Fiscal Year 2021 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 2021 REPORT

Commonwealth Cyber Initiative

October 1, 2021

Message from the Executive Director

In the Commonwealth Cyber Initiative (CCI), we have the bold objective of making Virginia a globally recognized center of excellence in cybersecurity, and in doing so to contribute to the commonwealth's economic diversification and prosperity.

It is common for this sort of program to take several years to show tangible benefits, so we were delighted to learn, from an economic impact study commissioned this year, that CCI has already brought significant research funding, job growth, and contribution to Virginia's economy.

We have hit the ground running in our interconnected mission lines of research, workforce development, and innovation. This report summarizes our progress on each of those fronts in Fiscal Year 2021 (FY21) and outlines our plans for the next year.

Our focus, the intersection of cybersecurity, autonomy, and intelligence, is more relevant than ever, and we expect unprecedented government and industry funding and innovation opportunities in the next year. In this context, forming a qualified and diverse cyber workforce, one of CCI's strategic goals, is of paramount importance to Virginia's economic development. CCI is poised to take advantage of those opportunities and continue to contribute to the nation's leadership in this important area.

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

AAEA Agricultural and Applied Economical Association

AI Artificial Intelligence

API Application Programming Interface

AREC Agricultural Research and Extension Center

CAV Connected Autonomous Vehicle

CBRS Citizens Broadband Radio Service

CCI Commonwealth Cyber Initiative

CIT Center for Innovative Technology

CV2X Cellular Vehicle-to-Everything

CVN Central Virginia Node

CIA Central Intelligence Agency

CNU Christopher Newport University

CoVA Coastal Virginia

CPS Cyber Physical System

CTO Chief Technology Officer

CV2X Cellular Vehicle-to-everything

CyManII Cybersecurity Manufacturing Innovation Institute

DNS Domain Name System

DoD Department of Defense

DoE Department of Energy

DTN Delay and Disruption Tolerant Network

EIRP Effective Isotropic Radiated Power

EPC Evolved Packet Core

FPGA Field Programmable Gate Array

FY20 Fiscal Year 2020

FY21 Fiscal Year 2021

FY22 Fiscal Year 2022

GAA General Authorized Access

GAN Generative Adversarial Network

GDP Gross Domestic Product

Mason Mason

GPS Global Positioning System

GPU Graphics Processing Unit

GRA Graduate Research Assistant

HBCU Historically Black Colleges and Universities

HR Human Resources

ICAT Institute for Creativity, Arts, and Technology

IDC Inclusion & Diversity Committee

IEEE Institute of Electrical and Electronic Engineers

IoT Internet of Things

IoMT Internet of Medical Things

IP Intellectual Property

JMU James Madison University

LC Leadership Council

MAAP Mid-Atlantic Aviation Partnership

MANO Management and Network Orchestration

MEC Mobile Edge Computing

MU Marymount University

NFV Network Function Virtualization

NGA National Geospatial-Intelligence Agency

NoVA Northern Virginia

NOVACC Northern Virginia Community College

NSA Non-Standalone

NSF National Science Foundation

NSU Norfolk State University

ODU Old Dominion University

ONR Office of Naval Research

OS Operating System

PaaS Platform as a Service

PAL Priority Access License

PAWR Platforms for Advanced Wireless Research

PI Principal Investigator

R&D Research and Development

RAN Radio Access Network

RIC RAN Intelligent Controller

RT Real Time

SAS Spectrum Access System

SDN Software Defined Network

SDR Software Defined Radio

SIM Subscriber Identity Module

SME Small and Medium Enterprise

SMO Service Management and Orchestration

STEM Science, Technology, Engineering, and Mathematics

SWVA Southwest Virginia

TAB Technical Advisory Board

TCPS Transportation Cyber Physical System

UAV Uncrewed Autonomous Vehicle

UE User Equipment

USRP Universal Software Radio Peripheral

UVA University of Virginia

VASEM Virginia Academy of Science, Engineering, and Medicine

VCU Virginia Commonwealth University

VIPA Virginia Innovation Partnership Authority

VLAN Virtual Local Area Network

VM Virtual Machine

VMASC Virginia Modeling, Analysis and Simulation Center

VMI Virginia Military Institute

VPRI Vice President for Research and Innovation

VRIC Virginia Research Investment Committee

VSGC Virginia Space Grant Consortium

VSU Virginia State University

VT Virginia Tech

VT-ARC Virginia Tech Applied Research Corporation

VTTI Virginia Tech Transportation Institute

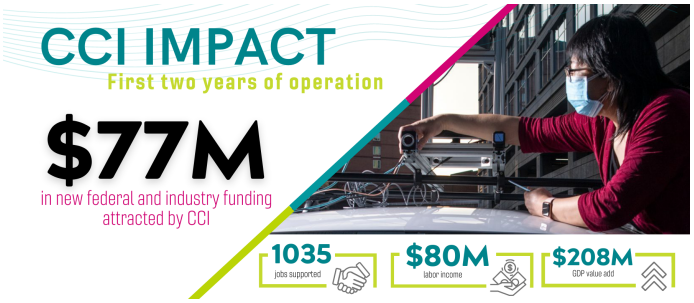
W&M William & Mary

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).

Our ambitious vision is to *establish Virginia as a global leader in cybersecurity*, and by doing so, help diversify the economy of the state, and attract industry investment and jobs. Fiscal Year 2021 (FY21) was the first year with the full leadership team in place, including the executive director, the managing director, and the four regional node directors responsible for regional programs in Central, Coastal, Northern, and Southwest Virginia. We have already seen major economic and reputation impact across the three CCI mission lines of *research, workforce development, and innovation at the intersection of cybersecurity, autonomy, and intelligence.*

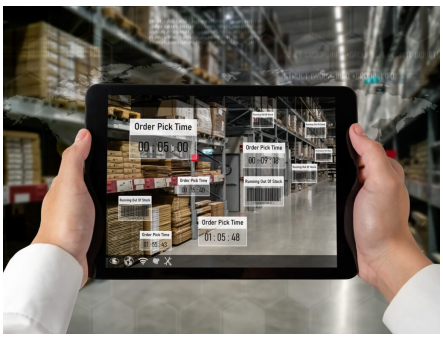


This year, CCI commissioned an economic impact study, conducted by Research Triangle Institute (RTI). It was gratifying to learn that despite our short history, we already see a great impact on jobs, the Virginia economy, and the competitiveness of our researchers for external funding. RTI found that, in the last two years, CCI researchers attracted $77 million in extramural funding, a strong direct return on the investment made by the Commonwealth. CCI activities were responsible for creating 1035 jobs, corresponding to $80 million in labor income and $208 million value-add to the Virginia Gross Domestic Product (GDP).

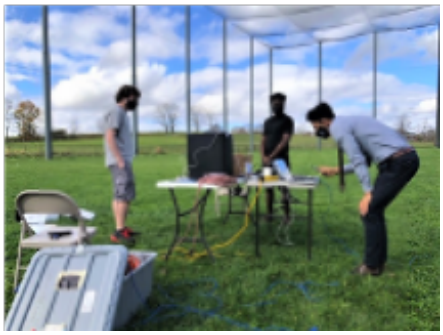
Furthermore, the investments and early success of CCI in areas including 5G and NextG security, Artificial Intelligence (AI) Assurance, and securing cyber-physical systems, position us particularly well to contribute to the goals of the United States Innovation and Competition Act of 2021 and other national initiatives currently being considered by Congress.

This report highlights some of the major accomplishments from the past fiscal year, which are indicative of what the CCI network can achieve for the state.

Intra-network Collaboration. To accomplish our ambitious goal of making Virginia a recognized world leader in cybersecurity, strong collaboration among researchers across the entire CCI network is key. These relationships are part of the lasting legacy of CCI. In FY21, we funded 22 new research collaboration projects that brought together researchers from multiple regional nodes in CCI, with a total budget of $4 million, on topics that range from secure sensors for lung health to user-centric privacy for smart home devices. The ability to convene teams of researchers to work on large projects is already bearing fruit. In early 2021, a team of CCI researchers received a Department of Defense (DoD) grant to create a resilient and energy-efficient smart warehouse pilot in the U.S.



Marine Corps logistics base in Albany, GA. This $13 million project involves researchers from George Mason University (Mason), Old Dominion University (ODU), University of Virginia (UVA), Virginia Commonwealth University (VCU), and Virginia Tech (VT), and would not have been possible without CCI: it is the combined expertise of these researchers into a single team that makes Virginia competitive for large grants such as these. This year, Virginia Military Institute (VMI) joined the network, and we are now more than 300 researchers across 40 institutions of higher education.



Shared Research Infrastructure. CCI has made a major investment in creating a unique, geographically distributed testbed for experimentation and innovation in Next Generation networks and AI Assurance. CCI's NextG testbed is based on principles of openness and programmability that allow our researchers to prototype and test technologies that will make up the next generation of network and computing systems. In 2021, we joined the O-RAN Alliance and the NextG Alliance, and through our participation in these industry-led organizations we help translate inventions into commercially viable solutions and contribute to the emerging vision for the next generation of networks, which will eventually replace 5G. Our investments in research infrastructure leverage existing assets in the participating universities, such as smart vehicles at Mason and the Drone Park at VT, to experiment with how networks can enable transformation in key verticals such as transportation and manufacturing.

Broadening Participation in the Workforce. One of our strategic goals is to contribute to increasing the diversity of the cyber workforce and to foster a culture of inclusion in the work environment. The CCI Diversity and Inclusion Committee, with representation from across the Commonwealth, designs programs aimed at increasing participation of under-represented groups in the cyber workforce and ensures that diversity goals are embedded in all programs funded by CCI. The results are starting to show: our cyberstartups program, which funds internships for Virginia students in startups focusing on cybersecurity, had 15 students selected out of 145 applicants; 80% of the selected students were from under-represented groups. And our INNOVATE Cyber program, where teams of students develop a new product in response to a cybersecurity challenge, has attracted highly diverse cohorts.

Leadership in Cybersecurity. In FY21, CCI researchers brought in a total of $37.1M in new research contracts to Virginia. 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. CCI makes the consortium of Virginia institutions of higher education competitive against any of the top universities in the U.S. and globally, in terms of scholarship and the ability to attract funds for cybersecurity research. We have created the CCI Fellows program, which currently provides seed funding to nine faculty members at Mason, Norfolk State University (NSU), ODU, Radford University, UVA, VCU and VT; the fellows provide leadership in CCI for larger programs in research and workforce development. In FY21, the CCI Fellows attracted $13.1 million in new extramural research funding, an incredible $1.5 million per researcher, well above the average new funding per faculty member in any university in the country. Two assistant professors, one at ODU and one

at VT, who benefited from early grants from CCI have now received extremely prestigious CAREER awards from the National Science Foundation (NSF); empowering junior faculty and helping them build successful careers is one of the benefits of CCI.

Transdisciplinary Cybersecurity. We take the approach that cybersecurity is inherently multidisciplinary, and that to grow the workforce requires reaching out to students with diverse interests and skills across disciplines. In FY21, we funded five projects by researchers in the arts and design that examine cybersecurity from the point of view of the creative arts, from choreography to sound design. Some of these projects explore new technical challenges, such as how to enable network communications with latency low enough to enable a string quartet to play together from distinct locations. Others educate the public on cybersecurity issues: an assistant professor in the Mason School of Art has created the "Undeleted" project, where he displays information that was not properly deleted from dozens of discarded smart phones. We also launched a program investigating the role of cybersecurity in curbing the spread of disinformation and misinformation, funding seven transdisciplinary teams to build capacity in combating the fast growing and serious problem of misinformation campaigns. These teams of computer scientists, political scientists, philosophers, engineers, and others apply AI to detect and stop disinformation in areas including science, local government, national security, and autonomous systems.

Experiential Learning. CCI has funded 13 new experiential learning programs, for a total of $1.7 million. We fund three internship programs, where students are paired with Virginia-based companies; for startups CCI pays the full stipend to students, and for small and medium sized companies CCI provides 25% of the stipend. At the conclusion of one of these internship programs, which finished in summer 2021, 73% of the interns were offered a permanent position or extended internships fully funded by the company. We also funded a highly successful program led by an assistant professor in geography at William & Mary (W&M) that exposed students to the real-world problem of data poisoning attacks on AI systems. And the first CCI Battledrones Competition is planned for early 2022, with student teams programming autonomous drones to complete an obstacle course; the drones themselves were designed and 3D-printed by researchers at VT.

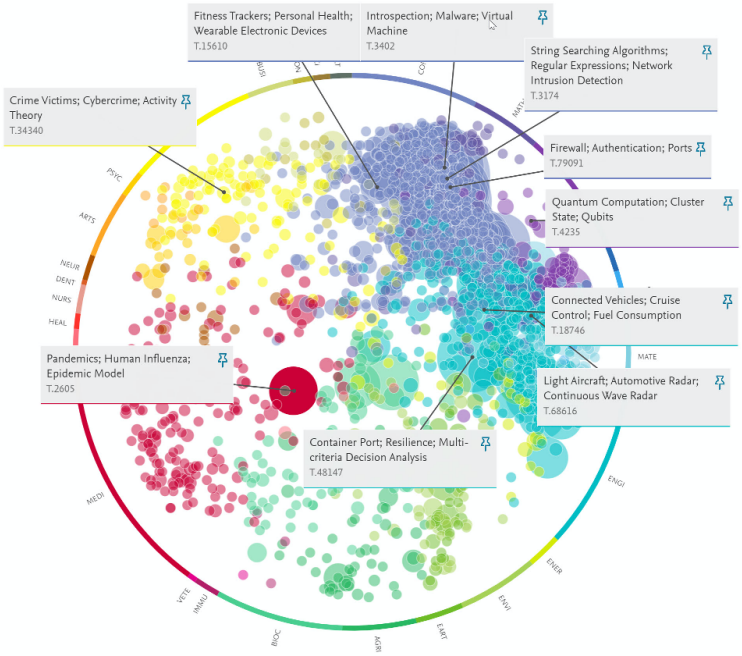
Innovation Ecosystem. CCI's Innovation Committee launched two new programs this year, with total funding of $1 million. The Virginia Cybersecurity Challenge, publicly announced by Governor Northam, funds inventions that leverage unique elements of emerging 5G technologies to provide secure operations or communications in ways not possible on previous generation networks. The Cybersecurity Innovation Bridge Fund program aims to enhance pre-product, cybersecurity innovation companies and university projects by developing a cyber technology prototype to attract seed and series-A funding. Our students are important participants in the innovation ecosystem, and we are increasing our focus on programs that prepare students for entrepreneurship. The highly successful INNOVATE Cyber program graduated its second cohort of students from universities and colleges in Coastal Virginia; this next generation of innovators and entrepreneurs work in teams to propose solutions to cybersecurity challenges, creating business models with support from the ODU Entrepreneurial Center.

CCI funding is distributed to researchers through open calls for proposals, with proposals peer-reviewed

and final recommendations made by CCI's Leadership Council. In FY21, we issued seven calls for proposals to researchers across the network. We centrally managed 122 submitted proposals, which were evaluated by 85 reviewers. This hard work ensures that the best ideas, aligned with the mission of CCI, are selected for funding in an open and transparent manner.

Industry and Public Engagement. In all of the activities discussed above, we are actively engaging with industry: to build our NextG 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, opportunities 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 ultimately lead to high-quality jobs and a thriving entrepreneurial ecosystem in cybersecurity and autonomous systems in Virginia. We have also engaged with the broader public and local government. The country experienced a number of high profile cyberattacks in the last year. We organized webinars that informed the public about impactful events such as the SolarWinds software supply chain attack. This year, we also partnered with Arlington County in their smart communities pilot: two CCI researchers serve on a board that advises the county on privacy protection measures that need to be incorporated into this pilot.

We are particularly proud of the multi-disciplinary approach we have adopted for CCI. The figure on the right is a visualization of the recent publications by our researchers, and their respective fields of expertise. The concentration of blue and purple circles represent engineering, math, and computer science: there is very strong activity in areas such as quantum computing, authentication, autonomous systems and network intrusion detection, as is expected in a cybersecurity center. What is also interesting is the strong showing by other disciplines. The green circles represent work in energy, the environment, Earth sciences, and agriculture: work there includes the emerging areas of cyberbiosecurity and securing the power grid. The work in red represents medicine and the health sciences: CCI's activities in that area include epidemic models, resilience of the healthcare system against cyber attacks, and securing networked medical devices. The yellow and orange circles represent the humanities and social sciences: there, CCI produces work on cybercrime, ethical issues in the adoption of AI, and dis/misinformation spread. The combined expertise in all these disciplines is a unique strength of CCI. It also equips us well for our workforce development mission: to meet the particularly strong demand for cybersecurity professionals in Virginia will require forming and recruiting talent with a variety of skills and interests in many disciplines.



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

- Updating our research focus areas to reflect the evolving areas of particular interest from industry and government, and the strengths of the CCI network.
- Launching a large program in Securing NextG, which will position our researchers to lead in the vision and technology development for the next generation of communication networks.
- Expanding our experiential learning program, with additional funding to support internships, organizing the CCI Cyber Camp, partnering with VMI to co-organize the Cyber Fusion competition, and scaling up the successful programs that have been created by the CCI.
- Launching a new innovation program with special emphasis in student entrepreneurs.
- Converging the two CCI testbeds into a single NextG testbed that supports experimentation and prototyping in the next generation of AI assurance and networking solutions.

As CCI reaches its two-year mark, we already see measurable impact on Virginia's competitiveness in cybersecurity research, innovation, and workforce development. With the increased adoption of AI and communication networks becoming a key element of our critical infrastructure, the need for robust cybersecurity will only grow. The investment that the Commonwealth has made in CCI positions us to play a leading role and to contribute to the state's and the country's economic development.

Chapter 1

The Commonwealth Cyber Initiative

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

1.1 Vision and Mission

CCI Vision

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

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

This report describes our progress in each of the mission lines in FY21, in pursuit of the vision of global leadership in cybersecurity for the Commonwealth of Virginia.

1.2 The CCI Network

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

1.2.1 An Evolving Network

In FY21, VMI joined CCI, and our network today comprises 40 institutions of higher education across Virginia, depicted in Figure 1.1.

