power and Energy Center (PEC) and Center for Power Electronics Systems (CPES). This testbed will integrate very closely both physical and cyber facilities to position the State of Virginia as a leader of a new research field to enable the future power grids with the emerging 5G communication capabilities. Indeed, the envisioned “5G Power Grid (5GPG)” will allow power systems to greatly enhance the monitoring, operation, control, protection, and trading functions. A design of the 5GPG testbed has been developed, and is illustrated in Figure 2.50. The testbed will include the following components:

- Power System: This includes a real-time simulation platform, RTDS, and scaled-down lines, including microgrid topologies. PEC is progressing well in acquiring on-line power grid operational data from VT Electric Service (VTES). Some online data have already been received. A secured area in the lab is being set up for the VTES data.
- Distributed Energy Resources (DER): DERs include PV (actual) and wind (emulated) and battery (actual) as well as microgrid resources interconnected to the rest of system via an inverter-amplifier combination.
- Load: The testbed includes load devices. Some resistive loads will be connected to the power system via a converter to enable control, power factor modulation, and single-phase operation.
- Controllers: Controllers at different timescales have been included; higher-level central controllers, e.g., SCADA will entail communication representation. The proposed testbed includes microgrid controllers.
- Network: Connecting the 5GPG testbed to the 5G testbed in Arlington (Wireless@VT) is in process. The connection will enable the 5GPG devices and systems to deliver measurements and control commands through the 5G testbed. Connectivity with the 5G facilities at GMU is also under development.

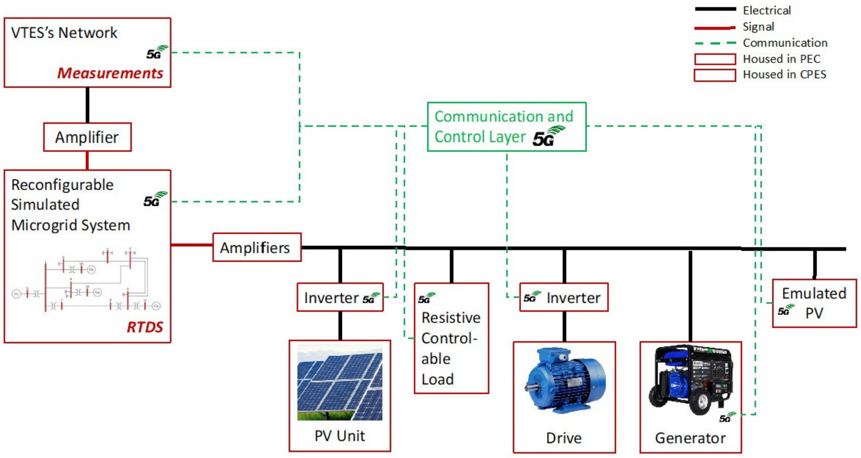


Figure 2.50: High-level depiction of the components of 5GPG testbed.

Additionally, system-level simulations are being conducted on the notional microgrid featuring photovoltaic, energy storage, wind power converter, and distributed load to demonstrate advantage of utilizing communication between system power converters over 5G network. Test cases include islanding, resynchronization, protection, and control-mode changes to avoid system instability due to loss of grid. The team has made a significant progress on utilization of the White Rabbit protocol for fast subnanosecond synchronization between power electronics cells within a power converter (work funded by the Office of Naval Research). Building on this concept the team is now exploring the use of the 5G network for system-level clock synchronization in a 4 microseconds range between power converters and microgrid controller, as well as between power converters directly, in order to achieve fast time-stamped data exchange. Through this project, a state of the art microgrid testbed is being deployed at Virginia Tech in Whittemore Hall. The testbed will enable hardware in the loop simulation of the power system with power electronics in a microgrid setting. The testbed is being built with modularity in mind to allow expansion in the future, with some opportunities summarized in Figure 2.51.

Multi-university Proposal Development for Efficient Measurement of Robustness/Resilience of Spectrum Sharing 5G Networks to Physical and Higher-layer Attacks

SWVA CCI researchers are developing effective, efficient performance measurement of spectrum-sharing radios and networks and systems such as spectrum access systems (SAS) that coordinate spectrum use.

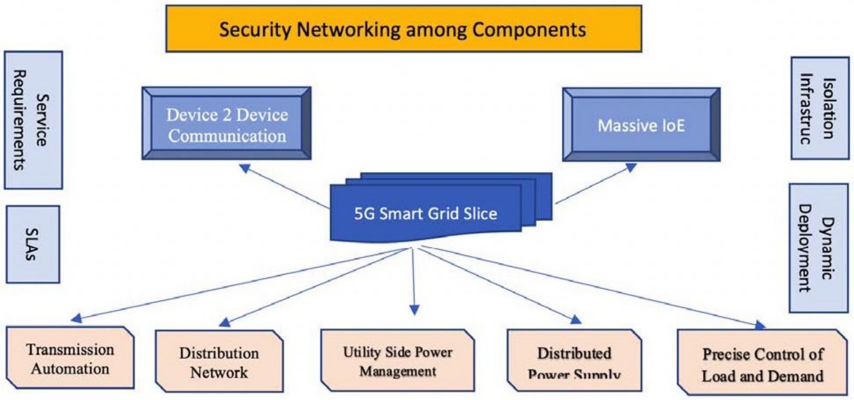


Figure 2.51: Summary of components of and opportunities afforded by 5GPG.

Novel testing approaches can be used to accelerate the research and development process, assess compliance with regulations, and enable objective comparisons between competing products. Sharing Federal radio frequencies with commercial users is needed to meet fast-growing demand for wireless data capacity for video, the Internet of things, telehealth, and increasingly for intelligent transportation systems including self-driving vehicles, UAVs / UAS, and other emerging applications. Early adoption of spectrum sharing by the US is expected to have great social and economic benefits, and will require real-time decisions regarding how radios and networks use shared frequencies, and security of the wireless systems and the applications that they serve depends on robustness of these decisions to a variety of potential attacks including jamming, MAC layer attacks, physical denial of service, primary user emulation, and spectral honeypot attacks.

Currently, VT operates a cognitive radio testbed (Figure 2.52), which is being leveraged in support of a large project on the robustness and resilience of spectrum sharing 5G networks to physical and higher-layer attacks. Figure 2.53 illustrates the testbed development and testing approach envisioned.

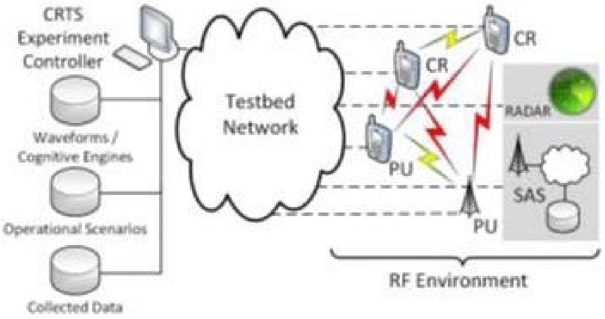


Figure 2.52: Current infrastructure from VT's Cognitive Radio Test System and CORNET radio testbed.

Preliminary research and proposals for a more extensive project are under way with researchers from George Mason University, MIT, and the Air Force Institute of Technology to:

- Model decision-making and performance of spectrum sharing radios, networks, and spectrum access systems, including specific abilities like detecting weak signals, adapting quickly, or recognizing patterns, and making robust adaptations despite attacks that attempt to manipulate them;
- Use several statistical, optimization, and testing methods to develop reliable and efficient tests for the radios and networks; and
- Evaluate radio and network performance through experiments and large-scale simulations.

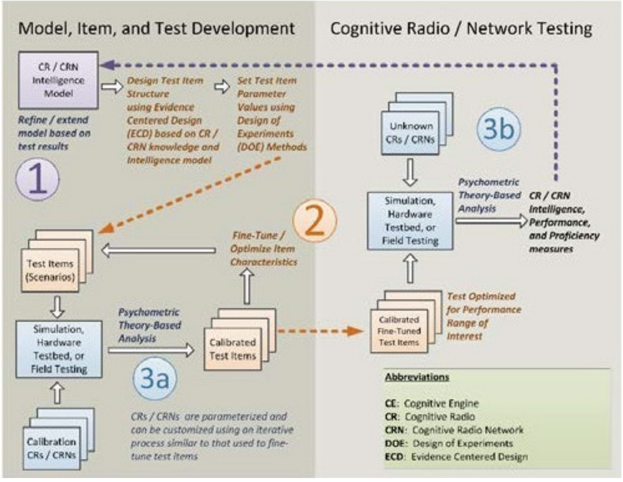

Model, Item, and Test Development
Cognitive Radio / Network Testing
CR / CRN Intelligence Model
Refine / extend model based on test results
1
Design Test Item Structure using Evidence Centered Design (ECD) based on CR / CRN knowledge and intelligence model
Set Test Item Parameter Values using Design of Experiments (DOE) Methods
2
Fine-Tune / Optimize Item Characteristics
Test Items (Scenarios)
Simulation, Hardware Testbed, or Field Testing
Psychometric Theory-Based Analysis
Calibrated Test Items
3a
Calibration CRs / CRNs
CRs / CRNs are parameterized and can be customized using an iterative process similar to that used to fine-tune test items
Unknown CRs / CRNs
3b
Simulation, Hardware Testbed, or Field Testing
Psychometric Theory-Based Analysis
CR / CRN Intelligence, Performance, and Proficiency measures
Calibrated Fine-Tuned Test Items
Test Optimized for Performance Range of Interest
Abbreviations
CE: Cognitive Engine
CR: Cognitive Radio
CRN: Cognitive Radio Network
DOE: Design of Experiments
ECD: Evidence Centered Design

Figure 2.53: Example testbed development and testing approach for Robustness/Resilience of Spectrum Sharing 5G Networks to Physical and Higher-layer Attacks.