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

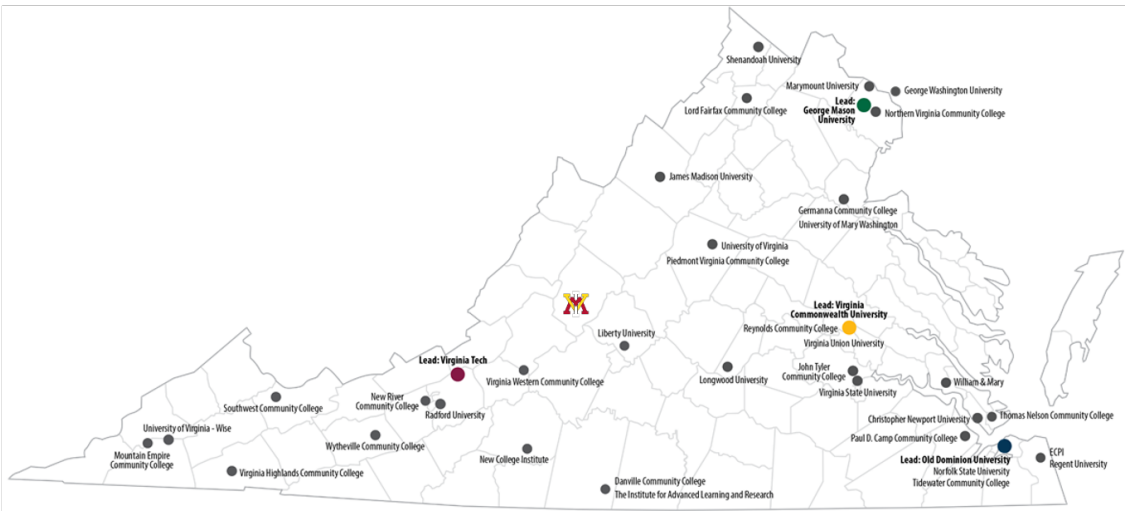


Figure 1.1: The CCI network comprises 40 institutions of higher education across Virginia. VMI is the latest member to join.

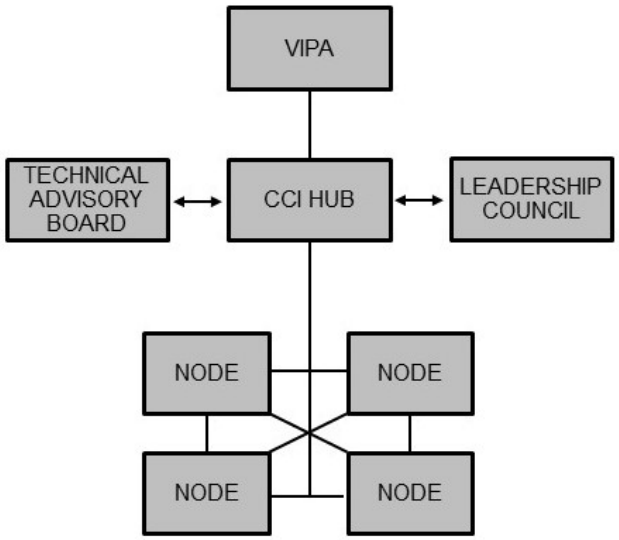


Figure 1.2: CCI governance structure.

The CCI executive director chairs the Leadership Council (LC) and is responsible for articulating the research agenda and the innovation and workforce development strategy for the network. The CCI Hub designs, coordinates, and funds some network-wide programs and deploys key research infrastructure available to all CCI researchers. The hub also houses faculty and graduate students with established expertise in key research areas in cybersecurity, autonomous systems, and intelligence. A communications team in the hub is responsible for external dissemination of CCI activities and successes. Finally, the hub convenes teams throughout the network to put together large, multi-million dollar research proposals for external funding. The CCI Regional Nodes are responsible for developing capacity in research, innovation, and workforce development in their respective geographic regions, establishing leadership in key focus areas. They also recruit eminent faculty and promising junior faculty for their member institutions and fund programs in the node,

as well as collaborations across multiple nodes. The main roles of the hub and the nodes are summarized in Figure 1.3.

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

Figure 1.3: Roles of the CCI Hub and Nodes.

The CCI executive director, managing director, and the four node directors form the CCI Leadership Council (LC), depicted in Figure 1.4. Dr. Luiz DaSilva serves as CCI executive director and holds the position of Bradley Professor of Cybersecurity at VT. Mr. John Delaney, former Chief of Staff for the US Army Cyber Command, is CCI's managing director. Dr. Liza Wilson Durant serves as NoVA node director; she is also a professor and Associate Provost for Strategic Initiatives and Community Engagement in the Volgenau School of Engineering at Mason. Dr. Brian Payne serves as CoVA node director; he is also vice provost for Academic Affairs at ODU. Dr. Erdem Topsakal serves as CVN director; he is also a professor and chair of the Department of Electrical and Computer Engineering at VCU. Dr. Gretchen Matthews serves as SWVA node director; she is also a professor in the Department of Mathematics at VT. The LC meets virtually every other week and in person for a full-day meeting once per quarter; in FY21, all in-person meetings were held in Richmond.

1.2.2 CCI Hub Organization

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

The CCI Hub held its first in-person retreat in June 2021, with participation by faculty, staff, interns, and graduate students resident in the hub (Figure 1.6).

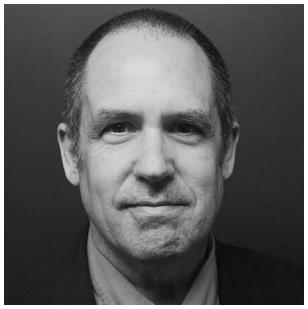
1.2.3 CCI Node Organization

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

Dedicated facilities in the hub and each of the nodes host CCI. In FY21, Mason opened its CCI Living Innovation Lab in their Arlington campus. The lab hosts CCI research infrastructure in autonomous vehicle security and cyber-manufacturing, depicted in Figure 1.7.

(a) Dr. Luiz DaSilva, Executive Director.

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



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

(d) Dr. Erdem Topsakal, CVN Director.

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

(f) Mr. John Delaney, Managing Director.

Figure 1.4: CCI Leadership Council.

Commonwealth Cyber Initiative

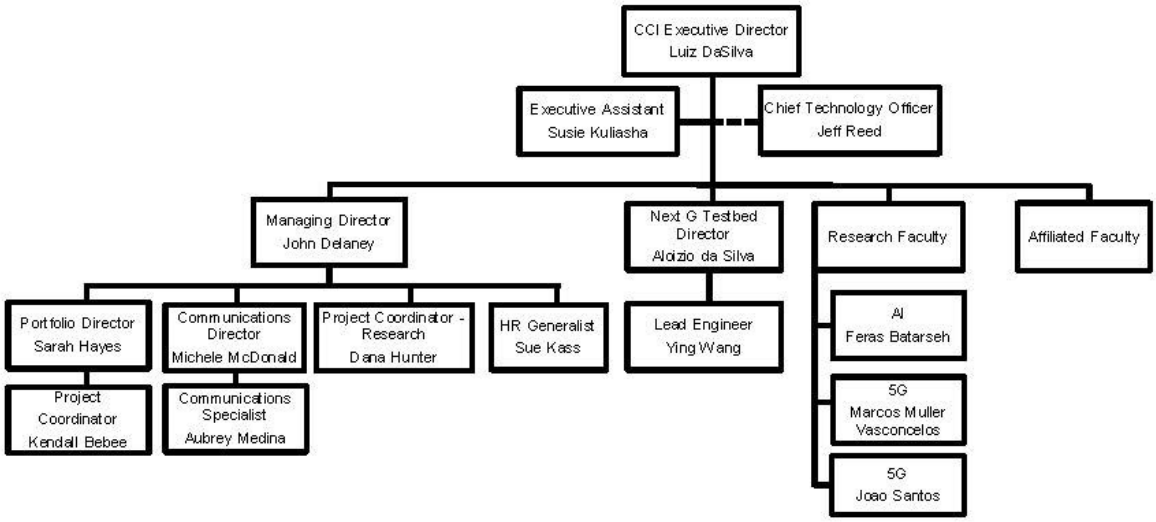


Figure 1.5: CCI organization chart.

Figure 1.6: CCI Hub staff, faculty, and students.

1.3 The CCI Technical Advisory Board

We established the CCI TAB in Fall of 2020, with its inaugural meeting held on November 17, 2020. The TAB is a key component of our governance structure, shown in Figure 1.2, providing advice and guidance on strategic direction for CCI.

The composition of the TAB is as follows:

- One Vice President for Research and Innovation (VPRI) from one of the institutions of higher education in CCI;
- One member appointed by the VIPA board or, 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.

We are fortunate to have an extremely distinguished inaugural TAB. Its members are (Figure 1.8):

- Prof. Elisa Bertino, Samuel D. Conte Professor, Purdue University;
- Mr. David Ihrie, Chief Technology Officer, CIT;
- Prof. Melur (Ram) Ramasubramanian, Vice President for Research, UVA;
- Prof. Sennur Ulukus, Anthony Ephremides Professor, University of Maryland College Park;
- Ms. Tracy Gregorio, Chief Executive Officer, G2Ops;
- Mr. Jim Mollenkopf, Vice President, Qualcomm;

(a) Dr. Liza Wilson Durant and Dr. Duminda Wijesekera.

(b) Autonomous vehicle testing equipment.

Figure 1.7: Cyber-manufacturing and autonomous vehicle testbed equipment in the CCI Living Innovation Lab at Mason.

- Mr. Zachary Tudor, Associate Lab Director, Idaho National Laboratory; and
- Mr. Dan Wooley, Strategic Partnerships Director, The MITRE Corporation.

(a) Prof. Elisa Bertino.

(b) Mr. David Ihrie.

(c) Prof. Melur (Ram) Ramasubramanian.

(d) Prof. Sennur Ulukus.

(e) Ms. Tracy Gregorio.

(f) Mr. Jim Mollenkopf.

(g) Mr. Zachary Tudor.

(h) Mr. Dan Wooley.

Figure 1.8: CCI Technical Advisory Board (TAB).

The TAB meets twice a year. In FY21, those meetings took place in November 2020 and June 2021; both meetings were held virtually.

1.4 The CCI Inclusion and Diversity Committee

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

Strategic Goal

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

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

- The establishment of programs that aim at increasing participation of under-represented groups in the cyber workforce;
- Diversity goals and considerations in all programs funded by CCI;
- The organization of seminars, workshops, and training events that highlight diversity issues of particular relevance to CCI research, such as gender and racial bias in AI systems and consideration of persons with disabilities in the design of autonomous systems;
- Outreach activities geared towards under-represented groups in Science, Technology, Engineering, and Mathematics (STEM).

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

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

The committee advised CCI in the selection process for participants in the CCI Summer Camp to be held in Summer 2021 and is currently designing a program to be launched in Fiscal Year 2022 (FY22).

1.5 CCI Communications

1.5.1 CCI Social Media Strategy, Website, and Metrics

CCI communications efforts began in late August 2020 and centered on the website as the main form of outreach with social media, newsletters, events, emails, and news articles bringing people to the website.

CCI created its social media accounts in early September 2020. Twitter and LinkedIn are the primary focus, showing strong and increasing engagement (Figure 1.9). Twitter followers and impressions have increased from 41 and 1,063 respectively in September 2020 — the first month of tracking — to 233 followers and 7,375 impressions 10 months later (Figure 1.10). At the end of June 2021, LinkedIn followers numbered 383, up from 42 in September 2020 (Figure 1.11). In spring 2021, the communications team started using Instagram for a Cyber Tip of the Week campaign to increase cyber hygiene awareness, in addition to a campaign for CCI's first Cyber Camp, to take place in July-August 2021.

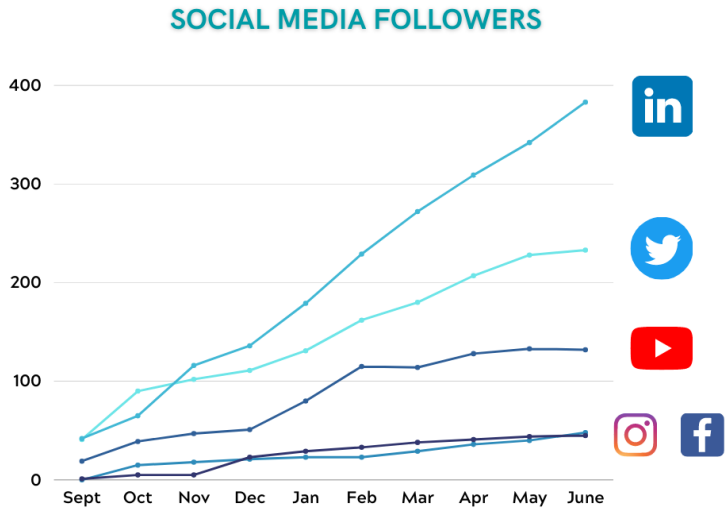


Figure 1.9: Social media followers for CCI's LinkedIn, Twitter, YouTube, Instagram, and Facebook accounts, from September 2020 to June 2021.

Figure 1.10: Evolution of Twitter impressions, profile visits, and followers from September 2020 to June 2021. The post with the highest number of impressions is also shown.

The monthly e-newsletter began in November 2020 with a subscriber base of about 300 at the start of FY20 and expanding to 1,600 by June 30, 2021. The average open rate for emails and newsletters is 39 %, with many emails exceeding 50 % open rates, well above typical average open rates of 21.33 %. Newsletters and emails also draw people to the CCI website, where they can find more information, resulting in spikes of website visits coinciding with outreach efforts. This is a simple way to show that our subscribers are engaged and interested in CCI's activities.

The CCI website has expanded as the informational needs of the network grow, and is today a useful site where researchers can find collaborators, news, events, programs, funded projects and more. Ongoing projects by the communications and marketing team include refreshing the faculty bio pages, adding new sections, and improving the user experience. The website had 1,116 users with 5,803 page views in October 2020, when analytics tracking began. That activity jumped to 3,316 users and 10,837 page views in February 2021 when CCI had a number of events and calls for research proposals (Figure 1.12).

Events for the Fall and Spring Seminar Series and informational workshops are recorded and featured on CCI's YouTube channel. Some webinars, such as "Reframing the Cyber Crisis: Patterns in Adaptive Systems and Design for Continuous Adaptability" by David Woods, an integrated systems engineering professor from

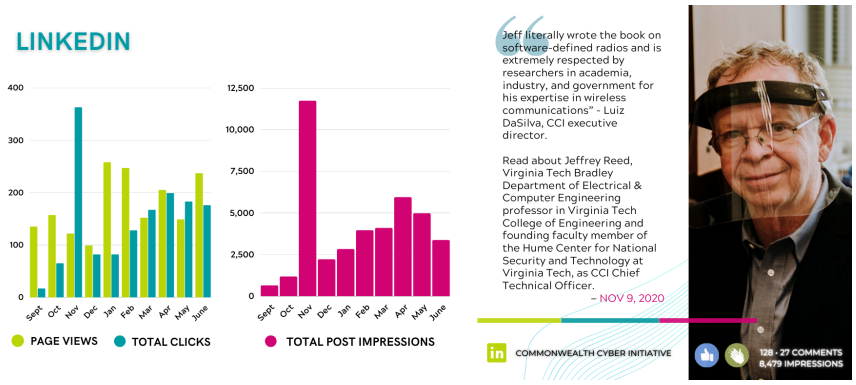


Figure 1.11: Evolution of LinkedIn page views, clicks, and impressions from September 2020 to June 2021. The post with the highest number of impressions is also shown.

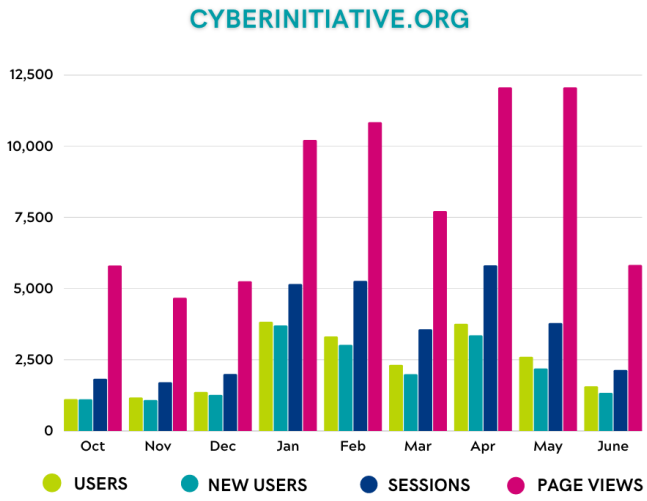


Figure 1.12: CCI website metrics: users, new users, sessions, and page views.

The Ohio State University, have as many as 500 views, allowing people who did not attend to still learn from nationally renowned speakers. Metrics for CCI's YouTube channel are shown in Figure 1.13.

The communications and marketing team members, who joined CCI in late August/September 2020, will continue to expand outreach efforts in FY22 to inform the community, increase CCI's name recognition and support research collaboration.

1.5.2 Appearances in the Media in FY21

Many of the programs and major achievements from CCI researchers and staff have appeared in the print and online media. The following is a list of media hits from July 2020 to June 2021, in reverse chronological order.

- **Old Dominion University**, June 25, 2021: "ODU Receives $1.45 Million State Grant Aimed at Boosting Cybersecurity Workforce".
- **George Mason University**, May 25, 2021: "New pilot space debuts in Arlington".
- **Fox 5 Washington, DC**, May 13, 2021: "Analysis: Hybrid and electric cars: Virginia Tech Professor

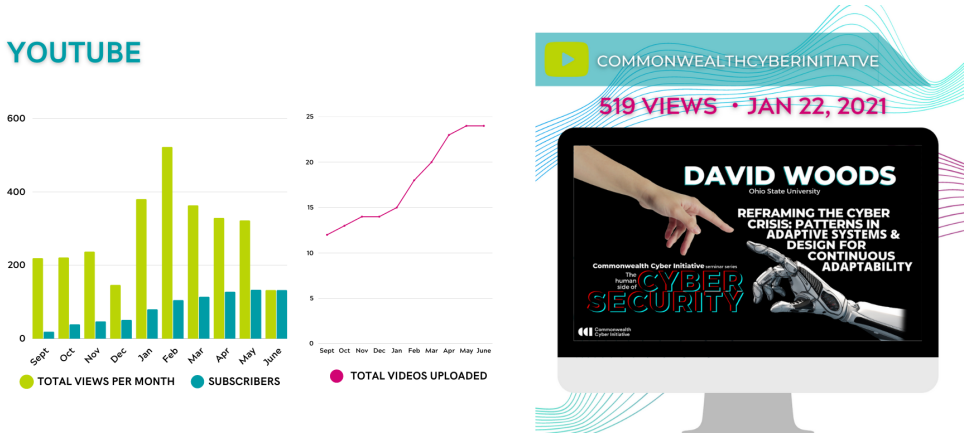


Figure 1.13: CCI YouTube metrics: total views, subscribers, number of videos uploaded. Also shown is the video with the most views in FY21.