Secure Wireless IoT Sensors for Smart Farms

The College of Agriculture and Life Sciences of Virginia Tech has provided a seed fund to establish "Smart Farms" at Middleburg and Shenandoah Valley Agricultural Research and Extension Centers located in Virginia to enable the exploration of strategies to enhance usability of technology in pastoral livestock production systems. The system will leverage IoT technologies to enable animal care personnel to monitor the behavior and health of cattle remotely through the Internet. Naturally, the communications through the Internet expose cybersecurity vulnerabilities that can be easily exploited by cyber attackers aiming to disrupt the normal system operations and functionalities. SWVA Node researchers complement the above "Smart Farms" research by considering information security in wireless IoT sensors to ensure the trustworthiness of information for the cattle monitoring system. This project leverages machine learning/deep learning (ML/DL) techniques to process a large amount of high dimensional data collected from the wireless IoT sensor networks, with the aim of extracting trustworthy information with high certainty. The wireless IoT sensor system measures major biometrics of cattle, such as body temperature, heartbeat rate, weight, distance traveled with a GPS, activity and behavior with a 3-axis inertial accelerometer. These data will be leveraged to develop uncertainty-aware and robust ML/DL algorithms in the presence of cyberattacks to accurately assess animal health status. In addition, application of the uncertainty-aware ML/DL algorithms drastically reduces an immense amount of data generated by the sensor system, enabling the adoption of the low data rate and low power communication protocol, LoRa (Long Range).

SWIFT: Southwest Wireless Information Freshness for Power Grid Technologies

The collaboration goal of this project is to capitalize on the expertise in power system (Power and Energy Center) and communication (Wireless@VT) and evaluate the impact of communication non-idealities within the CCI-funded 5G for the Power Grid (5GPG) testbed being developed at VT. This is important as the power system and communication networks have become increasingly interdependent due to the need to increase wide-area situational awareness in a grid with increasing distributed/renewable energy resources. This project creates models and experiments that enable the study of the impact of information freshness, measured as Age of Information (AoI), on the power system. Along this route, we also identify power system features (e.g., measurements, statuses, and renewable generation predictions) that have a dominant impact on the grid's performance so they need to be given priority in utilizing the limited network bandwidth. These efforts will contribute to the understanding of how future 5G networks will enable new distributed and decentralized functionality for the power system. The intellectual challenges in the proposed research vision require close synergies among experts in power engineering and communications engineering. Additionally, this project will inform the design of the communication aspects of the 5GPG testbed we are creating at

Virginia Tech under a separate CCI support project.

Secure Communication between Autonomous Systems

The Virginia Tech Transportation Institute (VTTI) is supporting SWVA CCI via autonomous system security testing in the context of remote operation through secure communications between ground, aerial, and infrastructure. Building upon VTTI's existing Automated Truck Mounted Attenuator (ATMA) platform, CCI funding has provided an opportunity to investigate and develop two useful additions: 1) Remote Operator, providing remote control and a live video feed allowing a remote operator to safely maneuver the ATMA around unexpected hazards, and 2) a paired UAV that provides operators with a live aerial video feed of the ATMA and mobile work zone environment. Establishing and verifying secure communications via CV2X are a critical component for safe deployment.

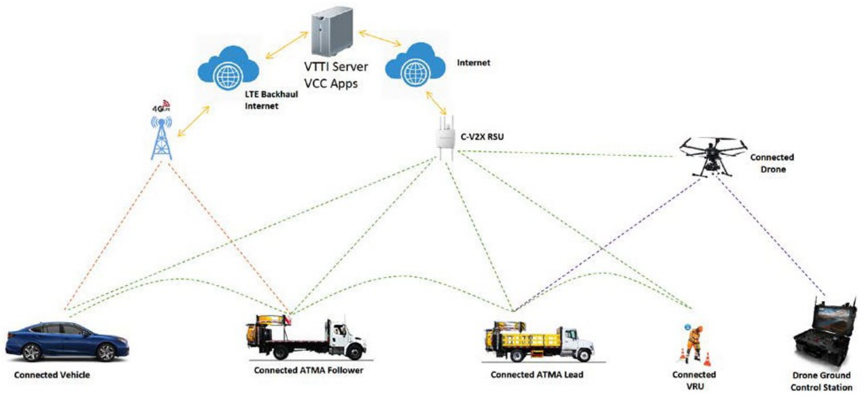


Figure 2.54: High-level depiction of communication between autonomous systems as related to transportation project involving Automated Truck Mounted Attenuator (ATMA), UAV, and remote operator

This project sets out to perform autonomous system security testing in the context of remote operation, as illustrated in Figure 2.54. Proposed test concepts aim to combine secure communications between ground, aerial, and infrastructure components, contributing to communication standards between actors within the targeted context. Efforts undertaken address research gaps in terms of secure interaction between an automated vehicle and a remote operator, as well as an unmanned aerial vehicle (UAV) and ground vehicles. Proposed concepts build upon VTTI's existing Automated Truck Mounted Attenuator (ATMA) platform, which provides an automated solution to a mobile crash barrier. TMA's are often used in work zone support, but present significant risks to a driver should a rear-end collision by another road user occur. As such, the ATMA concept eliminates the need for a driver by using a leader/follower strategy, where the ATMA follows a lead vehicle associated with the mobile work zone, but at a safe distance. CCI funding has provided an opportunity to investigate and develop two useful additions:

- Remote Operator: current limitations in automation make it likely that remote operation will be required in order to maneuver around unexpected hazards, further maintaining the safety advantage of not requiring a human operator controlling the ATMA from the driver's seat. Secure control mechanisms and protocols, as well as live video is required to support operator decision making
- UAV support: a paired UAV that maintains a prescribed, relative position through continuous and secure communication with the ATMA would assist work zone personnel in monitoring the environment around the ATMA, particularly to the rear. This live video feed provides operators with useful information regarding the mobile work zone's possible interference with normal traffic flows, while also useful for detecting incidents involving ground vehicles for post review and analysis

In both cases, establishing and verifying secure communications via C-V2X are a critical component for safe deployment.

To date, VTTI has successfully implemented the remote operator concept. The basic scenario envisioned is a cone or construction barrel that blocks the ATMA's path while in autonomous follow mode. Upon detecting the hazard, the ATMA automatically brakes to a stop, interrupting the lead follow pairing between the ATMA and lead work-zone vehicle. In order to safely maneuver around this new hazard, a remote operator in the lead vehicle can request control via an internally developed human machine interface (HMI), and provide throttle, steering, and brake input through a joystick controller. In its current format, the remote operator maintains line of sight of the ATMA, while also having access to a live video feed and vehicle parameters such as speed, brake position, throttle position, steering position, and vehicle error states. Thresholds for throttle input and max achieved speed ensure that speeds are kept at a minimum while under the remote operator's control, and multiple emergency-stop methods are in place. Once safely around the hazard, the remote operator, using the HMI, can transition back to the ATMA's follow-mode. Efforts to finalize the communication approach and the HMI continue. Final validation will also ensure seamless transition throughout the scenario described herein. Development continues with the UAV concept, and significant progress is expected during the upcoming review period.

Note: The VTTI research team changed the approach of this effort at kickoff to address changes partially due to the departure of Liberty University as team members (due to staffing changes at Liberty).

Correlated economic outcomes (jobs and new business formation)

In FY20, SWVA CCI kicked off a number of research, innovation, and workforce development projects which support the Regional Innovation Ecosystem and Talent Pipeline and ultimately bring economic growth to Southwest Virginia. Additional funding will be used in FY21 to further invest in programs that facilitate job and new business creation.

Geographic distribution of awards from the funds contained in HB30

The funds spent in FY20 were distributed as follows: VT ($755,485); Radford ($14,917); and UVa ($5000). As noted above, some changes were made to the planned distribution in light of COVID-19 and staffing changes at some partner institutions. SWVA CCI looks forward to further engagement across the node and larger network in FY21.

2.5.3 Additional Programs, Projects, Accomplishments

Two faculty from SWVA CCI were selected as CCI Fellows as part of the 2020 cohort

Dr. Kevin Heaslip (VT) and Dr. Jeff Pittges (Radford). Through the CCI Fellows program, Dr. Heaslip is using his expertise in AI and CPSS in infrastructure to further the AI-team research and external funding opportunities, provide workforce development opportunities, and actively explore patents for technologies developed from the research conducted as well as the forming of companies to commercialize research. As a CCI Fellow, Dr. Pittges is creating pipeline infrastructure to prepare students for and connect students with industry employment opportunities.

Dr. Jon Black (VT) leads the Drone Racing Competition - Learning, Defending, and Attacking which is funded via the hub's Scalable Pilot Programs for Experiential Learning in CCI. Aligned with CCI's aims of developing and enhancing experiential learning projects at the intersection of cybersecurity, autonomous systems, and data, this project will build multidisciplinary teams across the SWVA CCI and Commonwealth to compete in "battle" drone racing competitions.

2.6 CCI in the Media

Many of the programs and major milestones from CCI researchers and operations staff have appeared in the print and online media. The following is a list of media hits from December 2019 to September 2020.

- **Virginia Commonwealth University**, September 9, 2020: "VCU named National Center of Academic Excellence in Cyber Research".
- **Virginia Business**, August 29, 2020: "A sense of possibility: Commonwealth Cyber Initiative's first executive director aims high".
- **Virginia Commonwealth University**, August 4, 2020: "Doctoral student takes top honors at major digital forensics conference".
- **Virginia Business**, August 3, 2020: "Commonwealth Cyber Initiative names managing director: John P. Delaney is a former chief of staff for Army Cyber Command".
- **George Mason University**, July 7, 2020: "Commonwealth Cyber Initiative (CCI) NoVa Node announces winners of Cyber Advanced Translational Research Development Grants".
- **Richmond Times-Dispatch**, June 17, 2020: "Luiz A. DaSilva column: Accelerating secure technology during and after a pandemic".
- **The Roanoke Star**, June 1, 2020: "Commonwealth Cyber Initiative Awards Learning Grants to Faculty and Students Across Virginia".
- **Virginia Tech**, May 26, 2020: "Commonwealth Cyber Initiative awards experiential learning grants to faculty and students across Virginia".
- **Virginia Pilot**, May 25, 2020: "ODU cybersecurity program gives out $680,000 in research grants".
- **Old Dominion University**, May 22, 2020: "INNOVATE Cyber Challenge: ODU Takes the Lead Toward Preparing the Commonwealth's Cybersecurity Workforce".
- **George Mason University**, April 6, 2020: "Commonwealth Cyber Initiative (CCI) NoVA Node announces call for proposals".
- **Richmond Times-Dispatch**, February 28, 2020: "Todd Stottlemyer and Jim Dyke column: Virginia leadership in the cyber dominion".
- **George Mason University**, February 18, 2020: "George Mason University establishes first-of-its kind Cyber Security Engineering Department".
- **Virginia Pilot**, December 18, 2019: "ODU awarded $3 million to boost cybersecurity workforce".
- **George Mason University**, December 12, 2019: "Mason to unveil a new Cyber Living Innovation Lab as part of the CCI".

Chapter 3

Financial Report

3.1 CCI Hub

The CCI Hub FY20 budget was $10M to establish Hub operations, hire research faculty, initiate network research projects and establish network programs. A significant portion of Hub funds were allocated to the Regional Nodes or for network programs that benefit one or more of the Regional Nodes and focus on CCI's core missions. In FY20, the Hub transferred approximately $2.6M to the Nodes to support the CCI Fellows program, six Experiential Learning Pilot programs, and development of the portions of the 5G testbed that are physically deployed in the Nodes. The vast majority of CCI Hub fund expenditures are dedicated to personnel and programs that act on behalf of the entire network and/or multiple stakeholders (universities, innovators, industry partners) and that have a whole-of-state impact that moves CCI and the Commonwealth closer to achieving its vision of Virginia positioned as a global leader in cybersecurity.

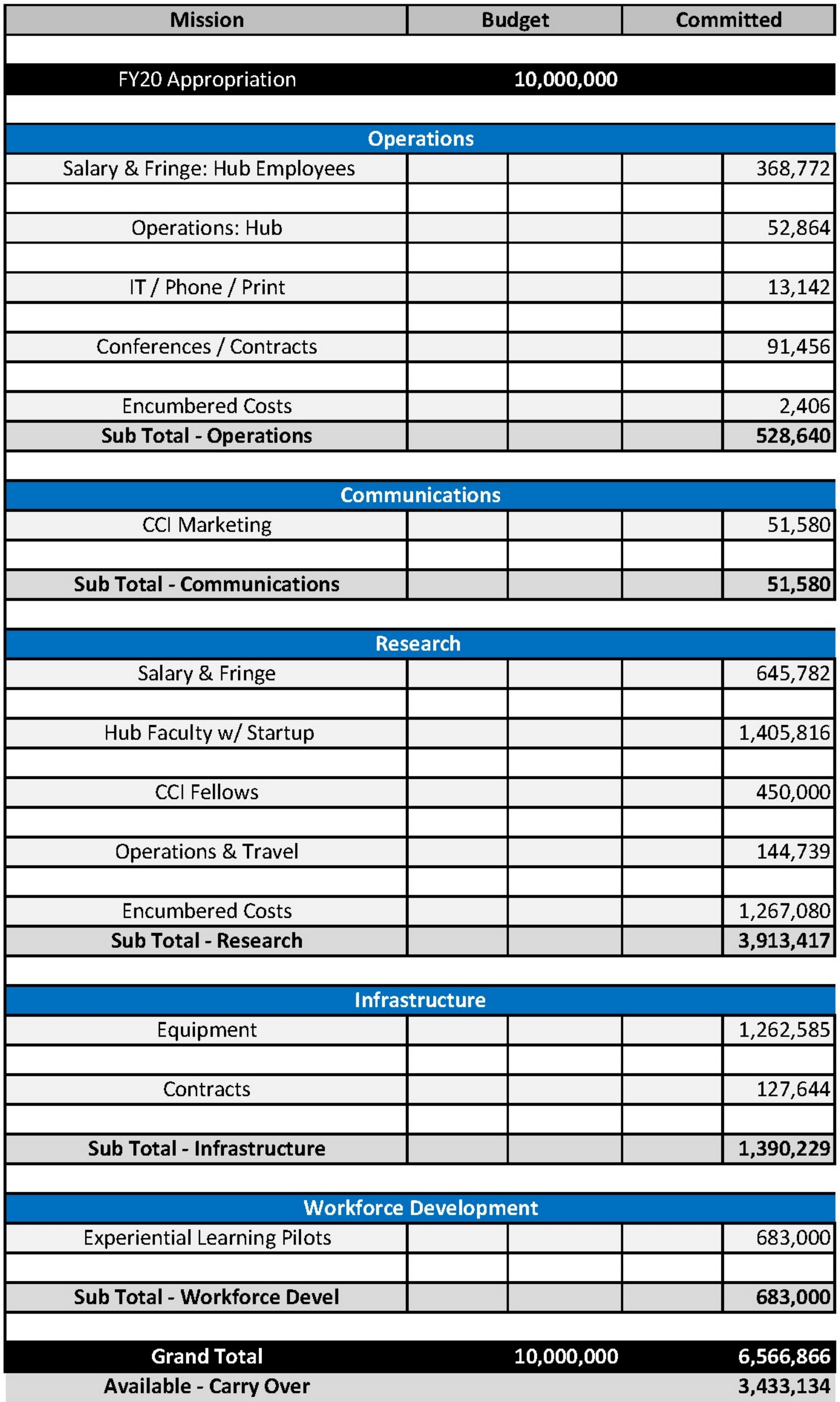
The budget and expenditures for the CCI Hub in FY20 are shown in Figure 3.1.

Due to long recruitment lead times, key personnel in the CCI Hub, including the Executive Director and the Managing Director, did not join until the last quarter of FY20. Other personnel, such as the Director of Communications and Marketing, the Director of the 5G Testbed, and the Director of the AI Assurance testbed, did not join until FY21. This resulted in substantial salary savings in FY20. In FY21, the Hub has suffered a budget reduction, from $10M to $7.5M. The carry over from FY20 will make up for this reduction, allowing the Hub to run the programs that were originally planned and that are described in Chapter 4.

3.2 CCI Nodes

In November 2019, the CCI LC on behalf of the four CCI Nodes submitted a request for Matching Funds to VRIC for $10M. VRIC approved these funds at their December 10, 2019 meeting. As part of the Matching Funds request to VRIC, each Node submitted a Spend Plan ensuring the expenditure of funds were aligned with the goals and strategies of CCI and the Commonwealth. Additionally, VRIC provided guidelines for the allocation of the funds as follows:

- No more than 25% of CCI funds requested shall be used for Node Operations / Commitment to CCI network;
- At least 50% must be used for the research category;

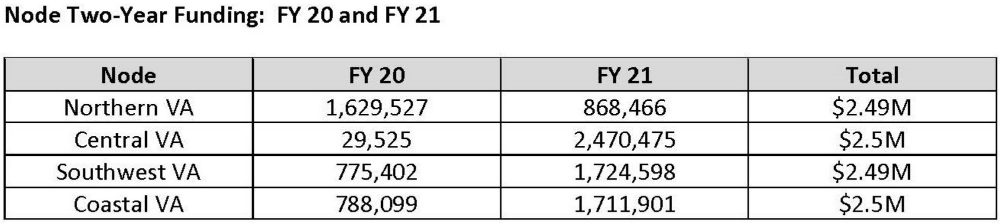


Mission	Budget	Committed
FY20 Appropriation	**10,000,000**	
Operations		
Salary & Fringe: Hub Employees		368,772
Operations: Hub		52,864
IT / Phone / Print		13,142
Conferences / Contracts		91,456
Encumbered Costs		2,406
Sub Total - Operations		**528,640**
Communications		
CCI Marketing		51,580
Sub Total - Communications		**51,580**
Research		
Salary & Fringe		645,782
Hub Faculty w/ Startup		1,405,816
CCI Fellows		450,000
Operations & Travel		144,739
Encumbered Costs		1,267,080
Sub Total - Research		**3,913,417**
Infrastructure		
Equipment		1,262,585
Contracts		127,644
Sub Total - Infrastructure		**1,390,229**
Workforce Development		
Experiential Learning Pilots		683,000
Sub Total - Workforce Devel		**683,000**
Grand Total	**10,000,000**	**6,566,866**
Available - Carry Over		**3,433,134**

Figure 3.1: CCI Hub FY20 Financial Report.

- The remaining 25% may be used for the Regional Innovation Ecosystem and Talent Pipeline categories.

The Node Spend Plans included programs to be carried out during FY20 and FY21, and the funds were apportioned within three categories spanning CCI's mission lines: Research, Regional Innovation and Talent Pipeline, and Operations. Each of the four CCI Nodes planned independently for how those funds would be budgeted to span the two fiscal years (Figure 3.2). While the funds were approved by VRIC in December 2019, they were not released to the Regional Nodes until February 2020, eight months into the fiscal year. Because of the participants' dedication to the CCI mission, many projects were initiated before CCI funds were received. This was accomplished through the use of university-contributed funds in lieu of appropriated funds during the unfunded portion of FY20, July 2019 – February 2020. This innovative funding method enabled the CCI Regional Nodes to initiate some research projects, submit proposals, and execute a limited number of programs during the early portion of FY20.



Node Two-Year Funding: FY 20 and FY 21

Node	FY 20	FY 21	Total
Northern VA	1,629,527	868,466	$2.49M
Central VA	29,525	2,470,475	$2.5M
Southwest VA	775,402	1,724,598	$2.49M
Coastal VA	788,099	1,711,901	$2.5M

Figure 3.2: Node Two-Year Funding: FY20 and FY21.

3.2.1 NOVA Node

The budget and expenditures for the NoVA Node in FY20 are shown in Figure 3.3.

Based on the robust engagement with the partners of the NoVA Node, a detailed strategic plan was developed in advance of the NoVA Node's call for proposals to support the tenets of the strategic plan. The LC approved funding for $2,497,993 of proposals in research, innovation and entrepreneurship, workforce development, and operations and administration. In FY20, $1,629,527 of these resources was budgeted, and a total of $1,575,222 was committed to the approved projects. Although FY20 resources were not received by the node until January 2020, the NoVA Node was able to advance its planned initiatives beginning in 2020 as a result of the investment of the NoVA Node's contributed funds and equipment. One project, "Building Capacity for a Cyber Workforce" involved funding stipends for summer internships in industry. Due to the COVID-19 pandemic, the NoVA Node decided to postpone placement of these interns until summer 2021. Therefore, the resources for this program have been reserved for FY21 instead of FY20. Also due to the ongoing restrictions associated with the pandemic, travel funds for the Node Director to attend meetings across the Commonwealth, and funds for printed reports and materials have been deferred to FY21.

3.2.2 CEVA Node

The budget and expenditures for the CeVA Node in FY20 are shown in Figure 3.4.