Dr. Kevin Heaslip is here with the top five things drivers need to know about hybrid and electric cars.".

- **Richmond Times Dispatch**, May 13, 2021: "Pipeline shutdown highlights 'everyday threats' from cyber attacks as Congress looks to act".
- **William & Mary**, May 5, 2021: "Adwait Nadkarni is trying to keep 'smart cities' from becoming really dumb".
- **Virginia Tech**, April 28, 2021: "Commonwealth Cyber Initiative funds $1 million in experiential learning projects for Virginia students".
- **Virginia Tech**, April 28, 2021: "Daphne Yao recognized for pioneering contributions to the cybersecurity industry".
- **Virginia Tech**, April 16, 2021: "Taking it to the streets: Commonwealth Cyber Initiative funds research for autonomous cars".
- **George Mason University**, April 15, 2021: "Secure Manufacturing Saves Energy and Protects Businesses".
- **George Mason University**, April 15, 2021: "Mason Cybersecurity Engineering Design Team Protects Critical Infrastructure".
- **George Mason University**, April 13, 2021: "Mason Competitive Cyber Heads National Competition for the First Time".
- **Defense One**, March 29, 2021: "A Marine Logistics Base May Be the Warehouse of the Future".
- **Old Dominion University**, March 25, 2021: "Old Dominion University Part of Collaboration on $13 Million Department of Defense Contract".
- **George Mason University**, March 25, 2021: "Taking it to the Streets: Commonwealth Cyber Initiative Funds Research for Autonomous Cars".
- **Virginia Tech**, March 24, 2021: "Commonwealth Cyber Initiative researchers awarded $13 million contract to create 5G smart warehouse".
- **Richmond Times Dispatch**, March 23, 2021: "Brian Payne column: Cybercrime wave is a human – not a technological – problem".

- **Virginia Tech**, February 23, 2021: "Virginia Tech researchers receive cybersecurity research collaboration grants from the Commonwealth Cyber Initiative".
- **Washington Business Journal**, February 22, 2021: "GMU taps powerhouse business coalition to guide Arlington campus growth".
- **Old Dominion University**, February 19, 2021: "ODU School of Cybersecurity and Center for High Impact Practices Receive $3.9 million NSF Grant".
- **Old Dominion University**, February 8, 2021: "Old Dominion University Professors Awarded Nearly $1 Million in Cybersecurity-Related Grant Funding Through Coastal Virginia Center for Cyber Innovation".
- **George Mason University**, February 3, 2021: "Mason Researchers Receive CCI Grants for Cyber and Arts Program".
- **George Mason University**, February 2, 2021: "Researchers receive over $1.5 million from DARPA to optimize security and energy tradeoff".
- **Virginia Tech**, January 28, 2021: "Department of Defense awards Virginia Tech $1.5 million to prepare students for cybersecurity careers".
- **George Mason University**, January 19, 2021: "Mason Engineering BS in Cybersecurity Engineering Earns ABET".
- **Virginia Commonwealth University**, January 4, 2021: "Electrical and computer engineering chair co-edits book on medical applications of antenna and sensor technologies".
- **George Mason University**, January 4, 2021: "Mason Competitive Cyber Club Cracks the Code, Hacks a Building".
- **George Mason University**, December 2, 2020: "Mason Engineering Cybersecurity Expert Receives Prestigious Award for His Research".
- **George Mason University**, November 20, 2020: "Mason to Lead Regional Hub for National Cybersecurity Advanced Manufacturing Innovation Partnership".
- **George Mason University**, November 16, 2020: "Cybersecurity Researchers Developing a Toolkit to Protect Open-Source Software from Cyberattacks".
- **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".
- **George Mason University**, August 4, 2020: "Cybersecurity Engineering Masters Ranked in Top 20".
- **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".

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

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

1.6 Report Structure

This report describes the progress and achievements of the CCI Hub and four Regional Nodes throughout FY21. Chapter 1 outlines our vision and mission, describes the organization of the CCI Hub and Nodes, and summarizes our media strategy. Progress on the three mission lines of research, workforce development, and innovation is described in Chapters 2, 3, and 4, respectively. Chapter 5.1 is devoted to CCI's collaborative partnerships and projects. Chapter 6 contains the financial reports from the hub and nodes for FY21. Finally, Chapter 7 describes our main activities and programs planned for FY22.

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

- 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.

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

Chapter 2

CCI Research

This chapter summarizes the main achievements in FY21 for the CCI research mission line.

2.1 External Grants to Support the Work of CCI

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

2.1.1 Extramural Funding in FY21

In FY21, the CCI Hub and the four Regional Nodes received 112 external grants totaling $37,126,064 to support our mission lines of research, workforce development and innovation/commercialization. The CCI Hub faculty attracted 14 grants to their institution, totaling $7,078,594. 90% of all grants were from federal agencies and 10% were from state agencies and industry. Summary information is shown in Figure 2.1 and details are found in Appendix 1.

Federal Grants	Industry Grants
10	4
Total Funds	**Total Funds**
$6,207,925	$870,669

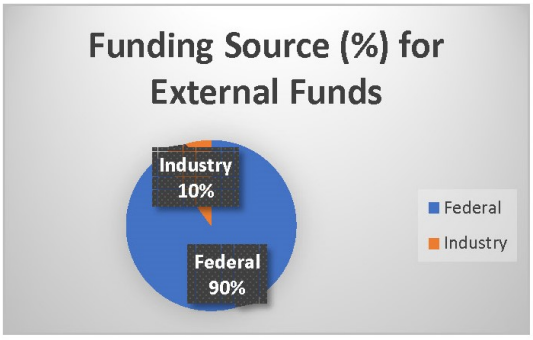


Figure 2.1: External funding obtained by the CCI Hub in FY21.

Faculty engaged in the CCI Regional Nodes attracted 98 grants totalling $30,047,470. A summary is displayed in Figure 2.2 and detailed information is found in Appendix 2.

Node	Number of Grants	Grant Total
Central Virginia	25	$3,750,688
Coastal Virginia	32	$12,250,505
Northern Virginia	21	$7,004,825
Southwest Virginia	20	$7,041,452
Total	**98**	**$30,047,470**

Federal Grants	State/Industry Grants
68	**30**
Total Funds	**Total Funds**
$26,913,206	**$3,134,264**

Figure 2.2: Extramural funding obtained by regional nodes in FY21.

2.1.2 Spotlight: NSC 5G Smart Warehouse Project

This project is one of the best examples of how CCI can bring to Virginia large projects that require breadth of cybersecurity expertise and collaboration among researchers across the network. In early 2021, we were awarded a $13 million DoD contract to develop a 5G-enabled smart warehouse at the Marine Corps Logistics Base in Albany, Georgia.

The project is primed by Virginia Tech Applied Research Corporation (VT-ARC), with a team of researchers from five CCI universities: ODU, VT, Mason, VCU, and UVA. Sachin Shetty is the project's technical lead and holds dual appointments as executive director of the Center for Secure & Intelligent Critical Systems at Virginia Modeling, Analysis and Simulation Center (VMASC) and associate professor in the Department of Computational Modeling and Simulation Engineering; all at ODU.

Fast 5G wireless connectivity combined with internet of things sensor networks promises to change how warehouses move and track items to ensure they arrive at their intended destination in a timely manner. It is no easy task: the 5G communications architecture must be adept at navigating a noisy warehouse environment, be quick about it, and have a long battery life to boot. Figure 2.3 illustrates how this technology can revolutionize warehouse operations.

CCI was critical to the contract, creating the connections to build a team and funding a substantive portion of the proposal development. CCI researchers from Virginia Tech, Old Dominion University, Virginia Commonwealth University, University of Virginia, and George Mason University will collaborate across disciplines, including electrical and computer engineering, systems engineering, wireless communications, modeling, simulation, and analysis to develop the low-latency, resilient, and energy-efficient 5G network for the Marine Corps Logistics Base's smart warehouse prototype. Four industry partners — Intelligent Automation Inc., PerspectaLabs, Keysight, and B3 Advanced Communications — are also part of the project.

The project will utilize the CCI NextG Testbed, one of the few in the nation. The CCI NextG Testbed is a testable and integrative piece across the main milestones of the project. It will serve as an intermediate platform for testing 5G connectivity with the resilient distributed position system before integrating it with the Albany smart warehouse. The CCI NextG Testbed will also allow the partners working in different subtasks to test and improve the performance of different building blocks before they're put to work at the Albany warehouse site.

5G can bridge the gap between indoor and outdoor mobile communications, connecting 4G for outdoor use with WiFi for the indoor environment, to help monitor an outbound order that includes goods in-transit that have not yet been received at the warehouse. 5G enabled sensors also can track smaller items, a task too expensive with current technology. Other advantages include 5G's reduced latency means there is little lag time between when a sensor detects information and when it is recognized by the system. This will enable vehicle-to-vehicle communication for automated trucks and warehouse robots. Processing power will

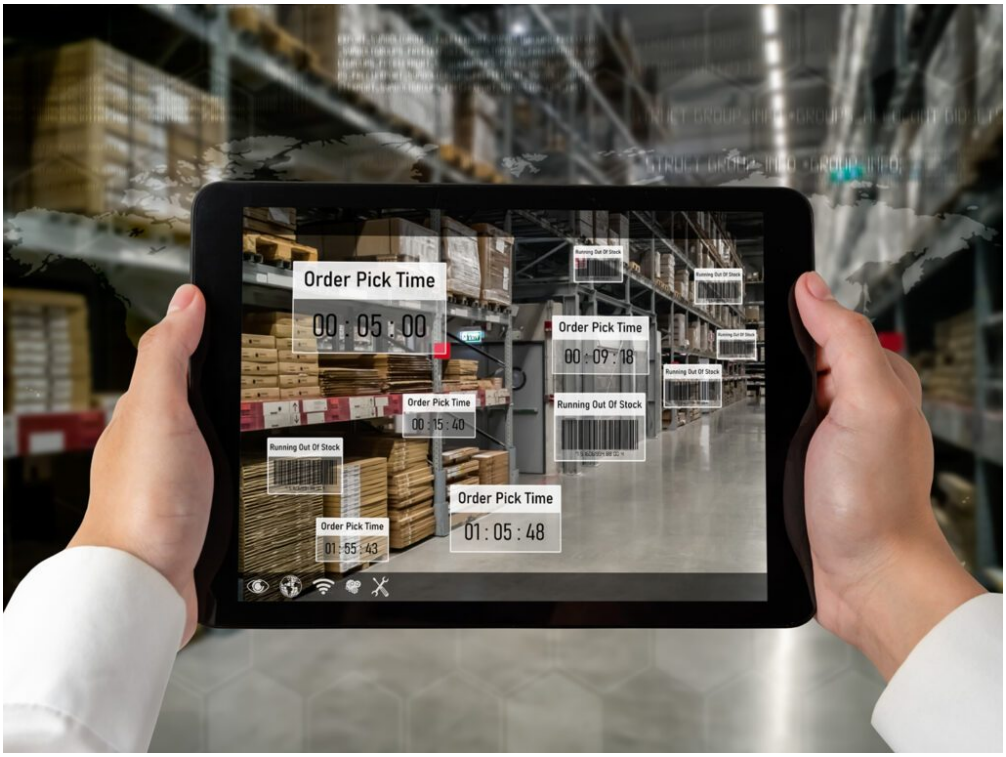


Figure 2.3: Smart warehouse functionality.

be able to move closer to the work, increasing the capability of sensors and mobile devices.

2.2 Research Grants Awarded from the Funds in HB30

In FY21, CCI awarded grants to the participating institutions, aligned with our goals in research, workforce development, and innovation. These funds were awarded on a competitive basis, with researchers responding to calls for proposals issued by CCI. Proposals were reviewed by experts in the area of each call, and the LC made final funding decisions based on recommendations from reviewers. This section describes the grants awarded in this Fiscal Year from CCI funds.

In FY21, we issued seven calls for proposals to researchers across the network. We centrally managed 122 submitted proposals, which were evaluated by 85 reviewers. This hard work ensures that the best ideas, aligned with the mission of CCI, are selected for funding in an open and transparent manner.

2.2.1 Collaborative Research Program

Objective of the Call

This CCI Cybersecurity Research Collaboration funding program aims to create cross-pollination opportunities for cybersecurity researchers to collaborate across the commonwealth and to develop a commonwealth-wide ecosystem of innovation excellence in cybersecurity. All projects have collaborators from more than one CCI Node.

A budget of $4M was allocated to this call, with approximately $1M for projects led by researchers in each of the CCI Nodes. Proposal budgets could not exceed $250K. Proposals were aligned with the strategic areas identified by each of the nodes, namely:

- Central Virginia: cyber physical systems, autonomous systems, Internet of Things (IoT) as they apply to smart cities and communities, as well as medical device security.

- Coastal Virginia: the intersection of cyber-physical systems and artificial intelligence in maritime, defense, and transportation sectors.
- Northern Virginia: cybersecurity in national defense, transportation, electric/power distribution, and manufacturing sectors. Also, the impact of human behavior on cyber security and resilience of cyber systems to human behavior.
- Southwest Virginia: Cybersecurity related to wireless communications and application domains such as transportation, power systems, manufacturing, autonomous vehicles, and agriculture; cybersecurity and emerging technologies, such as quantum computing; and cryptography.

Selection Criteria

Proposals were reviewed by subject matter experts and evaluated according to the following criteria: strong intellectual merit related to CCI's mission; strong broader impacts related to CCI's mission; responsiveness to node focus areas and relevance to industry needs; multi-institutional, cross-node collaborations; and potential to generate additional funding and revenue.

Research Grants Awarded

The number and value of grants associated with each CCI node are tabulated in Figure 2.4. Individual grants are listed in the Appendix.

Node	Number of Grants	Grant Total
Central Virginia	5	$999,275
Coastal Virginia	5	$994,850
Northern Virginia	6	$999,999
Southwest Virginia	6	$1,000,000
Total	**22**	**$3,994,124**

Figure 2.4: Collaborative research grants in FY21, per node.

2.2.2 Arts and Design Program

Objective of the Call

This program targets researchers from the arts and design community across the CCI Network. The program is funded by CCI and co-organized with Institute for Creativity, Arts, and Technology (ICAT) at VT, and the da Vinci Center for Innovation at VCU. The program challenges the community of researchers in the Arts and Design to reimagine and depict the results of cybersecurity research (and in particular research that occurs in CCI) either for scientific purposes, or for creative arts practice purposes.

Selection Criteria

Proposals were reviewed by subject matter experts and evaluated according to the following criteria: alignment with CCI research and responsiveness to the objectives of this call; impact to commonwealth residents, students, and employers; clear deliverable and dissemination strategy proposed for the project.

Research Grants Awarded

The number and value of grants associated with each CCI node are tabulated in Figure 2.5. Individual grants are listed in the Appendix.

Node	Number of Grants	Grant Total
Central Virginia	1	$25,000
Coastal Virginia	1	$25,000
Northern Virginia	1	$25,000
Southwest Virginia	2	$50,000
Total	**5**	**$125,000**

Figure 2.5: Arts and Design Research Grants in FY21.

Spotlight: What Does Dance Have to Do with Cybersecurity?

Kate Sicchio, assistant professor of Dance and Media Technologies at VCU School of the Arts, is the principal investigator for the CCI-funded project "Moving Choreography to a New Universe: an AI-Driven Privacy Automation Approach." Dr. Sicchio's research is part of the CCI Building Bridges Arts and Design Collaboration Program, which was created to engage the community of researchers in arts and design to re-imagine and depict the results of cybersecurity research either for scientific or creative arts purposes.

When developing choreography using technology, a legacy is left beyond the ephemeral material of movement. There are libraries of data such as photos, motion capture data or even biofeedback from sensors. How can this data still be used and not breach privacy concerns of dancers and performers who may not realize the longevity of the data they have provided, or the implications of future uses of this data? This project is developing an AI algorithm-driven deep learning framework to detect, identify, extract the dancer bodies in specific dancing scenes, and use the Generative Adversarial Network (GAN) model to cover-up and translate the image to protect the privacy of the dancer.

Dr. Sicchio is collecting movement data to see how the team can potentially train AI to protect the identity of those being tracked. The research will also be featured in a dance performance the research team plans to premiere this fall. Research assistants Tamara Denson, VCU dance major, and Taylor Colimore, VCU kinetic imaging major, depicted in Figure 2.6, are helping to bring the project to life. The project's co-principal investigators are Yan Lu, research assistant professor, VMASC, ODU; and Sachin Shetty, executive director of the Center for Secure & Intelligent Critical Systems at VMASC.

Figure 2.6: Kate Sicchio's research assistants Taylor Colimore, VCU kinetic imaging major, and Tamara Denson, VCU dance major, are working on movement to capture for the CCI project.

2.2.3 The Role of Cybersecurity in the Spread of Disinformation and Misinformation

Objective of the Call

Many important problems in CCI's focus area require expertise in the relevant technologies combined with expertise in social/economic/policy/legal/ethical domains. Examples include election security, privacy and ethical concerns with the introduction of artificial intelligence, cyber offensive activities, misinformation, disinformation, data-driven public policy, etc. With CCI, we have a unique opportunity to build multi-disciplinary teams of researchers from across Virginia to collaborate on some of these problems.

The deliberate or inadvertent spread of false information is increasingly viewed as a national security issue with elements of cybersecurity, intelligence and foreign policy going to the heart of how and why these narratives are created, how they flourish, and what we can do about them. In the words of Dr. David Woods, an expert on human factors in cybersecurity and a recent speaker in the CCI seminar series, "disinformation campaigns – emergent and intentional – are the challenge of the next decade."

This program funds multi-disciplinary teams in the CCI network to conduct research on the how cybersecurity and artificial intelligence tools and concepts may help to limit, deter, or stop the creation and spread of disinformation and misinformation.