3.2.3 COVA Node

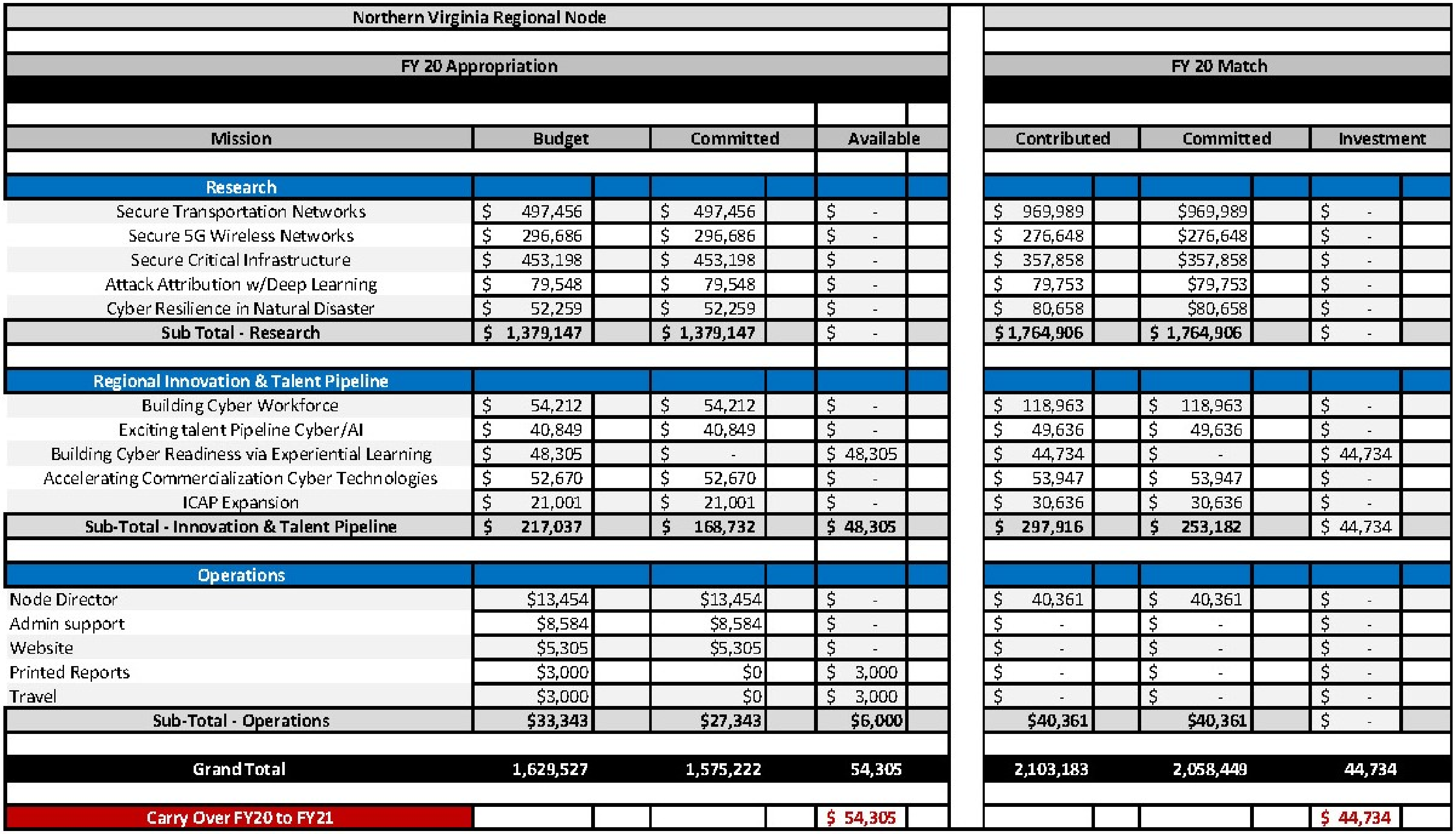
The budget and expenditures for the CoVA Node in FY20 are shown in Figure 3.6.

The Coastal Virginia Center for Cyber Innovation created a strategic plan aligning with the broader CCI goals. Based on this plan, a request of $2.5M was made to support Node activities. The LC approved the funding, with $788.099 allocated in year 1 (FY20) and the remaining funds committed to year 2 (FY21). FY20 funds were expended on building the Coastal Virginia Shared Academic and Research Environment, supporting collaborative research between Coastal Virginia higher education institutions, promoting innovative educational/workforce development, enhancing regional curricula, building new experiential learning programs, and supporting a robust internship program. The CoVA Node expended/committed all FY20 funds. In FY21, the Node will continue these programs and hire five research faculty across ODU, W&M, and NSU.

3.2.4 SWVA Node

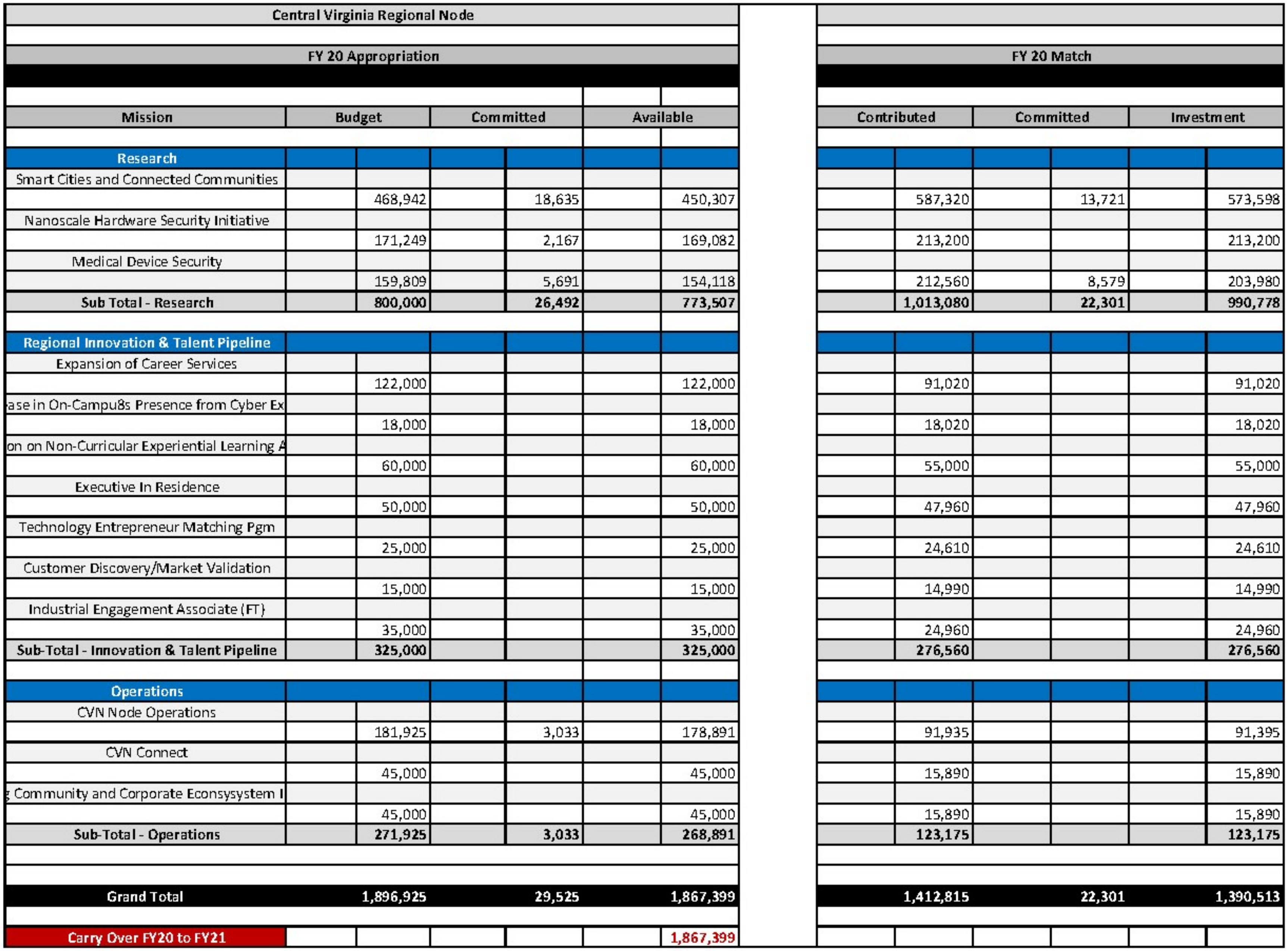
The budget and expenditures for the SWVA Node in FY20 are shown in Figure 3.7.

Along with the other CCI nodes, SWVA CCI submitted its strategic plan along with aligned initiatives in Research, Regional Innovation and Talent Pipeline, and Network Collaboration in November 2019. This document included detailed mission lines and a request for matching funds of $2,499,999 split over two fiscal years: $775,402 in FY20 and $1,724,598 in FY21. Although FY20 funds were not received until Spring 2020, CCI SWVA advanced its mission by beginning multiple efforts across research, innovation, commercialization, and workforce development. Some adjustment of funds at that time allowed CCI SWVA to make the best use of its FY20 resources, even when faced with the COVID-19 pandemic. For instance, some funds originally budgeted for internships were moved to Cyberteam VIPs to create research-oriented experiential learning opportunities in the wake of COVID-19.