The objectives of the program are: to provide seed funding for multi-disciplinary teams to address a research question that requires the combination of technical expertise in cybersecurity and artificial intelligence with expertise in the social sciences, humanities, and/or law; to generate research findings that advance the state of the art on the topic; and to increase the competitiveness of the teams for extramural funding.

Selection Criteria

Proposals were reviewed by subject matter experts and evaluated according to the following criteria: strong intellectual merit relevant to CCI's mission and to the topic of this call; strong broader impacts related to CCI's mission; relevance to the needs of industry and government agencies; building of multi-disciplinary expertise in Virginia on the role of cybersecurity in curbing the spread of misinformation and disinformation; and potential to generate additional funding and revenue.

Research Grants Awarded

The number and value of grants associated with each CCI node are tabulated in Figure 2.7. Individual grants are listed in the Appendix.

Node	Number of Grants	Grant Total
Central Virginia	1	$65,000
Coastal Virginia	2	$128,790
Northern Virginia	2	$129,967
Southwest Virginia	2	$130,000
Total	**7**	**$453,757**

Figure 2.7: Grants awarded in the program The Role of Cybesecurity in the Spread of Disinformation and Misinformation.

2.2.4 Experimental Research and Infrastructure Call

Objective of the Call

CCI has been investing in creating unique research infrastructure available for use by researchers in all CCI member institutions, in particular a NextG testbed that supports experimental research in AI and a 5G and beyond communication networks. This program funds research that uses current testbed capabilities in CCI,

as well as proposals that will augment these capabilities in the CCI Nodes in Central, Coastal, Northern, and Southwest Virginia.

This call sought proposals in two categories:

- Experimental research: proposals in this category must articulate a research problem in the focus area of CCI (cybersecurity, autonomous systems, and data) and address the problem through experimental investigations using the CCI AI Testbed or CCI 5G Testbed (or both).
- Research infrastructure: proposals in this category will augment the capabilities of the CCI AI Testbed or CCI 5G Testbed (or both), through the deployment of additional hardware and/or software in CCI's Regional Nodes.

Selection Criteria

Proposals were reviewed by subject matter experts and evaluated according to the following criteria: strong intellectual merit relevant to CCI's mission and to the topic of this call; strong broader impacts related to CCI's mission; relevance to the needs of industry and government agencies; building or use of shared research infrastructure in Virginia; potential to generate additional funding and revenue.

Research Grants Awarded

The number and value of grants associated with each CCI node, under the experimental research category, are tabulated in Figure 2.8. Individual grants are listed in the Appendix. Additionally, each node awarded a $150,000 grant under the research infrastructure category of this call.

Node	Number of Grants	Grant Total
Central Virginia	2	$100,000
Coastal Virginia	2	$99,906
Northern Virginia	1	$49,624
Southwest Virginia	3	$150,000
Total	**8**	**$399,530**

Figure 2.8: Grants in the Experimental Research in CCI Testbeds program.

2.2.5 CCI Fellows

The CCI Fellows Program completed its first full year in FY21. In 2020, CCI selected nine fellows (see Figure 2.9) from universities in the CCI network to represent CCI and conduct cybersecurity related research, develop experiential learning projects and develop and/or participate in workforce development programs. The primary objective of the CCI Fellows Program is for the fellows to contribute to CCI's research mission while fostering collaboration and engagement across the commonwealth's cybersecurity ecosystem.

In FY21, Dr. Hongyi Wu from Old Dominion University and Dr. Milos Manic from Virginia Commonwealth University each hosted and moderated a four-part seminar series for the Fall of 2020 and the Spring 2021 academic semesters.

The Fall Seminar Series theme was "AI for Cybersecurity" and featured the following four webinars:

- "Stealing Neural Networks with Model Extraction Attacks," Dr. Nocholas Carlini
- "Is AI Taking Over the World? No, But It's Making It Less Private," Dr. Giuseppe Ateniese
- "Security, Privacy and Safety in the Internet of Things," Dr. Elisa Bertino
- "Optimizing and Securing Wireless 5G, IoT and Beyond with Maching Learning," Dr. Timothy O'Shea

The Spring Seminar Series theme was "The Human Side of Cybersecurity' and featured the following four webinars:

Fellow	University	Grant Amount
Dr. Duminda Wijeskera	George Mason University	$50,000
Dr. Kai Zeng	George Mason University	$50,000
Dr. Hong-yi Wu	Old Dominion University	$50,000
Dr. Sachin Shetty	Old Dominion University	$50,000
Dr. Yeng-Hung Hu	Norfolk State University	$50,000
Dr. Milos Manic	Virginia Commonwealth University	$50,000
Dr. Jack Davidson	University of Virginia	$50,000
Dr. Jeff Pittges	Radford University	$50,000
Dr. Kevin Heaslip	Virginia Tech	$50,000

Figure 2.9: CCI Fellows FY21.

- "Reframing the Cyber Crisis: Patterns in Adaptive Systems and Design for Continuous Adaptability," Dr. David Woods
- "Security and Privacy for Humans," Dr. Lorrie Cranor
- "Universal Laws, Architectures, and Systemic Fragility's in Bio, Med, Neuro, Tech and Social Systems," Dr. John Doyle
- "A Cyber Concept of Operations for Human-in-the-Loop Resilience," Dr. Ronald, Boring

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

Dr. Sachin Shetty, Old Dominion University. Dr. Shetty is conducting research on blockchain- and 5G-empowered asset management resulted in commercialization of a blockchain-based IoT solution and efforts are under way to set up a startup company.

Dr. Jeff Pittges, Radford University. Dr. Pittges is leading a workforce development project to develop an infrastructure to recruit students into the STEM fields, prepare them for experiential learning and support them during the learning experience, develop an employer network, and identify best practices for successful experiences. Dr. Pittges worked with CivilianCyber and others to build an employer network and develop a sustainable funding model for companies in the network to support internships and co-ops.

Dr. Duminda Wijesekera, George Mason University. Dr. Wijesekera is conducting research on ways to advance the research in cybersecurity of 5G and Connected Automated Vehicles. Dr. Wijesekera developed a testbed for virtual driving under controlled weather and lighting conditions and created a testbed at the Mason Arlington campus using City Engine. This testbed provides repeatable testbed for multiple human drivers to drive among automated vehicles on a realistic rendering of roads.

Dr. Hongyi Wu, Old Dominion University. Dr. Wu leads the research and innovation project titled A Development and Experimental Environment for Privacy-preserving and Secure (DEEPSECURE) Machine Learning Research. The goal of the project is to close the cyber workforce gap by integrating a spectrum of essential functions and building blocks that are ready-to-use to flatten the learning curve for researchers coming from both the machine learning and security/privacy communities.

Dr. Frank Hu, Norfolk State University. Dr. Hu's research and workforce development projects focus on developing deep learning technology to identify advanced persistent threats and workforce development programs for students at Historically Black Colleges and Universities (HBCU) and other universities. The research developed several multi-layered deep learning approaches for classifying advanced persistent threats and developed four procedures for the project: data analytics, image conversion, deep learning models and simulation set-ups.

Dr. Kai Zeng, George Mason University. Dr. Zeng is conducting research on securing 5G wireless networks. 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 is pursuing a comprehensive research plan to

investigate 5G wireless network security 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 networks, secure 5G wireless communications under mobility, and testbed development.

Dr. Kevin Heaslip, Virginia Tech. Dr. Heaslip is one of two CCI members advising Arlington County on its Smart City Program. Dr. Heaslip is advising the county on the means and methods to ensure the privacy of citizens and the security of data if local governments install cameras in public spaces for safety, security, health, or movement management.

Dr. Milos Manic, Virginia Commonwealth University. Dr. Manic is working closely with Battelle Energy Alliance in a variety of cybersecurity and AI research projects.

2.2.6 Other Grants Awarded by the Hub and Nodes

CCI has affiliated faculty attached to academic departments at Virginia Tech and conducting CCI-funded research in the CCI Hub. These faculty members are listed in Figure 2.10.

Faculty	Department	Grant Amount
Dr. Tam Chantem	Electrical and Computer Engineering	$280,000
Dr. Ryan Gerdes	Electrical and Computer Engineering	Team w/ Chantem
Dr. Wenjing Lou	Computer Science	$270,000
Dr. Haining Wang	Electrical and Computer Engineering	$173,000
Dr. Laura Freeman	Statistics	% of Salary

Figure 2.10: CCI faculty grants in FY21.

Dr. Tam Chantem and Dr. Ryan Gerdes are teaming together for research on securing time-sensitive cyber physical systems. Many Cyber Physical Systems (CPSs) have Real Time (RT) requirements, such as a network of Uncrewed Autonomous Vehicles (UAVs) that deliver packages to customers' homes or a robot that performs/aides in cardiac surgery. In those applications, 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 goal of the research is to design secure RT-CPS that are less complex, easier to analyze, and more reliable for critical application domains such as defense, medicine, transportation, manufacturing, and agriculture.

Dr. Wenjing Lou is conducting research on developing a blockchain-based decentralized spectrum access system. In her work, Dr. Lou proposes a novel blockchain-based decentralized Spectrum Access System (SAS) that leverages a zero-trust network architecture without assuming full trust in each individual SAS server, i.e., the system can tolerate a certain level of server failure or malicious behavior. Additionally, the trustworthy record-keeping capability of blockchain will allow fair, transparent (auditable) spectrum allocation, and the smart contract supported by blockchain will allow automatic spectrum allocation. In the proposed system, a global blockchain (G-Chain) is used for spectrum regulatory compliance while smart contract-enabled local blockchains (L-Chains) are instantiated in individual spectrum zones for automating spectrum access assignment per user request. The two-layer structure has significant performance benefits.

Dr. Haining Wang is conducting a comprehensive investigation of account-identity inconsistency threats in online authentication. Authentication has been the key mechanism enabling secure access and privacy preservation for Internet users. Existing service providers (e.g., web service providers) typically delegate identity management and its security responsibilities to trusted identity providers such as email providers. While this approach enables centralized and reliable management of user identities, unexpected incidents on the identity provider side might be obscure to service providers, thus causing inconsistency between accounts and identities. Such inconsistency may pose serious security threats to both users and service providers, allowing adversaries to fully control the target accounts and commit fraudulent online activities. While extensive efforts have been devoted to designing robust authentication mechanisms, little attention has yet been paid to the emerging inconsistency threats that exist in user authentication. In this project, we secure existing user authentication systems by investigating security risks raised from emerging inconsistency threats.

2.3 Faculty Recruited

2.3.1 Hub Faculty

We were able to recruit four distinguished researchers to the CCI Hub in FY21. They come from the University of Southern California, Trinity College Dublin, Northeastern University, and Mason, and bring a unique mix of expertise in 5G systems, AI Assurance, and cybersecurity. They are:

Dr. **Feras Batarseh** is a research associate professor in CCI and the Bradley Department of Electrical and Computer Engineering at VT. His research spans the areas of AI for public policy, AI Assurance, data engineering, and context-aware software Systems. His work has been published in various prestigious journals and international conferences. Dr. Batarseh has published multiple chapters and books; his two recent books are: "Federal Data Science" and "Data Democracy", both by Elsevier's Academic Press. Dr. Batarseh is a member of the Institute of Electrical and Electronic Engineers (IEEE), the Agricultural and Applied Economical Association (AAEA), and the Association for the Advancement of Artificial Intelligence (AAAI). He has taught AI and data science courses at multiple universities including Mason, University of Maryland - Baltimore County (UMBC), Georgetown University, and George Washington University (GWU). Dr. Batarseh obtained his Ph.D. and M.Sc. in computer engineering from the University of Central Florida (UCF) (2007, 2011), a graduate certificate in project leadership from Cornell University (2016), and another in public policy economics from the University of Oxford (2020). Prior to joining Virginia Tech, Dr. Batarseh was a research assistant professor at the College of Science at Mason and the director of Turing Research, an applied AI research group at Mason. Additionally, he was a Program Manager at MicroStrategy Inc., where he helped many institutions such as federal government agencies develop their data infrastructure and data mining applications.

Dr. **Aloizio Pereira da Silva** is the CCI 5G and NextG Testbed director. Da Silva's areas of interest include wireless networks, 5G and beyond. His expertise includes Software Defined Network (SDN), Software Defined Radio (SDR), Network Function Virtualization (NFV), IoT, smart cities and communities, and Mobile Edge Computing (MEC). He also has a background in deep-space communication intersecting with delay and Delay and Disruption Tolerant Network (DTN). Da Silva is also technical project manager for Platforms for Advanced Wireless Research (PAWR) program at US-IGNITE/NSF PAWR PPO where he manages and oversees PAWR testbeds, including AERPAW, POWDER, COSMOS and ARANET. Da Silva has vast experience on European Horizon projects acquired during his role as 5G portfolio manager and research fellow at the University of Bristol, in the UK. Da Silva earned his bachelor of science degree in computer science from the Pontificia Universidade Católica de Minas Gerais, master of science (MSc) in computer science from the Universidade Federal de Minas Gerais, master of business administration (MBA) in project management from the Fundação Getúlio Vargas and Babson Executive College, and doctorate (Ph.D) in computer engineering from the Instituto Tecnológico de Aeronáutica, in Brazil.

Dr. **Joao Santos** joins CCI from Trinity College Dublin, Ireland, where he completed a Ph.D. in electrical engineering. His main research interests include radio resource management, radio virtualization, network slicing, network security, and end-to-end network orchestration. Dr. Santos' research experience includes developing SDR systems, implementing radio virtualization mechanisms, and bridging SDR with SDN in support of programmable end-to-end communication networks, which led to a number of articles published in international conferences and high-impact journals. Dr. Santos

obtained his Ph.D. in electronic & electrical engineering from Trinity College Dublin (2021) and B.Sc. in telecommunications engineering from Universidade Federal Fluminense (UFF) (2016). Prior to joining Virginia Tech, Dr. Santos was a research assistant at the CONNECT Centre, Ireland's national research center for Future Networks and Communications. Additionally, he formerly worked at Rede Nacional de Ensino e Pesquisa (RNP) as the main developer of the Clearinghouse for FIBRE, Brazil's national testbed federation for future internet experimentation.

Dr. **Marcos M. Vasconcelos** joins CCI from the University of Southern California, Los Angeles, CA, where he was a postdoctoral research associate in the Ming Hsieh Department of Electrical Engineering from 2016 to 2020. Dr. Vasconcelos received his Ph.D. and M.Sc. from the University of Maryland College Park in 2016 and 2014. He received his B.Sc. and M.Sc. from the Federal University of Pernambuco in Recife, Brazil. He is currently a research assistant professor in the Commonwealth Cyber Initiative and the Bradley Department of Electrical and Computer Engineering at Virginia Tech. His research interests include networked control, estimation, communication networks, game theory, multi-agent optimization, distributed machine learning, applied probability, and systems biology.

2.3.2 Node Faculty

2.3.3 Northern Virginia Node

Dr. **Guiseppe Alteniese**, George Mason University, Cybersecurity and Cryptography. Dr.Alteniese was the David and GG Farber Endowed Chair in Computer Science and department chair at Stevens Institute of Technology. He was with Sapienza-University of Rome (Italy) and assistant/associate Professor at Johns Hopkins University (USA), and one of the founders of the JHU Information Security Institute. He received the NSF CAREER Award for his research in privacy and security, and the Google Faculty Research Award, the IBM Faculty Award, and the IEEE CISTC Technical Recognition Award for his research on cloud security. He has contributed to areas such as proxy re-cryptography, anonymous communication, two-party computation, secure storage, and provable data possession. He is currently working on cloud security and machine learning applied to security and intelligence issues for which he received an IBM SUR Award. He is also investigating new security applications for decentralized computing based on the blockchain/bitcoin technology.

Dr.**Xin-Wen Wu**, University Mary Washington, Security and reliability for emerging networked systems, applied cryptography. Prior to joining University of Mary Washington, Dr. Wu was an associate professor of computer science at Indiana University of Pennsylvania. He held research and faculty positions at the University of California at San Diego (as a post-doctoral researcher), University of Melbourne, Australia (as a research fellow), University of Ballarat, Australia, and Griffith University, Australia. Dr. Wu's research is focused on the intersection of data and cybersecurity, applied cryptography, networking, coding techniques, security and reliability for emerging networked systems, and information theory. Dr. Wu is a senior member of IEEE.

2.3.4 Coastal Virginia Node

Dr.**Le Thanh Tan**, Old Dominion University, Ph.D., engineering, Institut National de la Recherche Scientifique (2015). Dr. Tan Le received his Bachelor of Engineering and Master of Engineering degrees from Ho Chi Minh University of Technology in 2002 and 2004, respectively, and his Ph.D. degree from the University of Quebec in 2015. From 2002 to 2010, he was a lecturer with the Ho Chi Minh University of Technology and Education. He was a postdoctoral research associate at the Ecole Polytechnique de Montreal in 2015-2016, Arizona State University in 2016-2017, and Utah State University in 2017-2020. He is currently working as a research assistant professor in the Virginia Modeling, Analysis and Simulation Center, Old Dominion University. Dr. Le's research focuses on artificial intelligence, machine learning, cybersecurity, Internet of

Battle Things, vehicular networks, Blockchain, 5G and beyond network, smart healthcare, edge/fog/cloud computing, and software defined networking.

Dr. **Rui Ning**, Old Dominion University, Ph.D., engineering, Old Dominion University (2020). Dr. Rui Ning, received his Bachelor of Science in Computer Science and Engineering from Lanzhou University, China in 20111, his Master of Science in Computer Science from the University of Louisiana at Lafayette in 2016, and his Ph.D. in Electrical and Computer Engineering from Old Dominion University in 2020. He is a research assistant professor in the School of Cybersecurity, Old Dominion University. He received the Mark Weiser Best Paper Award at the IEEE International Conference on Pervasive Computing and Communication in 2018, the IEEE INFOCOM 2019 best in-session presentation award. and the ECE graduate student award Ph.D. Researcher of the Year award in 2019. Dr. Ning's research interests fall into the intersection of cybersecurity and machine learning.

Dr. **Moeti Masiane**, Norfolk State University, Ph.D., computer science & applications, Virginia Tech (2020). Dr. Moeti Masine received his Bachelor of Science in Applied Computer Science from the University of the District of Columbia in 2005, his Master of Science in Computer Science from Norfolk State University in 2010, and his Ph.D. in Computer Science from Virginia Tech in 2020. He previously worked for Google, Adobe Systems and the US Army Research lab. His research focus is on in-person and crowd studies and perception modelling using machine learning. He was a research scientist at Norfolk State, but accepted a full-time position with the National Reconnaissance Office in July 2021.

Daniel Shin, William & Mary, JD, Law, William & Mary (2019). Daniel Shin, Esq., received his Bachelor of Science from Northwestern University, his Master of Arts from the University of Mannheim, Germany, and his J.D. from William & Mary. He is the cybersecurity researcher at the Center of Legal & Court Technology, College of William & Mary. His research supports the fields of cybersecurity and supply chain protection, deepfakes, and machine learning. He is working to bridge the gap between legal and technical fields of emerging technologies.

Dr. **Yan Lu**, Old Dominion University, Ph.D., modeling & simulation, Old Dominion University (2020). Dr. Yan Lu received her Bachelor of Science in Computer Science from Beijing Jiaotong University in 2004, her Master of Science in Circuit and Systems from the Chinese Academy of Sciences in 2007, and Master of Science in Computer Science from Virginia Commonwealth University in 2009, and her Ph.D. in Modeling and Simulation from Old Dominion University in 2020. She is a research assistant professor in the Virginia, Modeling, Analysis and Simulation Center, Old Dominion University in 2020. She is a member of the Association for Computing Machinery Special Interest Group on Simulation, and she received the Gene Newman Award from ODU in 2018. Her research includes artificial intelligence, deep learning, machine learning and its application in image processing, cybersecurity, and reliable and trustworthy artificial intelligence.

2.3.5 Southwest Virginia Node

Dr. **Anthony Vance**, professor, Department of Business Information Technology, Pamplin College of Business, Virginia Tech. Dr. Vance was recruited from Temple University in Philadelphia, PA where he led the Fox School of Business' Center for Cybersecurity. He was Danny & Elsa Lui Distinguished Associate Professor at University of Hawaii and held appointments at Brigham Young University. Dr. Vance earned Ph.D. degrees in information systems from Georgia State University, USA; in management science from the University of Paris—Dauphine, France; and in information processing science from the University of Oulu, Finland. He also worked as a cybersecurity consultant at Deloitte. Dr. Vance's research program focuses on behavioral and organizational aspects of security as well as neuroscience applications to cybersecurity. His CCI work will explore human-cyber security vulnerabilities in a lab setting.

Dr. **Viswanath Venkatesh**, Eminent Scholar and Verizon Chair of Business Information Technology, Department of Business Information Technology, Pamplin College of Business, Virginia Tech. Dr. Venkatesh was recruited from the University of Arkansas where he served as Distinguished Professor and Billingsley Chair of Information Systems. He earned his Ph.D. from the University of Minnesota and is widely recognized as one of the most influential scholars in business and economics with over 116,000 Google citations and more than 100 publications. He regularly ranks in the top three information systems researchers in the world and has held the number one ranking for publishing in the top two journals in the field for the past 5, 10 and 20 years. Dr. Venkatesh is best known for his technology adoption and diffusion research which in recent years

has been applied to security, privacy and trust, especially in reference to large data breaches. His CCI work will involve establishment of the Data Breach Research Lab.

Dr. **Peng Gao**, assistant professor, Department of Computer Science, Virginia Tech. Dr. Gao was recruited from the University of California, Berkeley. Previously, he received his Ph.D. in electrical engineering from Princeton University. His research centers on security, privacy, and systems. Dr. Gao's work focuses on creating secure and privacy-preserving systems to solve real-world challenges, especially in the domains of threat protection, threat intelligence, blockchain, trustworthy AI, and privacy-enhancing technologies. His CCI work will further cybersecurity research using techniques such as machine learning, natural language processing, program analysis, and network science.

Dr. **Wenjie Xiong**, assistant professor, Department of Electrical and Computer Engineering, Virginia Tech. Dr. Xiong was recruited from Facebook AI Research (FAIR). Previously, she received her Ph.D. in electrical engineering from Yale University. Her research focuses on leveraging hardware to build secure systems to enhance the security of computer systems as well as identify and mitigate security vulnerabilities that are rooted in hardware design. Dr. Xiong's recent work includes Physically Unclonable Functions (PUFs), cryptographic applications leveraging physical properties of hardware, security verification of processor architectures, and attacks and mitigations of timing channels in caches. Her CCI work will further these efforts to provide secure systems.

Dr. **Mai Abdel-Malek**, postdoctoral associate, Department of Electrical and Computer Engineering, Virginia Tech. Dr. Abdel-Malek was recruited from Florida International University where she received her Ph.D. in electrical and computer engineering. Her research interests include 6G and beyond, networking and security, drone communications and security, millimeter-wave, device-to-device communications, and IoT. Her CCI work will involve UAVs and 5G technology.

Ms. **Stephanie Travis**, director of the Senior Military College Cyber Institute, Intelligent Systems Lab, Hume Center, Virginia Tech. Ms. Travis previously served as a major in the U.S. Air Force with her most recent appointment as US Cyber Command Officer in Charge, Cyber Operations. She received an M.S. in cybersecurity from Johns Hopkins University. Her expertise includes cybersecurity planning and strategy, cybersecurity incident handling, network security architecture, and endpoint security architecture. Her CCI work will further connect students and faculty in CCI SWVA via designing and employing new experiential learning opportunities.

Dr. **Imran Ghani**, associate professor, Department of Computer and Information Sciences, Virginia Military Institute. Dr. Ghani is joining the software team at VMI's DoD Cyber Defense Laboratory. His expertise is secure software engineering. His CCI work will involve the construction of secure IoT cloud to be used for both research and education.

Dr. **Sherif Abdelhamid**, assistant professor, Department of Computer and Information Sciences, Virginia Military Institute. Dr. Abdelhamid is joining the cyberimmersion team at VMI's DoD Cyber Defense Laboratory. His research interests include and evaluating software systems and services that enable students, computer scientists, educators, and domain experts to easily access and interact with various learning resources and perform large-scale data analyses and simulations. His CCI work will apply his background in engineering education to K-16 cybersecurity education innovation.

2.3.6 Central Virginia Node

Dr. **Nibir Kumar Dhar**, will begin employment at VCU in the summer of 2021 and comes to VCU from the Army CCDC C5ISR Center at Night Vision & Electronic Sensors Directorate (NVESD). After earning his B.S at George Mason University, he went on to the University of Maryland to earn both his M.S. and Ph.D. from their respective electrical and computer engineering departments. After decades working in the defense industry, Dr Dhar is now joining the VCU team to bring "a perspective that is grounded on proven record of technology for the nation's warfighters. A holistic approach to a program that creates an ecosystem for learning, R&D, talent management and diversity."

2.4 Research Infrastructure

2.4.1 5G and NextG Testbed

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

Design Principles

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

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

The testbed has components located in the CCI Hub and each of the nodes, as illustrated in Figure 2.11. These components are aligned with verticals that are of particular focus in each node: transportation and manufacturing in the NoVA Node; IoT, smart communities, and medical devices in CVN; ports and warehouses in the CoVA Node; autonomous and unmanned vehicles, additive manufacturing, and the energy grid in the SWVA Node. The testbed component in the CCI Hub provides a full-stack 5G core and radio access network, including commercial-grade and experimental SDR equipment and open source software; it is accessible remotely by all CCI researchers.

Testbed Architecture

The testbed has been built to host research and development from physical to application layers and aligned with a variety of verticals. The testbed architecture embraces softwarization of network functions that are independent of hardware and emerging standard techniques to manage and orchestrate the network resources. The testbed provides a secure and reliable infrastructure and architecture for Research and Development (R&D) in 5G and NextG networks. To this end, it is critical for the testbed to have an architecture that is open and interoperable, including universally-accessible Radio Access Network (RAN) software running on general purpose processors and flexible and interoperable wireless network management and orchestration. The architecture is depicted in Figure 2.12.

In FY21, CCI joined the O-RAN Alliance as a contributing member, giving CCI access to the latest standards and documents produced by the alliance and providing an opportunity for CCI to help shape the evolution of an open RAN in 5G and beyond.

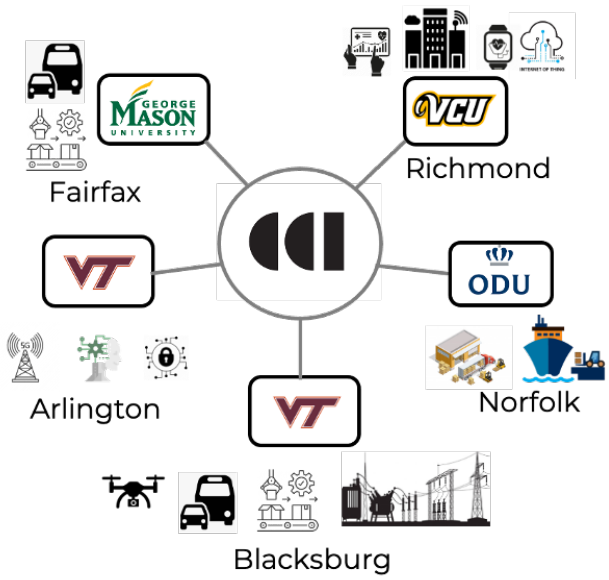


Figure 2.11: CCI 5G and Next G testbed alignment with key verticals in the Hub and regional Nodes.

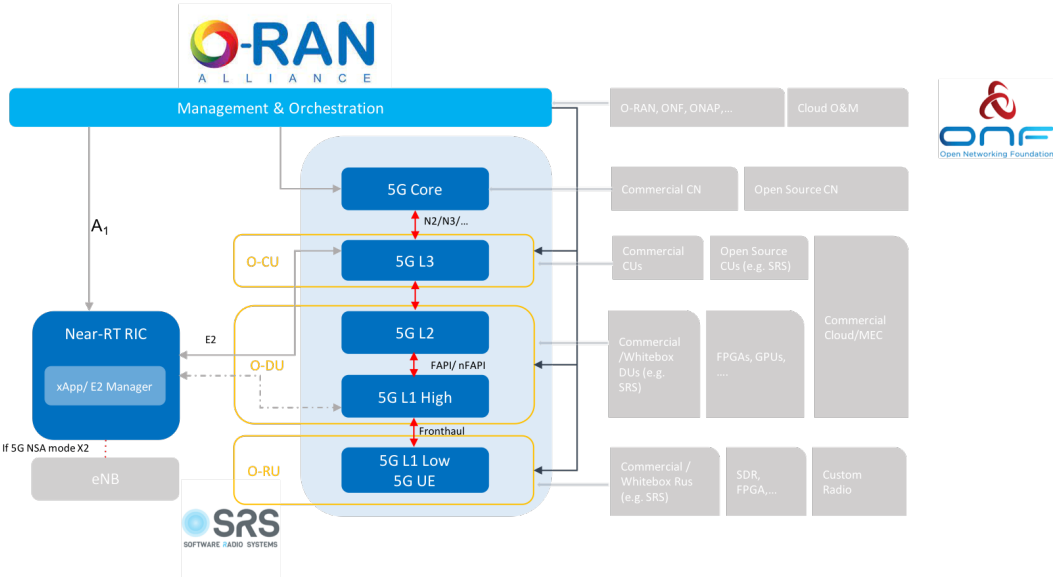


Figure 2.12: CCI 5G and Next G testbed architecture.

Testbed Components in the CCI Hub

The testbed in the hub comprises test and measurement equipment, a sandbox with SDR equipment, and a 5G NSA portable node, all of which are housed in VT facilities in Arlington. CCI currently has an end-to-end 5G NSA solution operational, based on the 3GPP Release 15 standards for 5G. The components of the solution are depicted in Figure 2.13.

The sandbox includes the following SDR platforms: 3 Universal Software Radio Peripherals (USRPs) N310; 6 USRPs X310; 6 USRPs B210; 5 USRP B205-mini. Four USRPs are equipped with Global Positioning System (GPS) and UBX-160 daughterboards. Also included in the sandbox are: 4 Intel NUC with Graphics Processing Units (GPUs); a signal generator; spectrum analyzers; 2 iphone 12 pro; 2 Google Pixel 5; 1 Samsung S20; 1 Huawei P40 (all smartphones unlocked); 20 programmable Subscriber Identity Module (SIM) cards; and a couple of Dell servers.

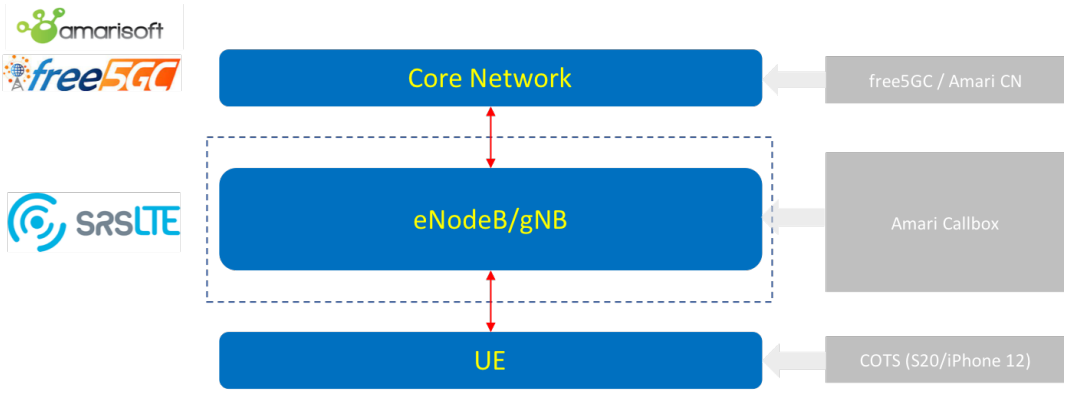


Figure 2.13: CCI 5G Non-Standalone (NSA) solution.

The 5G NSA portable node is composed of 5G core (both Amari Callbox and free5GC cores are supported), eNodeB (Amari Callbox and srsLTE), and gNodeB (Amari Callbox). The User Equipments (UEs) are the same available in the sandbox described in the previous paragraph. To connect to the eNodeB/gNodeB we also have: 1 pair of Omni antenna 600-02 (frequency bands: 3300 MHz — 3800 MHz; radiated power: 23 dBm; Effective Isotropic Radiated Power (EIRP): 30.7 dBm; mean/peak Gain: 2/6.2 dB; frequency tolerance: 5 MHz); and 1 pair of directional antennas XPOL-2-5G (frequency bands: 3300 MHz – 3800 MHz, radiated power: 23dBm, EIRP: 35.5 dBm, mean/peak gain: 9/11 dB, frequency tolerance: 5 MHz).

Some of the equipment in the 5G and Next Generation testbed in the CCI Hub in Arlington is shown in Figure 2.14

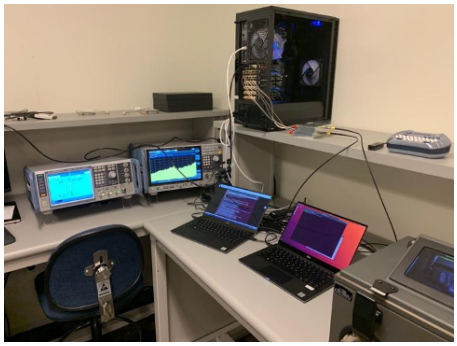
The CCI 5G Testbed supports profiles that can be instantiated and integrated to each experiment. A profile encapsulates the key software needed to run the experiments. Basically, the profile is represented by a Virtual Machine (VM) that has been configured with specific properties to support the software, such as the amount of memory, number of cores, specific otemperating sys, etc. The primary profiles available for instantiation include: srsLTE (eNodeB and Evolved Packet Core (EPC)), O-RAN (Service Management and Orchestration (SMO) and RAN Intelligent Controller (RIC)), Open Source Management and Network Orchestration (MANO) and OpenAirInterface (eNodeB and EPC).

Testbed Components in the CCI Northern Virginia Node

The 5G and Next Generation testbed in the CCI NoVA Node has unique capabilities to support experiments with vehicle connectivity and autonomy. The Cellular Vehicle-to-everything (CV2X) research infrastructure enables both direct communication between a vehicle and the roadside infrastructure and network-based communication between vehicles. The testbed is housed in Mason's recently opened facilities in Arlington, as part of the CCI Living Innovation Lab (Figure 1.7).

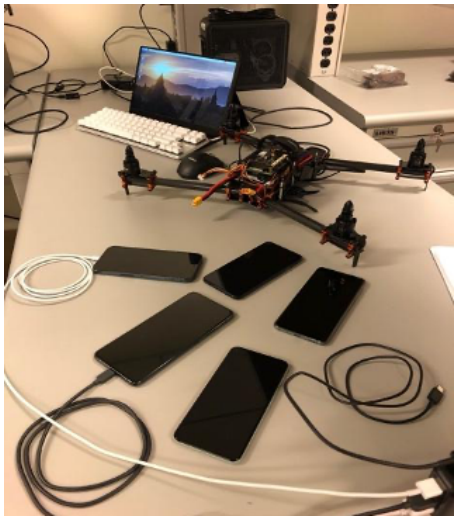
Assets in this testbed at Mason include a Toyota Corolla, a Toyota Prius, and a Honda Accord that can be used for research and innovation in autonomous vehicles (Figure 2.15). The testbed also includes a functional intelligent traffic signal box (Figure 2.16), four (green/red/yellow) signal lights, 15 USRP radios, three small radio chambers and one large radio chamber, three Lidar (916 scan, 24 scan, and 32 scan), one radar, two integrated infrared-color cameras (one of which with pan/tilt functionality), two stereo cameras, three driver simulation (racing) seats and driving gear, and three battery modules to power equipment in the vehicles. A battery test box (Figure 2.17) can be used to test cyber attacks on the battery controllers that may result in the explosion of a multi-cell battery.

Additionally, an Amtrol sorting machine with sensors, with four robots to load and unload the machine, support cyber-manufacturing research in the testbed.



(a) RF enclosure, spectrum analyzer, signal generator, and other 5G test equipment.

(b) USRPs with srsRAN software act as 5G UEs.



(c) 5G end devices: smartphones and drone.

(d) Several models of USRP are used in the testbed.

Figure 2.14: Equipment in the CCI 5G and Next Generation testbed.

Figure 2.15: The testbed at Mason supports research and innovation in cybersecurity in autonomous vehicles.

Testbed Components in the CCI Central Virginia Node

The CCI testbed in CVN provides unique capabilities in experimenting with medical device and smart city connectivity.