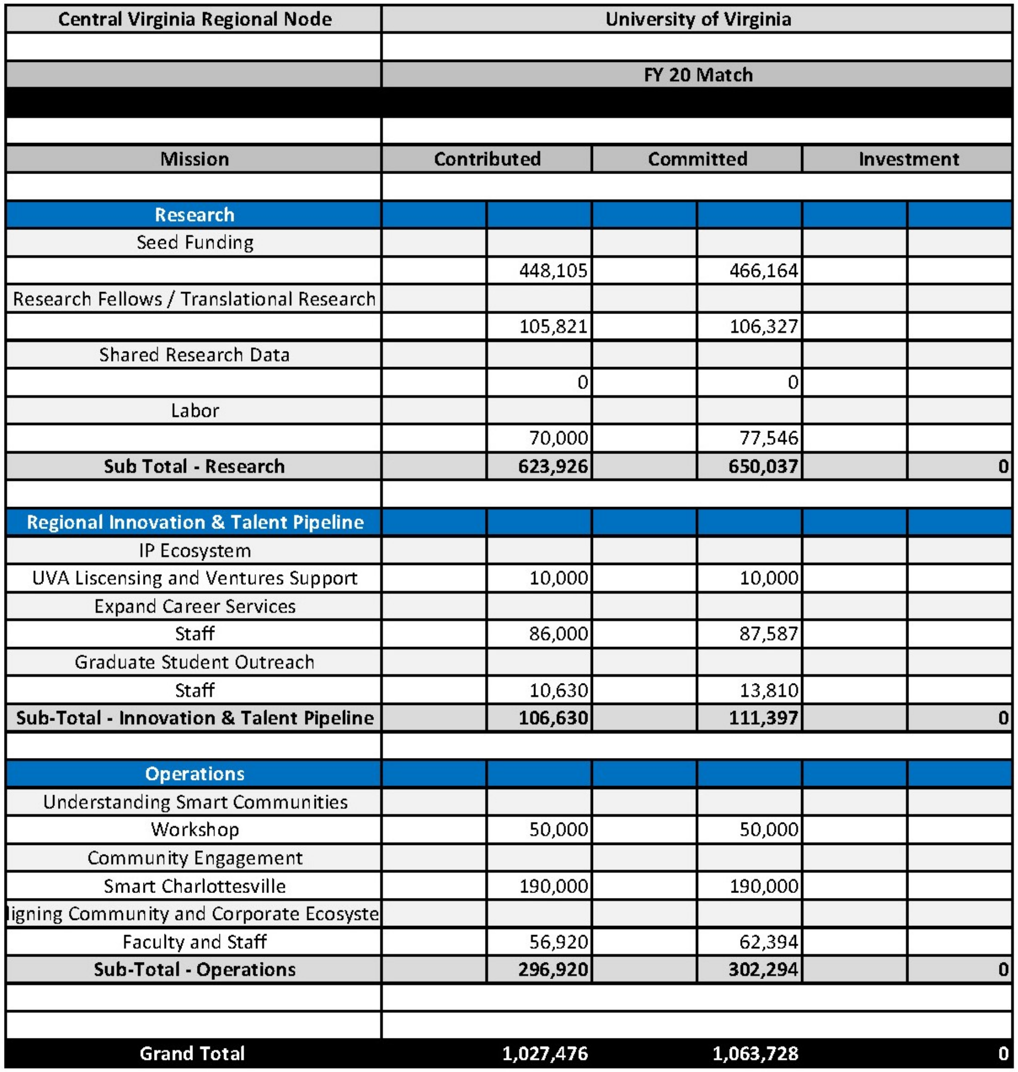
Northern Virginia Regional Node						
	FY 20 Appropriation			FY 20 Match		
Mission	Budget	Committed	Available	Contributed	Committed	Investment
Research						
Secure Transportation Networks	$ 497,456	$ 497,456	$ -	$ 969,989	$969,989	$ -
Secure 5G Wireless Networks	$ 296,686	$ 296,686	$ -	$ 276,648	$276,648	$ -
Secure Critical Infrastructure	$ 453,198	$ 453,198	$ -	$ 357,858	$357,858	$ -
Attack Attribution w/Deep Learning	$ 79,548	$ 79,548	$ -	$ 79,753	$79,753	$ -
Cyber Resilience in Natural Disaster	$ 52,259	$ 52,259	$ -	$ 80,658	$80,658	$ -
Sub Total - Research	**$ 1,379,147**	**$ 1,379,147**	$ -	**$ 1,764,906**	**$ 1,764,906**	$ -
Regional Innovation & Talent Pipeline						
Building Cyber Workforce	$ 54,212	$ 54,212	$ -	$ 118,963	$ 118,963	$ -
Exciting talent Pipeline Cyber/AI	$ 40,849	$ 40,849	$ -	$ 49,636	$ 49,636	$ -
Building Cyber Readiness via Experiential Learning	$ 48,305	$ -	$ 48,305	$ 44,734	$ -	$ 44,734
Accelerating Commercialization Cyber Technologies	$ 52,670	$ 52,670	$ -	$ 53,947	$ 53,947	$ -
ICAP Expansion	$ 21,001	$ 21,001	$ -	$ 30,636	$ 30,636	$ -
Sub-Total - Innovation & Talent Pipeline	**$ 217,037**	**$ 168,732**	**$ 48,305**	**$ 297,916**	**$ 253,182**	$ 44,734
Operations						
Node Director	$13,454	$13,454	$ -	$ 40,361	$ 40,361	$ -
Admin support	$8,584	$8,584	$ -	$ -	$ -	$ -
Website	$5,305	$5,305	$ -	$ -	$ -	$ -
Printed Reports	$3,000	$0	$ 3,000	$ -	$ -	$ -
Travel	$3,000	$0	$ 3,000	$ -	$ -	$ -
Sub-Total - Operations	**$33,343**	**$27,343**	**$6,000**	**$40,361**	**$40,361**	$ -
Grand Total	**1,629,527**	**1,575,222**	**54,305**	**2,103,183**	**2,058,449**	**44,734**
Carry Over FY20 to FY21			**$ 54,305**			**$ 44,734**

Figure 3.3: Northern Virginia Node Annual Budget.



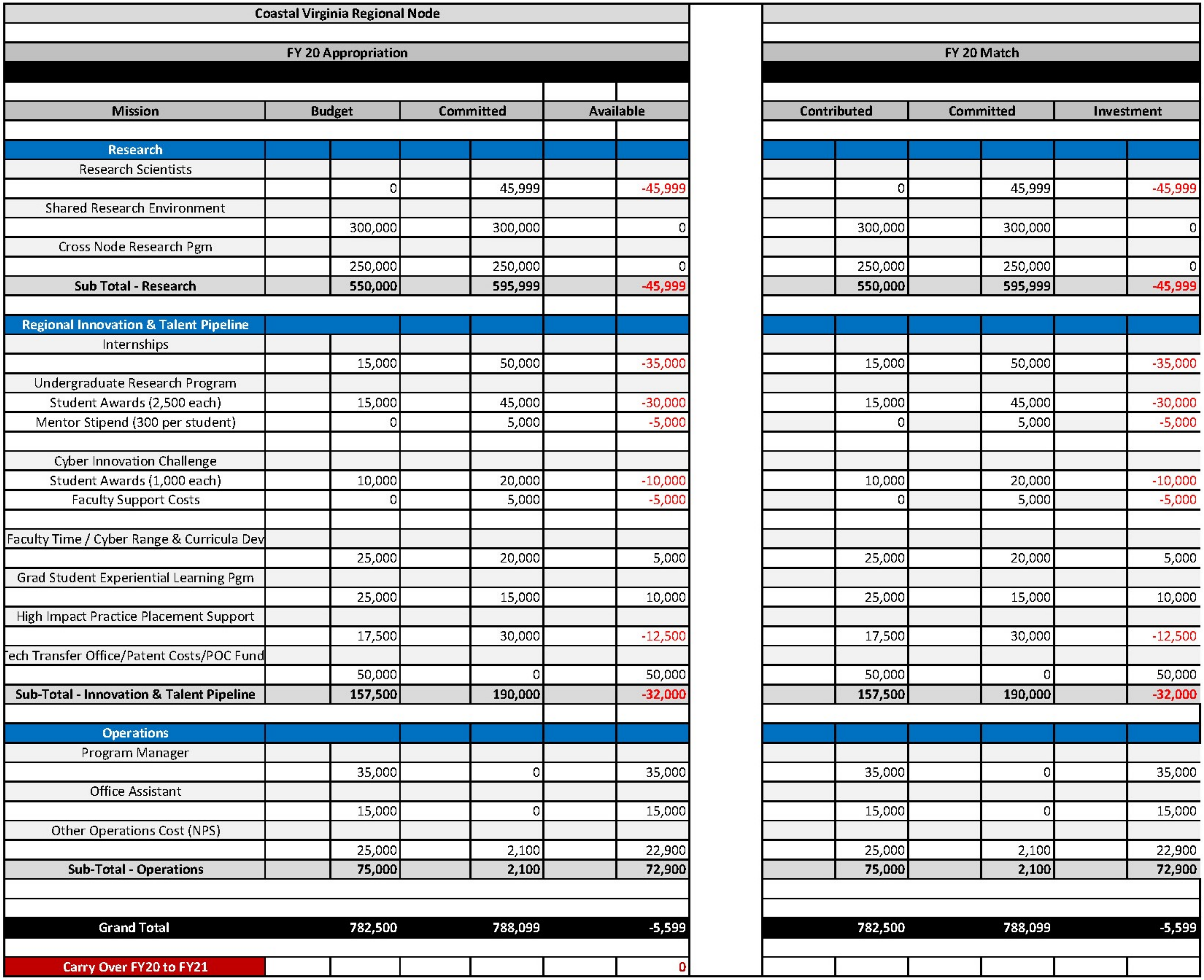
Central Virginia Regional Node						
	FY 20 Appropriation			FY 20 Match		
Mission	Budget	Committed	Available	Contributed	Committed	Investment
Research						
Smart Cities and Connected Communities	468,942	18,635	450,307	587,320	13,721	573,598
Nanoscale Hardware Security Initiative	171,249	2,167	169,082	213,200		213,200
Medical Device Security	159,809	5,691	154,118	212,560	8,579	203,980
Sub Total - Research	**800,000**	**26,492**	**773,507**	**1,013,080**	**22,301**	**990,778**
Regional Innovation & Talent Pipeline						
Expansion of Career Services	122,000		122,000	91,020		91,020
ase in On-Campu8s Presence from Cyber Ex	18,000		18,000	18,020		18,020
on on Non-Curricular Experiential Learning A	60,000		60,000	55,000		55,000
Executive In Residence	50,000		50,000	47,960		47,960
Technology Entrepreneur Matching Pgm	25,000		25,000	24,610		24,610
Customer Discovery/Market Validation	15,000		15,000	14,990		14,990
Industrial Engagement Associate (FT)	35,000		35,000	24,960		24,960
Sub-Total - Innovation & Talent Pipeline	**325,000**		**325,000**	**276,560**		**276,560**
Operations						
CVN Node Operations	181,925	3,033	178,891	91,935		91,395
CVN Connect	45,000		45,000	15,890		15,890
; Community and Corporate Econsysystem I	45,000		45,000	15,890		15,890
Sub-Total - Operations	**271,925**	**3,033**	**268,891**	**123,175**		**123,175**
Grand Total	**1,896,925**	**29,525**	**1,867,399**	**1,412,815**	**22,301**	**1,390,513**
Carry Over FY20 to FY21			**1,867,399**			

Figure 3.4: Central Virginia Node Annual Budget.



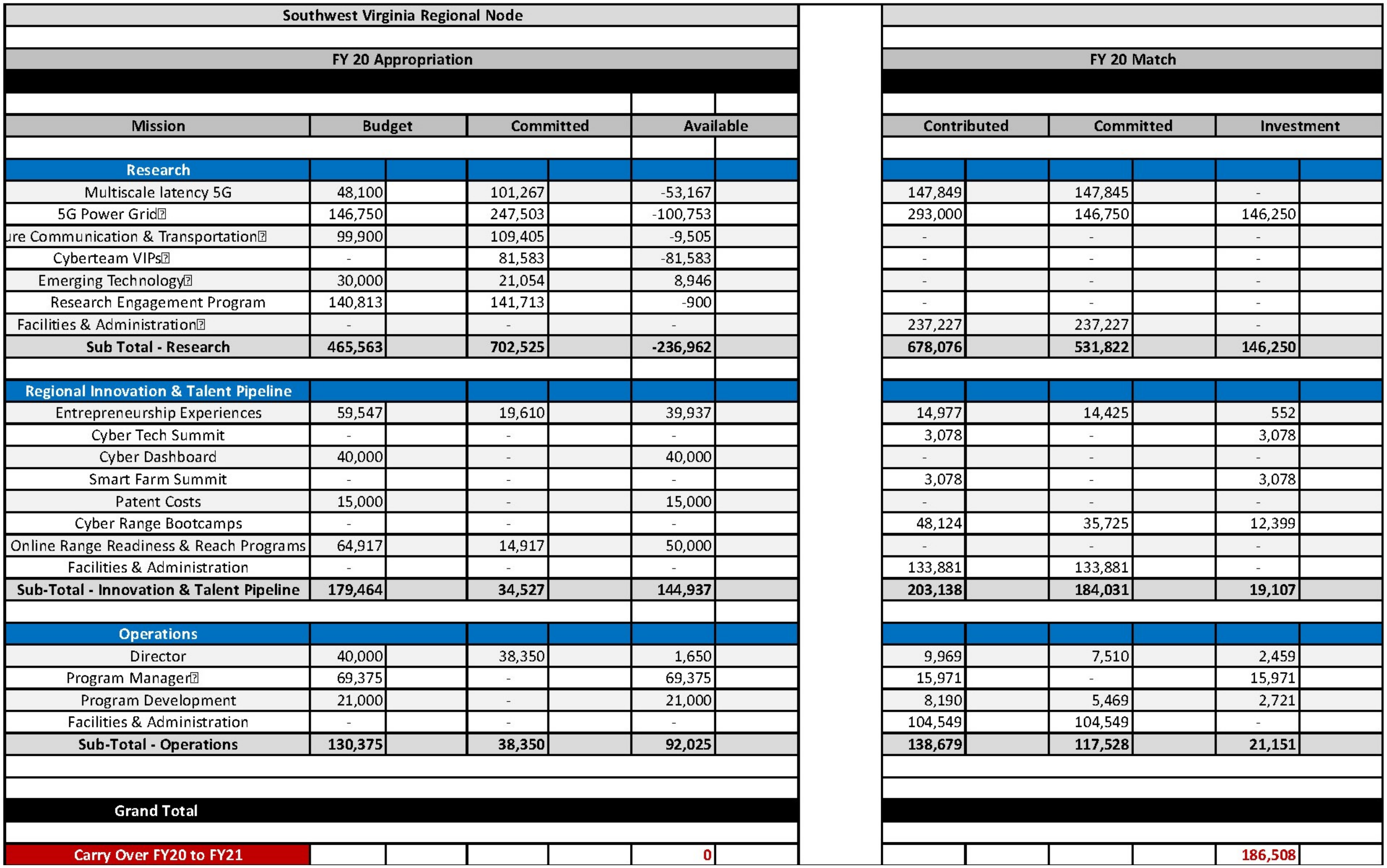
Central Virginia Regional Node	University of Virginia		
	FY 20 Match		
Mission	Contributed	Committed	Investment
Research			
Seed Funding			
	448,105	466,164	
Research Fellows / Translational Research			
	105,821	106,327	
Shared Research Data			
	0	0	
Labor			
	70,000	77,546	
Sub Total - Research	**623,926**	**650,037**	**0**
Regional Innovation & Talent Pipeline			
IP Ecosystem			
UVA Liscensing and Ventures Support	10,000	10,000	
Expand Career Services			
Staff	86,000	87,587	
Graduate Student Outreach			
Staff	10,630	13,810	
Sub-Total - Innovation & Talent Pipeline	**106,630**	**111,397**	**0**
Operations			
Understanding Smart Communities			
Workshop	50,000	50,000	
Community Engagement			
Smart Charlottesville	190,000	190,000	
igning Community and Corporate Ecosyste			
Faculty and Staff	56,920	62,394	
Sub-Total - Operations	**296,920**	**302,294**	**0**
Grand Total	**1,027,476**	**1,063,728**	**0**

Figure 3.5: UVA Matching Funds FY 20.



Coastal Virginia Regional Node						
FY 20 Appropriation				FY 20 Match		
Mission	Budget	Committed	Available	Contributed	Committed	Investment
Research						
Research Scientists						
	0	45,999	-45,999	0	45,999	-45,999
Shared Research Environment						
	300,000	300,000	0	300,000	300,000	0
Cross Node Research Pgm						
	250,000	250,000	0	250,000	250,000	0
Sub Total - Research	**550,000**	**595,999**	**-45,999**	**550,000**	**595,999**	**-45,999**
Regional Innovation & Talent Pipeline						
Internships						
	15,000	50,000	-35,000	15,000	50,000	-35,000
Undergraduate Research Program						
Student Awards (2,500 each)	15,000	45,000	-30,000	15,000	45,000	-30,000
Mentor Stipend (300 per student)	0	5,000	-5,000	0	5,000	-5,000
Cyber Innovation Challenge						
Student Awards (1,000 each)	10,000	20,000	-10,000	10,000	20,000	-10,000
Faculty Support Costs	0	5,000	-5,000	0	5,000	-5,000
Faculty Time / Cyber Range & Curricula Dev						
	25,000	20,000	5,000	25,000	20,000	5,000
Grad Student Experiential Learning Pgm						
	25,000	15,000	10,000	25,000	15,000	10,000
High Impact Practice Placement Support						
	17,500	30,000	-12,500	17,500	30,000	-12,500
ech Transfer Office/Patent Costs/POC Fund						
	50,000	0	50,000	50,000	0	50,000
Sub-Total - Innovation & Talent Pipeline	**157,500**	**190,000**	**-32,000**	**157,500**	**190,000**	**-32,000**
Operations						
Program Manager						
	35,000	0	35,000	35,000	0	35,000
Office Assistant						
	15,000	0	15,000	15,000	0	15,000
Other Operations Cost (NPS)						
	25,000	2,100	22,900	25,000	2,100	22,900
Sub-Total - Operations	**75,000**	**2,100**	**72,900**	**75,000**	**2,100**	**72,900**
Grand Total	**782,500**	**788,099**	**-5,599**	**782,500**	**788,099**	**-5,599**
Carry Over FY20 to FY21			**0**			

Figure 3.6: Coastal Virginia Node Annual Budget.



Southwest Virginia Regional Node						
	FY 20 Appropriation			FY 20 Match		
Mission	Budget	Committed	Available	Contributed	Committed	Investment
Research						
Multiscale latency 5G	48,100	101,267	-53,167	147,849	147,845	-
5G Power Grid⍰	146,750	247,503	-100,753	293,000	146,750	146,250
ıre Communication & Transportation⍰	99,900	109,405	-9,505	-	-	-
Cyberteam VIPs⍰	-	81,583	-81,583	-	-	-
Emerging Technology⍰	30,000	21,054	8,946	-	-	-
Research Engagement Program	140,813	141,713	-900	-	-	-
Facilities & Administration⍰	-	-	-	237,227	237,227	-
Sub Total - Research	**465,563**	**702,525**	**-236,962**	**678,076**	**531,822**	**146,250**
Regional Innovation & Talent Pipeline						
Entrepreneurship Experiences	59,547	19,610	39,937	14,977	14,425	552
Cyber Tech Summit	-	-	-	3,078	-	3,078
Cyber Dashboard	40,000	-	40,000	-	-	-
Smart Farm Summit	-	-	-	3,078	-	3,078
Patent Costs	15,000	-	15,000	-	-	-
Cyber Range Bootcamps	-	-	-	48,124	35,725	12,399
Online Range Readiness & Reach Programs	64,917	14,917	50,000	-	-	-
Facilities & Administration	-	-	-	133,881	133,881	-
Sub-Total - Innovation & Talent Pipeline	**179,464**	**34,527**	**144,937**	**203,138**	**184,031**	**19,107**
Operations						
Director	40,000	38,350	1,650	9,969	7,510	2,459
Program Manager⍰	69,375	-	69,375	15,971	-	15,971
Program Development	21,000	-	21,000	8,190	5,469	2,721
Facilities & Administration	-	-	-	104,549	104,549	-
Sub-Total - Operations	**130,375**	**38,350**	**92,025**	**138,679**	**117,528**	**21,151**
Grand Total						
Carry Over FY20 to FY21			**0**			**186,508**

Figure 3.7: Southwest Virginia Node Annual Budget.

Chapter 4

Strategic Goals and Action Plan

FY20 saw the establishment of the key structures in CCI and the recruitment of administrators and researchers in the initiative. It also saw the first research, innovation, and workforce development programs launched by the 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 FY20. In this chapter, CCI long-term goals are outlined in the operation of the initiative, in research, in innovation, and in workforce development. The main activities and programs planned for FY21 are also outlined.

4.1 CCI Operations

This section describes the long-term goals and actions in the operations and organizational structure of CCI.

4.1.1 Organizational Structure

Strategic Goal

CCI will establish organizational structures that incorporate advice from a broad array of stakeholders and mechanisms that assess the impact that the initiative has in Virginia, the Nation, and the world.

This section describes how we will enhance the organizational structure of CCI, including the addition of a Technical Advisory Board (TAB), an Inclusion & Diversity Committee (IDC), and a Chief Technology Officer (CTO).

CCI Technical Advisory Board (TAB)

In FY21, the CCI TAB will be formalized, envisioned in the governance structure of CCI (Figure 4.1). The CCI Blueprint describes the TAB as comprising 'leaders from industry and government providing advice and guidance on strategic direction for CCI' (Commonwealth Cyber Initiative, 2018). The CCI also envisions that the TAB will also serve as an advocacy group for the initiative.

The TAB will meet twice per year, with the first meeting planned for the Fall of 2020. After the initial two years, we will start a process of rotating TAB members in and out.