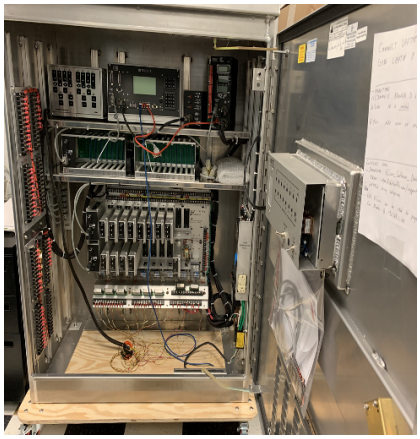


Figure 2.16: Intelligent signal box at the CCI testbed at Mason.

Figure 2.17: Battery test box.

The Medical Device Security Lab is one of the CCI labs under construction in VCU's College of Engineering. The purpose of this lab is to perform research that adds value to the security of operational technology as it applies to the healthcare industry, both in commercial/inpatient environments as well as home healthcare. As hospitals and home healthcare environments are an integral part of every community in the developed world, it becomes advantageous to explore how this operational technology impacts the larger community and how it could be integrated with smart city technologies in a productive fashion. It is also important to investigate how to mitigate risk associated with the increased threat profile that comes with doing so.

The Medical Device Security lab has three focal points in working to improve security in commercial and home healthcare environments: offensive security and pen testing; Field Programmable Gate Array (FPGA)-based secure by design systems; and secure IoT and sensing applications. Patient health data located on servers that work with these medical devices may be a component of this laboratory, but it is not the focus as that is already a well-researched topic. Communication between device and server, on the other hand, will be a focus. The network architecture for the lab is depicted in Figure 2.18.

The CCI CVN is also in the process of deploying a Smart City lab. All digital network communication

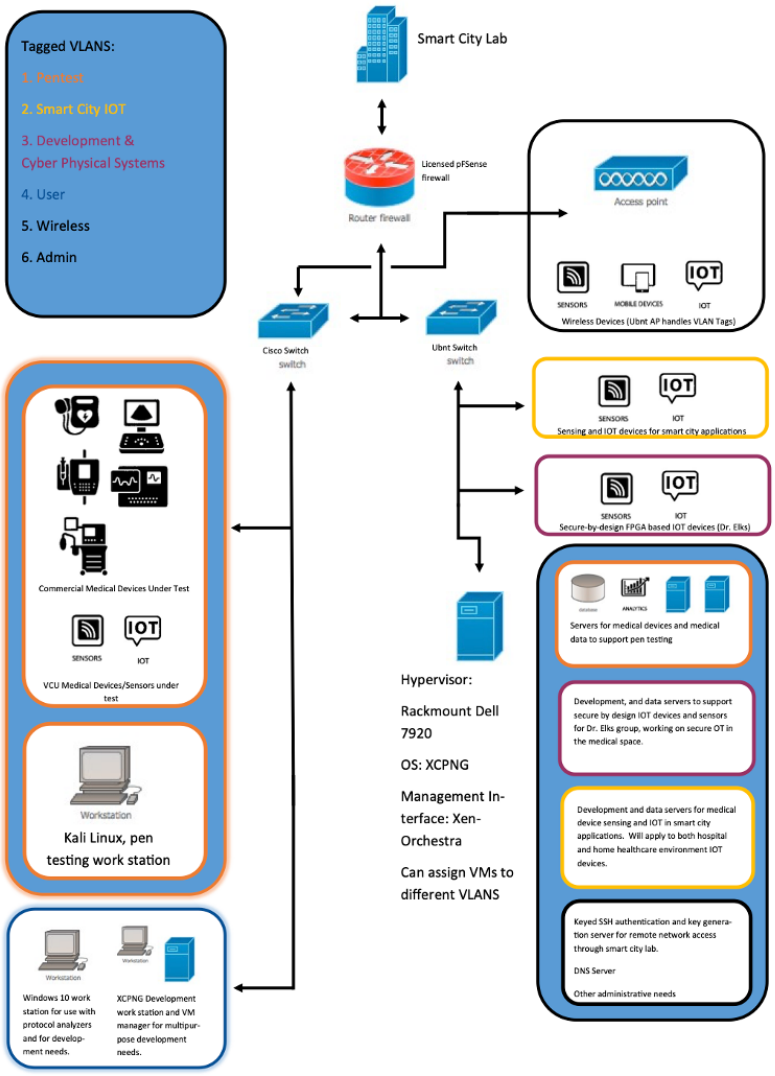


Figure 2.18: Architecture of the Medical Device Security lab at VCU.

between the Smart City lab and the Medical Device Security lab will occur through the Medical Device Security Lab firewall using RSA-4096 public/private key authentication. Inbound and outbound connections between the labs will only be allowed to and from the dedicated Smart City IoT Virtual Local Area Network (VLAN). This is to ensure the safety of both the Smart City and Medical Device Security labs and the integrity of the pen testing and development environments within the Medical Device Security lab.

Testbed Components in the CCI Coastal Virginia Node

The testbed components in the CCI CoVA Node are used to investigate 5G and Next Generation connectivity for ports and warehouses. The CoVA testbed site at ODU focuses on mmWave communications in the 28 GHz band. Equipment currently available in the testbed includes an Agilent N934C spectrum analyzer, a Cisco Catalyst 2690 Gigabit Ethernet switch, a Cisco 1921 router, and a Cisco ASA 5506 integrated security appliance. The testbed will be augmented with commercial mmWave network equipment currently being

tested in the CCI Hub.

Testbed Components in the CCI Southwest Virginia Node

The CCI testbed leverages existing research facilities in Southwest Virginia. These include a drone park operated by MAAP [1] and the smart road operated by VTTI [2], both at VT. The drone park is a netted area (dimensions 300'L x 120'W x 85'H) in the VT Blacksburg campus that supports experimentation with UAVs. In FY21, CCI has conducted, in partnership with MITRE, experiments in drone connectivity to 5G using these facilities. The drone park is depicted in Figure 2.19. The Smart Road, also located in VT's campus in Blacksburg, encompasses a 2.2-mile stretch of highway and rural roads that can be used for experimentation with vehicular connectivity in 5G and Next Generation networks, under a variety of weather conditions (rain, snow, and fog). It is depicted in Figure 2.20.

Figure 2.19: Aerial views of VT's Drone Park, operated by MAAP.

Figure 2.20: Views of VT's smart road, operated by VTTI.

Another unique asset for the testbed now available in Southwest Virginia is a Citizens Broadband Radio Service (CBRS) spectrum license obtained by VT in FY21. This includes eight 10 MHz blocks of CBRS Priority Access License (PAL) in Montgomery and Craig counties. Few academic institutions in the US hold spectrum licenses, and this provides us a unique opportunity to experiment with spectrum sharing in the 3.5 GHz frequency bands, of relevance to both civilian and military deployments of 5G and beyond.

2.4.2 AI Assurance Testbed

The CCI AI Testbed provides a Platform as a Service (PaaS) to facilitate AI Assurance research. The AI testbed is accessible to CCI researchers across academia, industry and government. As a PaaS, CCI currently provides the networks, servers, storage, Operating System (OS), middleware, database and other services to enable AI research. Participant activities on the testbed may include data transformations/wrangling, feature engineering, algorithm development, machine learning model training, and model evaluation. The architecture of the testbed is depicted in Figure 2.21.

[1] MAAP Drone Park website.
[2] VTTI smart roads website.

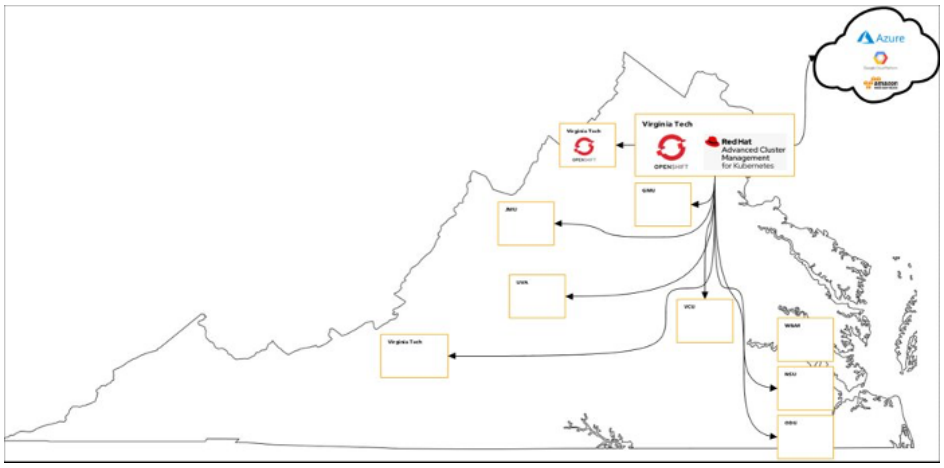


Figure 2.21: AI Assurance testbed architecture.

The CCI AI Testbed currently provides or plans to provide solutions for: 1) an AI Marketplace, a one-stop-shop for access to the testbed's offerings, including datasets, pre-trained models, APIs, libraries, cluster, etc.; 2) a Researcher Social Network, tools to enable researchers to connect about common research interests and collaboration opportunities; 3) Experiential Learning Modules, step-by-step educational material for how to perform AI research for different domains, applications, and methods; and 4) Integration with CCI's 5G Testbed, with the ability to leverage the capabilities of both testbeds to perform research at the intersection of 5G and AI.

The current hardware consists of 1 X NVIDIA DGX-2, 2 X NVIDIA A100s, and 200 TB of IBM General Parallel File System storage. This hardware provides over 288 CPU cores, 6 TB of system memory, 32 GPUs, and 1,792 GB of GPU memory (16 X 80 GB GPUs, and 16 X 32 GB GPU). All hardware is networked with 100G fabric, with the GPU machines featuring fully connected 100G HDR Infiniband. It is staffed by a team of a hardware engineers, a systems administrator, two developers, and a testbed director.

The platform utilizes OpenShift Container Platform for Kubernetes container orchestration, RedHat Enterprise Linux as the underlying operating system, and a suite of industry standard configuration and management software. The result is a highly configurable system where new capabilities can be rapidly deployed – often at the push of a button – to support expanding research needs.

Users can interact with the systems at multiple levels of abstraction. Jupyter notebooks provide a straightforward user interface for scientists and engineers to interact with the system. Datasets on the testbed are stored in an object-storage based data repository. Public datasets in the data repository are cataloged in a meta-data repository that facilitates discovery of datasets for AI experimentation and model development. Testbed documentation, including guides and tutorials, are provided to educate users on how to best leverage the testbed for AI research including, how to develop AI model development pipelines/experiments and leverage GPU accelerated training. An online community within CCI participating institutions has been established that includes a wiki along with a searchable question-answer forum to support accelerated responses to inquiries.

Chapter 3

CCI Workforce Development

This chapter summarizes the main achievements in FY21 for the CCI workforce development mission line.

3.1 Results of Entrepreneurship and Workforce Programming

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

3.1.1 Experiential Learning Program in FY20

The 2020 Experiential Learning call for proposals elicited 26 submissions, with six successful proposals totalling $683,000 awarded in grants. CCI researchers were eligible to respond to this call, and proposals were selected by the Leadership Council based on recommendations by a peer review group. The percentage of the funding for projects in each CCI Node is shown in Figure 3.1.

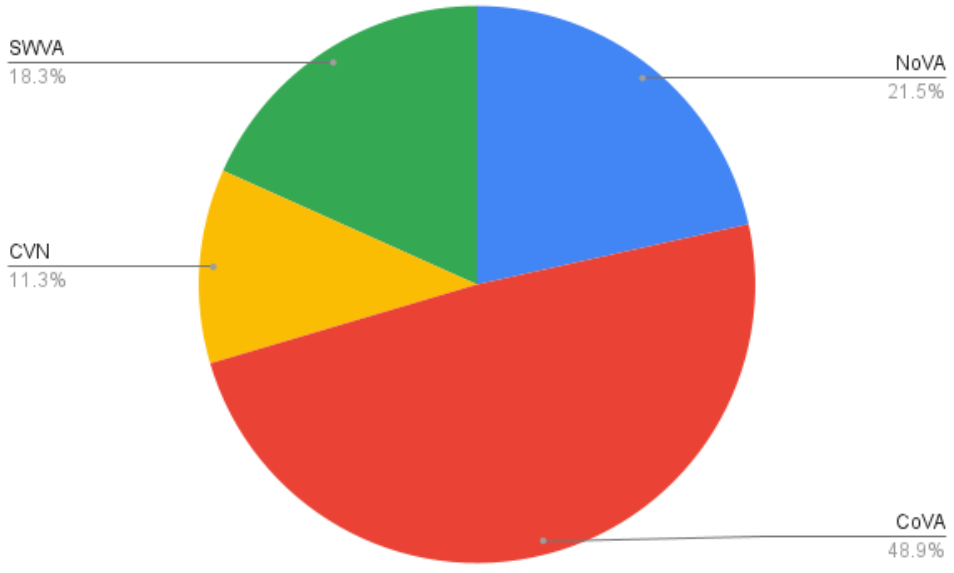


Figure 3.1: Funding percentage by Node for the FY20 Experiential Learning program.

The projects funded by this program are summarized below.

- **AISLE: an AI-Security Living Lab Experience**: Nektaria Tryfona, Ph.D..; Mason; $62,000. This project developed multidisciplinary experiential learning activities, namely an AI-Security Living Lab Experience (AISLE), at the intersection of cybersecurity, privacy, data science and AI for Mason, James Madison University (JMU) and high school students in collaboration with industry partners. These activities contributed to capacity building for a strong multidisciplinary cybersecurity workforce. This project included two cohort training weeks, one held on four consecutive weekends in February 2021 and one week of training in August (these were virtual due to the COVID-19 pandemic). Cohort one comprised five students with one graduate student as team lead, three undergraduate students and one high school student. The entire cohort female to male ratio was 9:10. Student teams directly engaged with industry members and worked together through peer-based and project-based learning methodologies to solve problems submitted by the industry partners. Students reported high satisfaction with the learning and format. Cohort two kicked off on August 9, 2021.

- **Cyber Startups: Pilot Program for Novel Experiential Learning**: Gisele Stoltz; Mason; $85,000. This pilot program provided students with experiential learning opportunities focusing on an important, and growing, part of the Virginia cybersecurity ecosystem, startups. These organizations need young cybersecurity talent and are often impacted in their hiring of workers because of limited financing and the high cost of cybersecurity labor. Through their participation in this program, the students not only continued to develop further their technical skills with real world experience, but also gain valuable soft skills, such as critical thinking and communication, that are essential in the dynamic startup environment. These young professionals were also encouraged to be part of the cybersecurity innovation ecosystem during their college education and upon graduation, also increasing the chances of their retention in the Virginia region. 147 Mason students applied for internships for 15 available positions, and Marymount University (MU) received 28 applications for 10 available positions. Mason down-selected to 65 candidates to present to the host companies. Out of the 15 Mason students that were ultimately selected, six were female; minorities accounted for 80 percent of the group; 10 Mason students received either a job offer or a summer internship offer from their hosts, indicating a high degree of satisfaction for the quality of the interns. At MU, female students accounted for 73 percent of the interns and 82 percent were under-represented minorities. Of the 10 host companies that Mason recruited, one was founded by a female entrepreneur and six were founded by minorities. Of the eight MU companies, three were women and four were minority started and owned, again highlighting the diversity of the cybersecurity field, helping to underscore to students that minorities are successful in creating tech startups in the region.

- **Data Poisoning & Satellite Reconnaissance: Bridging Application and Education**: Dan Runfola, Ph.D..; W&M; $125,000. Undergraduate students worked closely with already-identified external practitioners from the intelligence community and industry, building on already existing models of student-practitioner engagement. Among other key results, the key intellectual advance from this program is the first known application of data poisoning for convolutional neural networks designed to estimate information from satellite imagery, using road quality and condition as a case study. Additionally, 12 of 16 students indicating interest in an internship because of this program successfully obtained one, and even one full time job offer was received. Internship locations included Fiserv (Data Loss Prevention), CarMax (Data Analytics), Fidelity Investments (Software Engineer Intern), and Heron Systems (R&D).

- **Drone Racing Competition - Learning, Defending, and Attacking**: Jon Black, Ph.D..; VT; $125,000. 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 commonwealth to compete in "battle" drone racing competitions. The project serves as a pilot for a scalable drone-based AI competition in which the drones learn, defend, and are even allowed to attack their opponents to get to the finish line. While the COVID-19 pandemic delayed the project significantly, the team was able to produce trailed neural nets, a flying drone, and developed a simulation environment. The team was granted a no-cost extension in order to complete recruitment and competition.

- **Training in the Integration of Cyber-Physical Systems and Security**: John A. Stankovic,PhD.;

UVA; $77,000. The main objectives for this Cyber Physical System (CPS) experiential learning program are: 1. Package three newly developed UVA CPS classes for dissemination to other CCI colleges and universities; 2. Develop and package hands-on labs for each of these classes; 3. Identify the first group of schools to use one of more of the class and lab materials and support transferring the materials to them; 4. Support undergrad underrepresented minorities as summer interns. The first two cohorts of 51 students comprised 41 PhD students and 10 Masters students from a variety of engineering fields including, but not limited to computer science, electrical engineering, and systems engineering. In May 2021 the first four Cyber-Physical Systems Certificates were approved with one more scheduled for August 2021.

- **Virginia Space Grant Consortium Experiential Learning Through the Commonwealth STEM Industry Internship Program (CSIIP)**: Mary Sandy; ODU; $209,000. The Virginia Space Grant Consortium (VSGC), a CoVA CCI team member, is using its highly successful Commonwealth STEM Industry Internship Program (CSIIP.org) as a venue for facilitating state-wide experiential learning opportunities for Virginia STEM students pursuing CCI-defined majors in support of CCI's aim to create a commonwealth-wide ecosystem of excellence in Cyber Physical System (CPS) at the intersection of cybersecurity, autonomous systems and data. This partnership is serving as an innovative pilot program allowing for expansion to serve the entire commonwealth and support CCI's goal of closing the workforce gap in cybersecurity in the commonwealth. To date, the CSIIP has placed 19 students at cybersecurity internships because of this grant, and has added 11 new companies to their portfolio. Students come from across the commonwealth, including four community colleges.