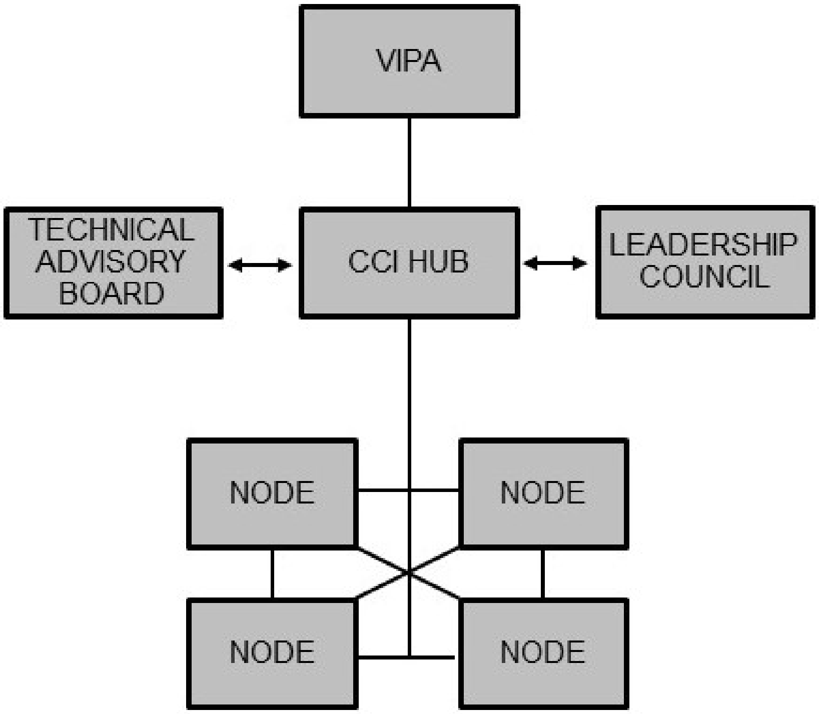


Figure 4.1: CCI governance structure.

The composition of the TAB is as follows:

- One Vice President for Research and Innovation (VPRI) from one of the institutes of higher education in CCI;
- One member appointed by Virginia Innovation Partnership Authority (VIPA) or, prior to that authority being constituted, by the Center for Innovative Technology (CIT);
- 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.

Inclusion and Diversity

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 will establish a Inclusion & Diversity Committee (IDC) with the role of advising the LC on matters of inclusion and diversity. The committee itself will have diverse representation from CCI-affiliated institutions throughout the Commonwealth. Roles of the committee will include to:

- Establish programs that aim at increasing participation of under-represented groups in the cybersecurity workforce;
- Advise the LC on diversity goals and considerations in all programs funded by CCI;
- Organize 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;
- Coordinate outreach activities geared towards under-represented groups in STEM.

Chief Technology Officer

CCI has created the role of CTO with the following attributions:

- Advise in the selection of priority areas of focus and areas of investment for CCI research;
- Participate in CCI investment decisions in research, including the launch and management of internal calls for proposals;
- Periodically brief the CCI LC and TAB;
- Supervise the design and deployment of shared infrastructure in CCI, including the 5G and AI testbeds;
- Advocate on behalf of CCI to funding agencies and relevant industry;
- Lead large proposals and white papers produced by CCI;
- Assist with the business development efforts for 5G and AI;
- Assist with marketing and strategy of marketing CCI;
- Conduct exploratory research that will link 5G and AI thrusts.

Professor Jeff Reed, Willis G. Worcester Professor at VT, will serve as the inaugural CTO of CCI. Professor Reed previously served as Interim Executive Director of CCI from its inception until March 2020. The CTO will continue to report to his home academic department, with a dotted line report to the CCI Executive Director, as shown in Figure 2.2.

Widely recognized for his work on wireless innovation, Reed's expertise is often sought out by industry leaders and the highest levels of the federal government. He has experience with the process of commercializing new technologies, a critical component of CCI's mission.

Professor Reed has a track record of entrepreneurship that demonstrates his ability to navigate the complex nexus of evolving technology and security. Reed is the co-founder of a commercial venture called Cognitive Radio Technologies, a company that develops cognitive radio technologies produced at Virginia Tech for commercial and military applications. In 2012, Professor Reed co-founded Federated Wireless: headquartered in Arlington, Virginia, the company employs more than 80 people and is leading the implementation of spectrum sharing in the 3.5 GHz band.

4.1.2 Impact Assessment

As CCI reaches its two-year mark at the end of FY21, an economic impact assessment will be commissioned, looking at the effect of the initiative on jobs and economic development in Virginia. The assessment will also consider other dimensions of research impact, including public policy, social, cultural, and legal impact.

4.1.3 Communications and Marketing

In August 2020, Michele McDonald joined CCI as Director of Communications and Marketing. She is currently working on a communications strategic plan that will elevate CCI's profile by hosting events with high-profile speakers, using traditional media and social media outreach, creating workforce development opportunities for students and CCI partners, and holding symposiums designed to enhance collaboration between node researchers, students, industry, and government.

4.2 Research

CCI's mission is to establish Virginia as a global center of excellence in research at the intersection of cybersecurity, autonomous systems, and data. The economic impact CCI 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 will build capacity and seed new areas of excellence. These are described in this section.

4.2.1 Research Infrastructure

Strategic Goal

CCI will establish unique research infrastructure in the areas of 5G security and AI Assurance, leveraging the existing research strengths of the partner universities.

5G Testbed

Uniqueness

The CCI 5G[a] testbed distinguishes itself by its close alignment with key verticals that are empowered by 5G, its focus on cybersecurity, and unparalleled access to licensed spectrum.

[a] We use the term for brevity, to also include emerging wireless mobile technologies that are expected to extend and eventually supersede 5G.

The first phase of the 5G network testbed is currently deployed in the CCI Hub, comprising an open source 5G Core, as well end-to-end connectivity to a Radio Access Network (RAN) and UE, as as discussed in Section 2.1.3. This deployment is already attracting the attention of industry, with advanced negotiations with AT&T and Mitre for the expansion of the testbed. Close alignment of the testbed with key verticals including smart transportation, manufacturing, healthcare, smart warehouses, and distributed power systems, will be a unique characteristic of the CCI 5G testbed. It will also leverage existing research infrastructure in the partner universities, including the smart road operated by the Virginia Tech Transportation Institute (VTTI), drone facilities operated by the Mid-Atlantic Aviation Partnership (MAAP), autonomous and connected vehicles at GMU, etc.

Activities in FY21 will include:

- Coordinate the deployment of the CCI testbed in the Nodes, aligned with key verticals in each of the Nodes.
- Recruit a 5G Testbed Director responsible for strategy, deployment, and partnership building.
- Deploy the first outdoor components of the 5G testbed.
- Participate as a founding member in the CTIA 5G testbed consortium. The CTIA is the main trade association representing the wireless communications industry in the US.
- Obtain additional funding for future expansions of the testbed.

AI Assurance Testbed

Uniqueness

The AI Assurance Testbed establishes a distributed, interdisciplinary, virtual exchange to learn about, develop, and rigorously test artificial intelligence technologies.

After establishing the basic infrastructure for the testbed, a full planning exercise for the next phase of the project will be conducted.

The vision is for the testbed to form the preeminent 'AI Commons' – an ecosystem of researchers, students, and technology that enable interdisciplinary learning and innovation. The breadth of academic talent in the Commonwealth of Virginia will be fully leveraged and cultivated to enable the development and commercialization of human-centered, trustworthy AI. The testbed must bring together unparalleled work domain expertise, data, and research talent. An ambition of CCI is to become a recognized independent body for AI Assurance testing.

The value proposition for the testbed is illustrated in Figure 4.2. Unlike existing testbeds in industry, academia, government, and non-profit institutions, CCI has the ability to bring together a truly transdisciplinary team from across 17 Virginia universities, to make available labelled datasets for AI/ML models, to accelerate commercialization of technologies created in our research groups, and provide a unique research infrastructure that can be used by students, academic researchers, industry collaborators, and government sponsors.

To this end, CCI has assembled a testbed planning committee with representation from across Virginia and activities in FY21 will include:

- Finalize the architecture of the testbed - the high-level reference architecture is shown in Figure 4.3.
- Define a phased implementation for the testbed and commission the work to be done in FY21.

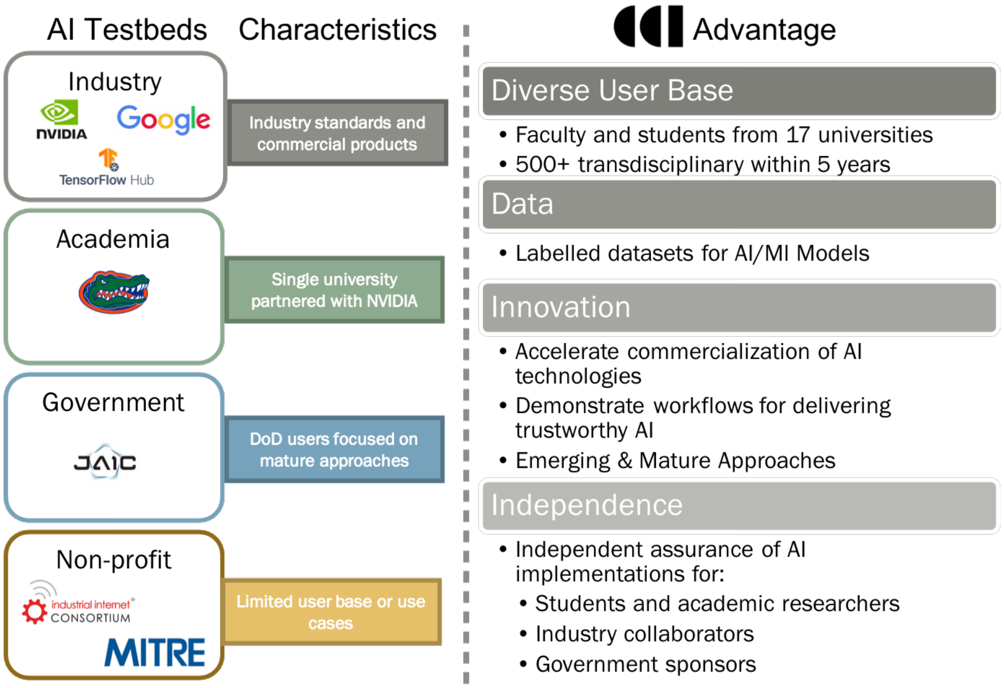

AI Testbeds
Characteristics
Advantage
Industry
NVIDIA
Google
TensorFlow Hub
Industry standards and commercial products
Academia
Single university partnered with NVIDIA
Government
JAIC
DoD users focused on mature approaches
Non-profit
industrial internet CONSORTIUM
MITRE
Limited user base or use cases
Diverse User Base
• Faculty and students from 17 universities
• 500+ transdisciplinary within 5 years
Data
• Labelled datasets for AI/MI Models
Innovation
• Accelerate commercialization of AI technologies
• Demonstrate workflows for delivering trustworthy AI
• Emerging & Mature Approaches
Independence
• Independent assurance of AI implementations for:
• Students and academic researchers
• Industry collaborators
• Government sponsors

Figure 4.2: AI Assurance testbed value proposition.

- Define a data governance structure, including data acquisition, data curation and metadata definition, model curation, and access policies.
- Staff the testbed operation team.
- Select pilot research projects to use the testbed.

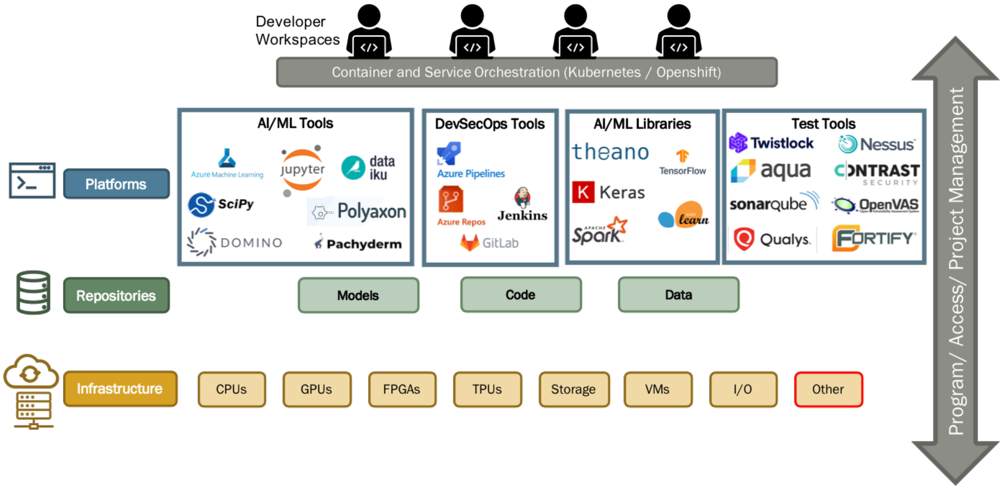


Figure 4.3: AI Assurance testbed architecture.

4.2.2 Research Programs in FY21

The following research programs are envisioned in FY21:

- Capacity building: CCI faculty has already been extremely successful in attracting external research funds. As discussed in Section 2.1, CCI faculty in the Hub has already obtained around $20M in external funding. In FY21, CCI will build further research capacity, in the Hub and the Nodes, to avail of additional research funding opportunities in the focus area of CCI. CCI will particularly focus on recruiting early-career research faculty with high potential to build a strong research program, and on faculty in key areas of investment to CCI.

- Strengthening collaborations within the network: In the first year of CCI, emergence of strong collaborations within the network were recognized. For example, Dr. Milos Manic led a group of faculty from six CCI universities in a proposal to NSF for a research center in trustworthy AI. CCI aims to strengthen these intra-network collaborations, and in FY21 will dedicate $4M in Node funding for research proposals that include Principal Investigators (PIs) in more than one Node.

- Research partnerships with industry: CCI will launch a call for co-funded research projects in 5G security and AI Assurance. The projects must be led by a CCI researcher and have a minimum of 50% cash contribution from industry. The objective is to create a research program that is closely aligned with problems of immediate relevance to industry, likely to result in new IP.

- Trans-disciplinary research: CCI will incentivize trans-disciplinary research in the CCI domains and will launch, in partnership with Institute for Creativity, Arts, and Technology (ICAT) and the da Vinci Center at VCU, a call for proposals directed at researchers in the Arts and Design. The objective is to foster collaboration between them and researchers already associated with CCI, to devise creative ways to display or use data that is the product of research in CCI. In FY21, CCI will continue to expand collaborations among researchers in the engineering and sciences and those in the arts, humanities, and social sciences.

4.3 Workforce Development and Education

Strategic Goal

CCI will provide unique experiential learning and early work experiences to Virginia students that complement the instruction provided through degree-granting programs across the state. These experiences combine early exposure to the latest advancements in the field with essential skills in ethics, entrepreneurship, and communication, to produce and retain the most diverse and qualified workforce on cybersecurity, autonomous systems, and data.

The 39 institutions of higher education across Virginia offer a variety of options for cybersecurity education. These include standalone undergraduate and graduate degrees; majors and minors; and accelerated certificates and experiential learning programs. A list of these programs can be found on the CCI website.

CCI will complement these programs by developing unique experiential learning opportunities, facilitating internships and apprenticeships, and providing essential skills in entrepreneurship and innovation, communication with the general public, and ethics.

4.3.1 Workforce Development Programs in FY21

The following programs are directed at workforce development and education in FY21:

- Call for innovative experiential learning projects: CCI will run, for the second time, a statewide call for innovative experiential learning projects (the first call was successfully run in FY20 and is described in Section 2.1.2). The funded projects will generate unique experiential learning and internship opportunities for community college and university students throughout Virginia. Improvement to the diversity of the cybersecurity workforce is an explicit objective of the program.

- CCI Summer Academy: the first CCI Summer Academy on AI Assurance took place on August 10-14, 2020. The Summer School included tutorial lectures by five subject matter experts and a leadership panel with practitioners from industry, government, and academia. The five-day program, fully conducted online, was attended by 90 researchers. The second Annual Summer Academy is being planned for Summer 2021, as an in-person event.
- Cybersecurity job fair: CCI will promote activities that bring together graduating students, industry, and government agencies with interest in recruiting in cybersecurity, autonomous systems, and data.
- CCI Seminar Series: CCI is running a Seminar Series each semester, with monthly talks by prominent speakers from industry and academia. The theme of the Fall 2020 Seminar Series is *AI for Cybersecurity*, with confirmed speakers from Google Brain, DeepSig (a successful Virginia startup in the area of deep learning for wireless communications), and Purdue University. A second Seminar Series will run in Spring 2021.

4.4 Commercialization and Innovation

Strategic Goal

CCI will facilitate the translation of research at the intersection of cybersecurity, autonomous systems, and data into innovation, through the development and protection of intellectual property developed in the CCI network and the fostering of a robust ecosystem of Virginia-based start-ups.

CCI will leverage successful innovation initiatives that exist in the partner universities to design programs that scale to all researchers in the CCI network. To this end, an Innovation Committee has been established and they will provide guidance to the LC in all commercialization and innovation activities undertaken by the network.

CCI innovation programs will focus on the protection of IP generated by CCI researchers and activities that lead to licensing and/or the development of start-ups using this IP.

4.4.1 Innovation Committee

CCI Innovation Committee

The Innovation Committee, with experts in innovation and technology transfer from six CCI universities, advises the LC on innovation initiatives, and designs and oversees network-wide innovation programs.

The CCI Innovation Committee, with experts on innovation and technology transfer from six of the partner institutions (Figure 4.4), is composed as follows:

- Sarah Hayes, CCI Portfolio Director (Chair)
- Mark Mondry, Associate Director for Launch, VT

- Jeff Pittges, Professor, Radford University
- Jason McDevitt, Director of the Technology Transfer Office, W&M
- Hina Mehta, Director of the Office of Technology Transfer, GMU
- Mary Lou Bourne, Director of Technology Innovation and Economic Development, JMU
- Travis Hite, Program Director of Link Lab, UVA

(a) Sarah Hayes, CCI Portfolio Director.

(b) Mark Mondry, Associate Director for Launch, VT.

(c) Jeff Pittges, Professor, Radford University.

(d) Hina Mehta, Director of the Office of Technology Transfer, GMU.

(e) Mary Lou Bourne, Director of Technology Innovation and Economic Development, JMU.

(f) Travis Hite, Program Director of Link Lab, UVA.

Figure 4.4: CCI Innovation Committee. Not depicted: Jason McDevitt, W&M

The primary role of the Innovation Committee is to advise the LC on innovation and commercialization programs that CCI runs or participates in. This committee also takes the lead on designing innovation programs directly funded by CCI.

4.4.2 Innovation Programs in FY21

The following programs are specifically planned for FY21.

- Intellectual Property (IP) repository: The Innovation Committee will select IP generated within CCI to be collected into a repository and made available for licensing to potential industry partners and investors. These inventions will be showcased in the CCI website and literature.
- Commercialization Program: The LC has designated $1M from FY21 Node funds for a network-wide commercialization program in CCI. The Innovation Committee is being tasked with designing the program, including setting objectives, drafting the call for proposals, and overseeing the selection of proposals to be funded.
- External partnerships: CCI is negotiating with external partners, including in local government and in the private sector, to run an innovation program centered on immediate needs of these partners. CCI is exploring structuring such partnerships in the form of reverse pitches that CCI researchers can respond to; selected proposals would be funded for further development towards commercialization.

Bibliography

Business Facilities. (2020). Business Facilities' 16th Annual Rankings: State Rankings Report [Accessed: 12 August 2020]. https://businessfacilities.com/2020/07/business-facilities-16th-annual-rankings-state-rankings-report/

Commonwealth Cyber Initiative. (2018). Commonwealth Cyber Initiative Blueprint [Accessed: 15 July 2020]. https://vt.edu/content/dam/cci-blueprint_vt_edu/docs/CCI-Blueprint%5C%20final.pdf

Cyber Seek. (2020). Cybersecurity Supply/Demand Heat Map [Accessed: 16 July 2020]. https://www.cyberseek.org/heatmap.html

Deloitte. (2020). 5G: The Change to Lead for a Decade [Accessed: 24 July 2020]. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf

Powell, R. (2019). Researcher to Lead Virginia Cyber Initiative [Accessed: 23 July 2020]. Virginia Business. https://www.virginiabusiness.com/article/researcher-to-lead-virginia-cyber-initiative/

Raymond, D. (2020). *Final Report: Virginia Cybersecurity Workshop* (tech. rep.). Virginia Cyber Range.

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/

Washington, DC Citybizlist. (2020). Commonwealth Cyber Initiative Awards Experiential Grants to Faculty and Students across Virginia [Accessed: 21 July 2020]. https://dc.citybizlist.com/article/612060/commonwealth-cyber-initiative-awards-experiential-learning-grants-to-faculty-and-students-across-virginia