Spotlight: Data poisoning, deep learning, and satellite imagery

One of the programs funded by the 2020 Experiential Learning Call for Proposals that had an incredibly successful year is the Data Poisoning and Satellite Reconnaissance Program, run by Dr. Dan Runfola from W&M. The program recruited heavily among non-traditional students and from across the commonwealth. They received 122 applicants in total and selected 36 students. Of the 36 students, 20 identified as female (61 percent), and 23 identified as a minority (70 percent). The students came from Christopher Newport University (CNU), Richmond University, VCU, Mason, VT, and W&M. The students were offered a paid fellowship opportunity to work directly with practitioners from Silicon Valley (Cloudera) and the intelligence community (National Geospatial-Intelligence Agency (NGA), Central Intelligence Agency (CIA)), and the only skills requirement to participate in the program was an introductory knowledge to Python.

Among other key results, the key intellectual advance from this program is the first known application of data poisoning for convolutional neural networks designed to estimate information from satellite imagery, using road quality and condition as a case study. Additionally, 12 of 16 students indicating interest in an internship because of this program successfully did so, and even one full time job offer was received. Internship locations included Fiserv (Data Loss Prevention), CarMax (Data Analytics), Fidelity Investments (Software Engineer Intern), and Heron Systems (R&D).

3.1.2 Experiential Learning Program in FY21

With the success of the experiential learning program in Fiscal Year 2020 (FY20), we funded a second batch of experiential learning projects in FY21. The 2021 Experiential Learning call for proposals elicited 20 submissions, with seven successful proposals totalling $966,770 awarded in grants. The percentage of the funding for projects in each CCI Node is shown in Figure 3.2.

- **Cyber Risk Management and Analytics: An Interdisciplinary Approach in Experiential Learning**: Chon Abraham, W&M; $150,000. Cyber risk management is a critical component of a meaningful cyber strategy. This project is enabling experiential learning for students regarding how cyber risk is defined in organizations, methods for collecting threat intelligence, legal and compliance constraints, and quantifying relevant cyber data to analyze options for defense and mitigation. The interdisciplinary approach taken seeks to expose students to business, legal, and technical aspects of cyber risk management by working on real-world projects for companies providing data analytics-driven cyber risk management services. We are particularly interested in businesses assisting small

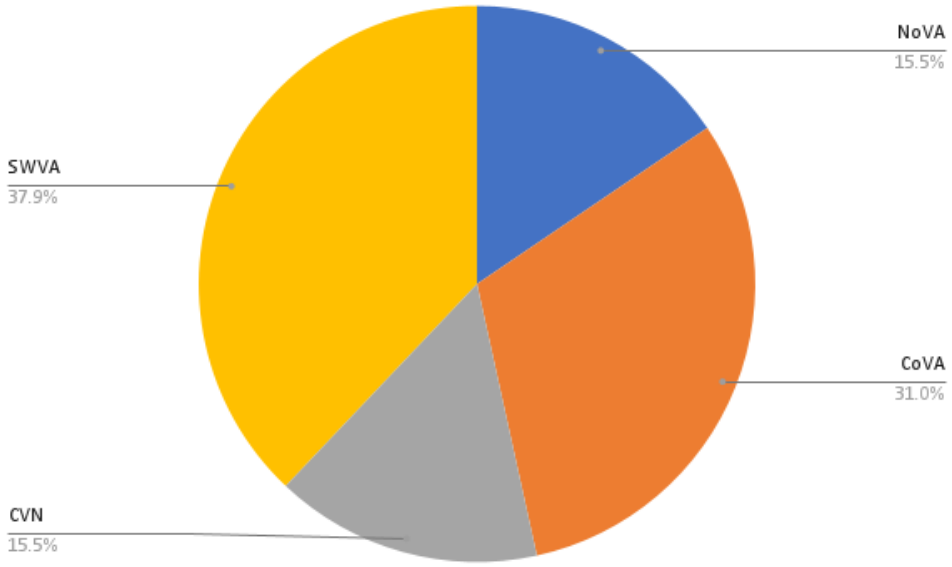


Figure 3.2: Funding percentage by Node for the FY21 Experiential Learning program.

and medium enterprises in the Southeast region of the commonwealth, which include greatly targeted sectors such as the maritime and defense industrial base. The goals of the projects are: (i) at the micro level, to expose students to these practical challenges, and equip them with valuable skill sets, and (ii) at the macro level, to contribute to the creation of competent workforce and to the cybersecurity maturity of the business ecosystem in the Commonwealth of Virginia.

- **Cybersecurity Monitoring and Assurance Training Program for Safe and Secure Port Operations**: Sachin Shetty, ODU; $150,000. The goal of this project is to cooperate with the Port of Virginia in the development of innovative experiential learning modules that aid in the implementation of cyber security monitoring and assurance systems to protect and safeguard port operations from cyber-security threats. The learning modules will provide insights into planning and configuration of cyber-security oversight systems that will monitor threats to port systems, assess the cyber risk, and facilitate appropriate mitigation responses. The training program will benefit engineering and computer science students enrolled in ODU, UVA, Longwood University, and Virginia State University (VSU). The trained students will have the opportunity to interact with Port of Virginia personnel to gain operational knowledge that will increase their understanding of the cyber risks and help the Port with providing inputs to the planning and configuration of its cyber security monitoring and response capabilities.

- **Cyber Startups: Expansion of Successful Pilot Program for Novel Experiential Learning**: Giselle Stoltz, Mason; $150,000. Recognizing that startups and small businesses are an important and growing part of the Virginia cybersecurity ecosystem, this project aims to achieve the following two objectives: to provide students in cybersecurity degree programs who are from diverse backgrounds with relevant, hands-on experiential learning opportunities; and to provide cybersecurity startups and Small and Medium Enterprises (SMEs) with the talent they need to scale their businesses. This project seeks to diversify the talent pipeline to cybersecurity jobs and build a resilient and diverse cybersecurity innovation ecosystem that will help Northern Virginia thrive post-pandemic.

- **Curating industry partnerships through experiential learning for workforce development in cyberbiosecurity**: Tiffany Drape, VT; $114,510. Students enrolled in colleges of agriculture and life sciences have limited opportunities to integrate the areas of data management and security into their education. This project encompasses the development, approval, and delivery of an experiential learning focused course that integrates these areas with early-career undergraduates interested in

learning about and pursuing a career in cyberbiosecurity. We will combine students in data science and food and agriculture (F+A) majors with F+A industry partnerships as the course focus. Course topics include evaluation of technology systems, agile methodology, and developing feasible and affordable holistic solutions. Students will develop technical and professional skills, while connecting to industry partners. Students can apply for 10-week internships with industry partners that would be completed during the summer. The course culminates with a three-day tour to the industry partners' businesses to learn about the industry and provide face-to-face time with students. The proposed work builds on the goals of CCI and VT's College of Agriculture and Life Sciences Center for Advanced Innovation in Agriculture to grow a workforce cyberbiosecurity. This project will disseminate all content via open educational resources on multiple platforms so higher education institutions can replicate and implement their own learning experience.

- **Experiential Learning Through Conducting Data-driven Adversarial Attack Creation and Control in Connected Autonomous Vehicle Cyber-Physical Systems**: Haying Shen, UVA; $150,000. As Connected Autonomous Vehicles (CAVs) become a part of the landscape of Transportation Cyber Physical Systems (TCPSs), the demand for CAV security solutions has been growing. This project will study how to create an adversarial attack to the deep learning models used in vehicles in near real-time and how to further detect an adversarial attack. Mitigation approaches developed for previously proposed adversarial attacks cannot be directly adopted in the CAV scenarios due to two challenges: real-time and low noticeability requirements. The Principal Investigators (PIs)' collaboration with industries will lead to commercialization, adoption, and distillation of the project results into real-world products. The developed software prototype will serve the CPS community as a vehicle to conduct further research and development. This project will serve as a key enabler for future TCPSs. Also, because of the pressing needs on such security solutions from the society, there will be many users for the software prototype.

- **Scalable, Systematic, and Holistic Approach to Internship Quality Enhancement**: John Ferris, VT; $102,260. The objective of this project is to integrate existing strengths, identify and address trans-disciplinary needs, aggregate the lessons learned, identify best practices across cybersecurity programs, and implement this continual acquisition of knowledge in a process improvement feedback loop. The deliverables for this project will be a scalable proof-of concept including: a set of student/business assessments from cybersecurity workforce experiences (internships) and corresponding lessons learned and best practices; and a roadmap to scale this project across the commonwealth to enhance students' essential skills to enter the cybersecurity workforce. A collaboration between Radford University and VT will leverage the strengths of both institutions and demonstrate the ability to scale this project across institutions.

- **Virginia Integrative Experiential Workforce for power system communication and cybersecurity (VIEW)**: Ali Mehrizi-Sani, VT; $150,000. The overall goal of this program is to create a sustainable and scalable work-force training program in cybersecurity focusing on electrical power systems. The power system is the largest man-made machine. Its growing dependence on information and communication technology significantly increases vulnerability to cyber attacks, potentially leading to power outages.

3.1.3 Workforce Programs Developed by the CCI Nodes

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

The NoVA Node carried out four workforce initiatives:

- **High School Cybersecurity Internship Program**: The CCI NoVA Node received 110 applications, and selected 20 high school students for internships in cybersecurity companies. The experience included a two-week professional skills training program to prepare the students for the professional work environment.

- **University/College Cybersecurity Entrepreneurship Internship Program**: The CCI NoVA Node received 140 applications for 26 internships (15 Mason students received stipends and 11 Marymount students received academic credit) with cybersecurity "start-up" companies. Eleven Mason and three MU students obtained job or internship offers from their respective host companies at the conclusion of their internships, essentially hired into newly created jobs. Out of the 15 Mason students, six were female and minorities accounted for 80 percent of the cohort. Out of the 11 MU students, seven were female and minorities accounted for 73 percent of the cohort.

- **AI-Security Living Lab Experience (AISLE)**: A mix of college/university and high school students worked in teams to undergo training in Python, data, networking, crypto, presentation skills and then applied those skills to real world cybersecurity challenges with deliverables. Of the 60 applicants, 23 students were accepted, including six high school students and 17 students from George Mason University and James Madison University. An additional 21 students will move through the AISLE program in August 2021.

- **High School Summer Cyber AI Camp**: A total of 48 high school students applied for 24 slots to participate in a week-long study and hands-on experience with the role of AI in cybersecurity. Of the 24 participating students, 8 were females and 17 of the 24-student cohort were minorities.

CoVA CCI is supporting several programs in innovation, workforce development, and student experiential learning. These include the INNOVATE Cyber Challenge, a graduate student experiential learning program, and a cybersecurity internship program.

- **INNOVATE Cyber Challenge**: The INNOVATE Cyber Challenge program takes a cohort of 20 students from across the region and groups them into four teams. Each team is assigned a cybersecurity problem/challenge. They use design thinking to come up with unique solutions for this problem. A total of 40 students have participated in the program - 20 in the Spring 2020 semester and 20 in the Fall 2020 semester.

- **Graduate student experiential learning program**: During the Spring 2021 semester, CoVA CCI supported nine graduate assistants with experiential learning opportunities in various CoVA CCI partner institutions. One Graduate Research Assistant (GRA) was provided to Paul D. Camp Community College, and one GRA is assisting Christopher Newport University, to support cybersecurity classes and students. Two GRAs supported the Experiential Learning and Academic Support committees with identifying all cybersecurity related classes being offered at CoVA CCI partner institutions. Five GRAs are supporting local cybersecurity businesses on current projects within these companies, including Peregrine Technical Solutions (two GRAs), CivilianCyber (two GRAs), and MI Technical Solutions (one GRA). The students are coming out of Norfolk State University, Old Dominion University, and the College of William and Mary.

- **COVA CCI Cybersecurity Internship Program**: CoVA CCI is partnering with the Virginia Space Grant Consortium (VSGC) to manage the CoVA CCI Cybersecurity Internship Program using their Commonwealth STEM Industry Program (CSIIP). VSGC will leverage CSIIP to build and improve on the relationships with employers across the Commonwealth to develop internship and experiential learning opportunities. To date, sixteen students have been placed within the region. The intern placed with Peregrine Technical Solutions, Sam Grant, is the nation's first Department of Labor Youth Registered Apprentice. He was also a keynote speaker at the 2020 NICE K-12 Education Conference.

  The SWVA Node funded 12 workforce programs:

- **Novel Schemes for Ensuring Trustworthiness and Reliability of Crowd-sourced Frequency Occupancy Data in Spectrum Sharing Systems**: One of the students involved in the project developed a demonstration simulation and an interactive, game-like simulation exercise in which students act as human spectrum access systems and seek to approve and deny requests for access to frequencies in a way that uses the radio frequency spectrum efficiently while guaranteeing access of high-priority (primary) users of the spectrum. This work is being expanded to develop interactive modules for use in university- and college-credit courses and asynchronous short courses (to be offered by VT Continuing

and Professional Education). The courses are being developed as part of a project supported by the Office of Naval Research (ONR) STEM Education and Workforce program and will be made available for a fee to U.S. Navy employees and the general public after the ONR project concludes.

- **Networking optimization in rural agriculture testbeds**: Three undergraduate students were funded in the Summer semester of 2021 to conduct undergraduate research and related activities, including training in drone use, data entry, data analyses related to wheat, barley, and soybean row crops. This research is conducted at the Eastern Virginia Agricultural Research and Extension Center (AREC).

- **Supporting Multi-Scale Latency Services in 5G Communications**: This project resulted in one summer intern at Nvidia Corp. in 2020 and one summer intern in 2021. One of the graduate students, Yan Huang, joined Nvidia Corp. in December 2020 following his summer internship at the company. Another graduate student, Yongce Chen, will join Nvidia Corp. in September 2021 following his summer internship at the same company.

- **Polar Coding and its use in 5G**: Students trained on topics associated with this project obtained Summer 2021 internships at DoD and Fermilab.

- **CyberTeams VIPs**: Five of the participants in this program took internships with cybersecurity companies in summer 2021. From the Use & Abuse team, one student started at Deloitte, one at MITRE, and one at Geico, all in cybersecurity or cyber policy. Three additional students now work for the U.S. government.

- **Algorithms for Supersingular Elliptic Curves**: One BS/MS student trained in this project. He was recently offered support as a PhD student at UVA.

- **Evaluation of Lattice-Based Candidates in the NIST Post-Cryptography Standardization Process in Terms of Security and Performance in Hardware**: William Mahaney was recruited as a graduate student (masters) at VT. He is currently working as a research assistant over the summer, and in the fall will be a graduate research assistant. He will be trained in cryptanalysis of post-quantum cryptosystems and algorithmic number theory and intends to pursue a Ph.D. at Mason. Ph.D. students are trained to become experts in hardware and software/hardware implementations of post-quantum cryptography. One of them, Luke P. Beckwith, already works part-time as a computer engineer in the company PQSecure. Two other Ph.D. students, Viet B. Dang and Duc T. Nguyen, have secured summer 2021 internships related to their Ph.D. research at Qualcomm and General Electric, respectively.

- **Support for the Student Training-Engagement Program (STEP) Enhancing Virginia's Cybersecurity Workforce Pipeline**: Candidates selected for the program associated with this project have been placed in internships or apprenticeships. Five of the ten students are participating in an apprenticship program, and five were placed in internships.

- **Cyber Range Accessibility Program**: The Virginia Cyber Range supports hands-on cybersecurity education in Virginia public high schools and colleges. CCI funds were utilized to support further accessibility of Cyber Range materials. We are thrilled to have an average of 8,000 students and teachers using the cyber range each semester, helping to build a pipeline of cybersecurity expertise from high school, to college, and into the workforce. With almost 4,000 cumulative enrollments, the U.S. Cyber Range is similarly supporting high school and college cybersecurity education in 41 states.

- **Wise Minds at Work**: This program has provided virtual internships and training for four UVA Wise undergraduates to date.

- **System-wide Measurement of Defense-in-depth Readiness of Medical CPS Devices**: The project provided graduate student training opportunities at VT, preparing them for future research collaborations. In the Fall 2020 semester, the project also created an independent study opportunity for a domestic undergraduate student on investigating existing defense-in-depth practices in U.S. government.

- **Probabilistic and Evidence-based Insider Threat Reasoning and Detection for Critical Infrastructures**: The project provided training opportunities for several graduate students. In the Fall 2020 semester at VT, the project also created valuable independent study opportunities for two domestic undergraduate students (including a female Hispanic student) on important real-world data breaches, including Target and Equifax data breaches.

3.2 Internship Programs

3.2.1 Internship Programs Funded by CCI

As a part of the 2020 CCI Experiential Learning Call for Proposals, CCI funded The Virginia Space Grant Consortium (VSGC), a Coastal Virginia Commonwealth Cyber Initiative (COVA CCI) team member to utilize its highly successful Commonwealth STEM Industry Internship Program (CSIIP.org) as a venue for facilitating statewide experiential learning opportunities for Virginia STEM students pursuing CCI-defined majors. The CSIIP hosts a portal for students to learn about available internships in cybersecurity throughout Virginia. It is a one-stop shop for students and parents to learn about opportunities and how to apply. This partnership would serve as an innovative pilot program allowing for expansion to serve the entire commonwealth and support CCI Goal Two of closing the workforce gap in cybersecurity in the commonwealth.

Another funded project out of the 2020 CCI Experiential Learning Call for Proposals was "Cyber Startups: Pilot Program for Novel Experiential Learning". The objective of this program is to conduct a pilot program that facilitates students experiential learning opportunities focusing on an important, and growing, part of the Virginia cybersecurity ecosystem, startups. These organizations need young cybersecurity talent and are often impacted in their hiring of workers because of limited startup financing and the high cost of cybersecurity labor. Through their participation in this program, the students will not only continue to develop their technical skills with real world experience, but also gain valuable soft skills, such as critical thinking and communication, that are essential in the dynamic startup environment. These young professionals are also encouraged to be part of the cybersecurity innovation ecosystem during their college education and upon graduating, also increasing the chances of their retention in Virginia.

Due to the successful pilot year of Cyberstartups, the program was funded again in the 2021 CCI Experiential Learning Call for Proposals. Recognizing that startups and small businesses are an important and growing part of the Virginia cybersecurity ecosystem, the second year of the proposed project aims to achieve the following two objectives: to provide students in cybersecurity degree programs who are from diverse backgrounds with relevant, hands-on experiential learning opportunities; and to provide cybersecurity startups and subject matter experts (SMEs) with the talent they need to scale their businesses. This project seeks to diversify the talent pipeline to cybersecurity jobs and build a resilient and diverse cybersecurity innovation ecosystem that will help Northern Virginia thrive post-pandemic.

3.2.2 CCI Internship Fairs

On January 27, 2021, the Commonwealth Cyber Initiative hosted a virtual internship fair connecting students with traditional and alternative paths to internship opportunities in Virginia within industry, government, academia, and startup programs. The internship fair consisted of a panel discussion and breakout rooms.

Through a panel discussion moderated by CCI, program leaders highlighted their organization or institutions' open opportunities, shared how to apply and expectations, described what internship opportunities looked like during the pandemic, and more. The program leaders shared more information in their assigned breakout rooms where students could visit and learn more.

The internship program recruited students within the STEM and cybersecurity field of study but was open to all. The internship fair had 500 plus registered and 250 in attendance.

From the success of CCI's first internship fair, CCI grew the program into a two-day, bi-annual, virtual internship fair to provide students with more opportunities to connect to traditional and alternative internship paths in Virginia within industry, government, academia, and startup programs. CCI will host the fair on the Brazen Technologies platform that offers students the feel of an in-person event. Both employers and

students have remarked on the convenience of having a virtual event to allow for maximum reach. The fairs will be held October 5 – 6, 2021, and January 2022.

On October 5, CCI will provide a series of panels highlighting program leaders' organizations or institutions' open opportunities, share how to apply and expectations, and answer questions live.

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

With student return to school at the end of August, registration for the Fall internship fair will open on August 30, 2021.

3.3 CCI Cyber Camp

In partnership with Deloitte, CCI developed an immersive cyber camp to enhance students' essential skills to enter the cybersecurity workforce, the Deloitte CCI Cyber Camp. The cyber camp will take place on three consecutive Saturdays, July 31, August 7, and August 14, 2021.

The camp was hosted on the Virginia Cyber Range with Jeopardy-style Capture the Flag (CTF) cybersecurity challenges. The camp targeted undergraduates within Virginia higher education institutes studying cybersecurity or related fields. Prospective campers competed in an online qualifying event, and top performers were extended an invitation to attend the camp.

The camp began with a four-day qualifying event on May 14 – 17, 2021, where students tested their skills in networking, reconnaissance, web security, and cryptography. Three hundred students registered for the qualifier, with 150 students competing. CCI invited 62 students to attend the camp, with 27 alternates.

The invited 62 students attended each Saturday for instruction in the cybersecurity-focused challenge area developed by the challenge creators. Students had the opportunity to network and discuss the challenges with other invited students. Students competed for points in the CTF challenges within network traffic analysis, reverse engineering, cyber analytics, and cryptography created by subject matter experts. In fact, in December 2020 the cryptography challenge creator, David Oranchak, was on a team that cracked the famous unsolved 340-character cryptogram of the Zodiac Killer. The challenges include:

- **Cryptograhy** - David Oranchak, software engineer, computer scientist, cryptographer, SHLD
- **Cyber Analytics** - Laura Freeman, director, Intelligent Systems Lab, Virginia Tech Hume Center
- **Network Traffic Analysis** - Stephanie Travis, director, Senior Military College Cyber Institute, Hume Center for National Security and Technology
- **Reverse Engineering** - Lee Allison, research staff member/cybersecurity analyst, Institute for Defense Analyses
- **Reverse Engineering** - Trampas Howe, adjunct faculty member, Virginia Tech Reverse Engineering

Students also improved their soft skills and received points by participating in mock interviews given by cyber professionals and resume writing workshops hosted by Northern Virginia Community College, University of Virginia, and Virginia Tech.

Given the changing nature of the pandemic, the 2021 Cyber Camp was scheduled to be virtual; future camps will be in-person events.

Chapter 4

CCI Innovation

This chapter summarizes the main achievements in FY21 for the CCI innovation mission line.

4.1 Results of Entrepreneurship and Workforce Programming

4.1.1 The CCI Innovation Committee

The purpose of the CCI Innovation Committee is to advise and provide recommendations to the CCI Leadership Council on programs that will build and maintain the innovation portfolio of CCI. The committee comprises members from across the CCI network, including:

- Mary Lou Bourne, director, Technology Innovation and Economic Development, executive director, James Madison Innovations, Inc.
- Mina Heta, Ph.D., MBA, director, Office of Technology Transfer, Mason
- Travis Hite, program director, Link Lab, UVA
- Jason McDevitt, Ph.D., director, Technology Transfer Office, W&M
- Ivelina Metcheva, Ph.D., MBA, director, Innovation Gateway, VCU
- Mark Mondry, director, LAUNCH, VT
- Jeff Pittges, Ph.D., professor, Radford

4.1.2 The CCI Bridge Funding Call

In June 2020 CCI launched a Bridge Funding Call for Proposals. The purpose for this call was to seek proposals for institutions of higher education cyber technologies to help Virginia university-affiliated, pre-product, cybersecurity innovation companies/university projects develop a prototype to attract seed/series-A funding. The objective is to enhance University-affiliated cyber technologies and bridge the gap between pre-seed and seed funding.

Cybersecurity innovations are defined as technologies and processes that protect systems, networks, programs, data, and operations from digital attacks. Aspects of protection can include risk analysis, vulnerability assessment, system protection/mitigation, information security, threat detection/characterization, real-time defense, restoration activities, and end-user education/training. CCI is especially interested in applications across the overlapping areas of cyber-physical systems, autonomous systems, robotic process automation, critical infrastructure, and endpoint security.

Eligibility requirements included: Institution of higher education (IHE) research team – Funds would go to a CCI-affiliated IHE to further develop a technology (by university or college employees and/or students) that: (i) researchers intend to commercialize; and (ii) is covered by a written invention disclosure received by the university's/college's technology transfer office.

Or, Institution of higher education (IHE) and company research team - Funds would go to the lead institution of higher education to further develop a technology in partnership with a company, wherein the company (corporation, or LLC)) must: (i) be headquartered in Virginia with intent to grow the company in Virginia; (ii) have a license/option for the technology with an CCI-affiliated IHE at the time of award; and (iii) be at a pre-product stage.

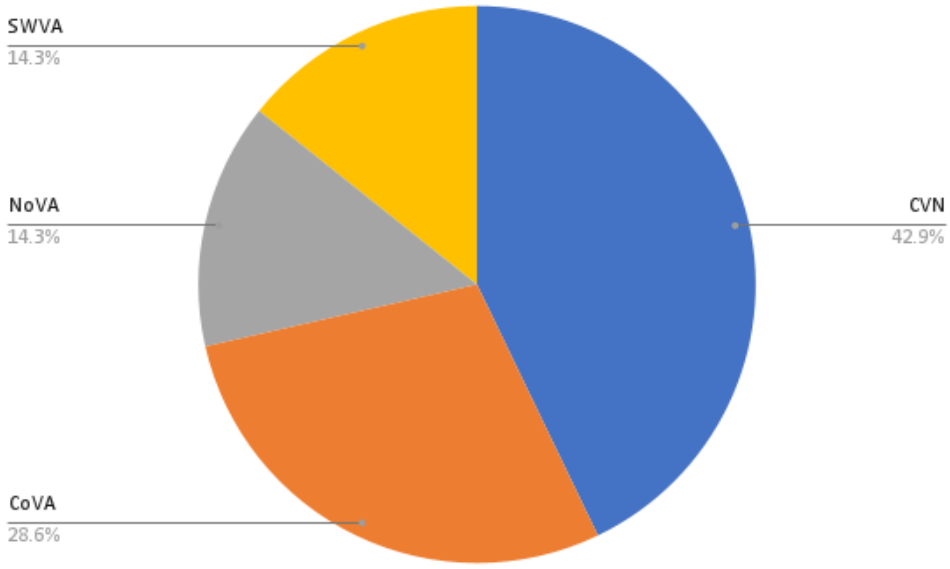


Figure 4.1: 2020 Funding percentage by Node

- **A Minimum Viable Product to Secure IoT Devices through Power Auditing and Privacy Preserved Convolutional Neural Networks**; Gang Zhou (W&M); Chunsheng Xin, Danella Zhao (ODU, ODU); $50,000; IoT devices were known for their weak security protection. They were found to serve as intermediaries of DDoS attacks in 2016. They were also found to serve as attack proxies for multiple cybercrimes, such as clickjacking and spearphishing. Furthermore, Information Stealer attacks could exploit the vulnerabilities of IoT devices to exfiltrate users' private data in the near future. Despite clear intrusion procedures of botnet attacks on IoT devices, it is not easy to characterize whether the threatening intrusion occurred. The main concern is that the network traffic generated on endpoint devices is not significant as malicious behavior at the initial stages. Therefore, there is motivation to address this unmet need.

  The proposed approach is to secure IoT devices via power consumption auditing and deep learning through three steps: modeling an IoT botnet detection classifier based on the power consumption data of IoT devices, building an online botnet classification system in a distributed setting to support heterogeneous IoT devices simultaneously, and designing an Information Stealer Detection System on IoT devices via power auditing. While the first two steps have been finished through a prior COVA CCI project as fundamental science, the scientific discoveries will be embedded and commercialized on the new area of IoT Information Stealer attack detection, i.e. the third step. A Minimum Viable Product (MVP) will be developed. Based on the MVP, the team will create demos and business pitches to engage partners, acquire customers, and seek investments.

- **A Platform for Improving AI Trust in 6G Networks**; Murat Kuzlu (ODU); Ozgur Guler (Thinking Makina, LLC); $50,000; With the rapid development and integration of artificial intelligence (AI) methods in 6G networks, AI algorithms have provided significant advantages for 6G networks in terms of frequency spectrum usage, latency, and security. The key feature of 6G is the integration of AI, i.e., self-learning architecture based on self-supervised algorithms, to improve the performance of

the network for tomorrow's cellular systems. It is also expected that a secure AI-powered structure can protect the 6G network against cyber-attacks. However, AI itself may be attacked or abused as well by model poisoning targeted by attackers, resulting in cybersecurity violations. This project proposes the development of a platform for improving AI trust in 6G networks that allows 6G researchers to evaluate, defend, certify, and verify their 6G AI models and applications against adversarial threats of evasion, poisoning, extraction, and inference. The team will focus on feasibility study of the innovation, including (1) Development of a platform for improving AI trust in 6G networks, (2) Development of novel adversarial sample detection methods, and (3) Increasing the robustness of AI models against adversarial machine learning.

- **A study on authentication usability of biometric-based multi-factor mechanisms**; Emanuela Marasco (Mason); Massimiliano Albanese (Mason); $50,000; Fingerprint-based authentication has been successfully adopted in a wide range of applications, including law enforcement and immigration, due to its numerous advantages over traditional password-based authentication. Despite the usability and accuracy of this technology, some significant concerns still exist, which can potentially hinder its further adoption. For instance, a subject's fingerprint is permanently associated with an individual and, once stolen, cannot be replaced, thus compromising biometric-based authentication. To mitigate this concern, we designed a multi-factor authentication approach that integrates type 1 and type 3 authentication factors into a fingerprint-based personal identification number. To authenticate, a subject is required to present a sequence of fingerprints corresponding to the digits of the PIN, based on a predefined secret mapping between digits and fingers. This result demonstrates how the parallel integration of the two factors considered in this scheme overcomes the limitations of both a PIN mechanism alone as well as an authentication purely based on fingerprints. The team conducted a preliminary vulnerability analysis and demonstrated that it is robust to the compromise of one or more of the subject's fingerprints.

  The goal of this proposal is to identify any usability problems, collect qualitative and quantitative data and determine the participant's satisfaction with the product. We will: 1) carry out systematic usability tests; 2) design suitable performance metrics for assessing perceived authentication usability; 3) perform a comparative analysis of the developed multi-factor scheme against traditional PIN or fingerprint systems; 4) incorporate additional biometric modalities for enhanced security and study its usability.

- **Embedding Expert Bias in Machine Learning for Cybersecurity of Critical Infrastructures**; Milos Manic (VCU); Chathurika Wickramasinghe, Daniel Marino (VCU, VCU); $50,000; In the last decade, there has been a considerable deviation in the previously established decision making process regarding Cyber-Physical Systems (CPSs). The human user used to be the main actor, however, they have been surpassed in capabilities and functionalities by AI, and is thus relegated to a more supervisory role. This has made the comprehension and understanding of the inner workings of AI frameworks of critical importance. The inherent bias that is generated by AI frameworks and negatively affects the acquired results is one of the areas that has not been adequately addressed through this prism. Simply relying on correlatory relationships massively hinders generalization as spurious correlations may provide good performance in development datasets, but fail in novel and unseen scenarios encountered during real-world deployments. In the context of bridging the gap between human and AI, while also allowing for better performing learning algorithms in terms of generalization, we propose a framework for bias control that is based on expert knowledge. More specifically, we propose the introduction of an expert actor that will provide field-specific heuristics and benchmark datasets. Expert knowledge will be used by the main AI framework component in order to minimize the inherent bias of the system or the data, and thus produce definite conclusions, without the negative effect of bias. In this sense, we are countering the effect of "bad" bias, employing "good" bias, or expert knowledge. Given that the only ad-hoc component is the field-specific expert, the proposed project is portable and application agnostic, while at the same time manages to establish the legitimacy and generalizability of the produced results.

- **GINDAR - Generative Adversarial Networks (GAN)-based Internet-of-Medical-Things (IoMT) Network Detection and Response**; Tamer Nadeem (VCU); Abdul Rahman, Sachin Shetty

(VT, ODU); $50,000; With growing healthcare demands and the need for ease of operational management, Internet of Medical Things Internet of Medical Things (IoMT) have grown significantly in recent years and are dominating the healthcare industry. The rise of IoMT is driven by "an increase in the number of connected medical devices that are able to generate, collect, analyze and transmit health data to either a cloud repository or internal servers," the Deloitte report notes. The term 'medical device' (MD) consists of both wearables (e.g., smart watches, fitness trackers, wearable biosensors) and standalone devices such as scales, defibrillators, hospital beds, syringes, blood glucose meters, electrocardiograph, ventilators, insulin pumps, vital signs/physiologic monitors, pacemakers, etc. However, these medical devices are "more" complex in software and hardware with several defects and vulnerabilities that have been found and can lead to possible malicious attacks. Healthcare organizations are the new focus of attackers for carrying out IoMT-focused cyberattacks that are now occurring with greater frequency. Recently, several healthcare security issues and incidents have been reported both in the media and the academic community. Cyberattacks and disruptions in clinical care can have a catastrophic effect on patient safety, which trickles down to the medical staff's responsiveness. Hence, it becomes crucial to efficiently detect and identify any malicious network activities in order to eliminate or minimize the impact of these attacks. In order to realize this, we need to effectively and efficiently be able to detect and identify network traffics corresponding to different medical devices. Gartner established the network detection and response (NDR) solution category in 2020, renaming what it previously called "network traffic analysis". In this project we are aiming at developing and testing GINDAR - an edge-based system that is able to efficiently to monitor and identify the network traffic of individual connected IoMT devices, malwares, or any anomaly and abnormal behavior of an IoMT device.

- **High-precision Insider Threat Detection and Reasoning with Probabilistic Evidence**; Danfeng (Daphne) Yao (VT); $50,000; The main enabler of our technology is the probabilistic programming based computation strategies that have an outstanding ability to handle uncertainties in discovering anomalous patterns. This new capability to handle uncertainties is particularly relevant for detecting insider threats, as there are usually no clearly defined rules and policies. An insider's behaviors would deviate from normally distributed inter dependent events and actions in various aspects. Our probabilistic evidence based system detects this deviation and explains the computational path of the deviation. Our result interpretation unit enables organizations to investigate the causes with accuracy, avoiding costly and embarrassing false alarms. Our technology detects and ranks abnormal events. This ranking capability helps prioritize follow-up manual confirmation. The proposed work will further develop our technology, readying it for commercialization.

- **MedGuard – Monitoring and Detecting Abnormal Activities/Behaviors of Medical Devices"**; Tamer Nadeem (VCU); $50,000; Medical IoT devices or IoMT have seen rapid advancement in recent years with medical applications [1]. This also includes much more sensitive applications such as neurostimulators, implanted cardiovascular defibrillators and more. The term 'medical device' (MD) range from wearables accessories (e.g., smart watches, fitness trackers, wearable biosensors) to bedside/standalone devices (e.g., scales, defibrillators, hospital beds, syringes, blood glucose meters, electrocardiograph, ventilators, insulin pumps, vital signs/physiologic monitors) to critical body implants (e.g., pacemakers, implanted cardiovascular defibrillators). These advancements led to a significant quality of life improvements for many patients and allowed hospitals to serve patients without them having to visit a clinic physically, a necessity given last year's COVID-19 pandemic. However, the more intricate and sophisticated these devices become, the more risk they pose on patients if exploited by malicious actors [10-13]. These security risks are magnified by the fact that the medical field in general has not dealt with such security threats as other industrial fields, and because of this security measures are sometimes considered an afterthought, relegated to be implemented after the fact, rather than an integral part of the core design philosophy. Because of the hackers can always find a way around security measures, and because of the catastrophic and life-threatening aspect of tampering and hacking IoMT devices, it is imperative to have an added layer of security with regards to tampering detection by monitoring the operations and activities of IoMT devices in order to detect and identify any malicious behaviors of the devices. Note that in this project we are focusing on the physical activities of the device and not its data traffic activities. In this project we are aiming at

developing and testing a novel solution; MedGuard – a low-cost high-accuracy real-time to tampering detection solution by monitoring the operations and activities of IoMT devices in order to detect and identify any malicious behaviors of the devices.

4.1.3 Virginia Cybersecurity Challenge

CCI, in partnership with US Ignite, is hosting the Virginia Cybersecurity Challenge to accelerate the Commonwealth's development of talent and products that enhance cybersecurity. Virginia has emerged as a national leader in cybersecurity, boasting the second-highest concentration of technology workers in the nation. The commonwealth considers it vital that Virginia researchers and students take advantage of opportunities to explore cybersecurity via programs such as this challenge. In fact, Governor Northam recorded an announcement kicking off this program that can be found on www.cyberinitiative.org/innovation/virginia-cybersecurity-challenge.html.

The challenge sought submissions from researchers and faculty members at public CCI member universities to develop a cybersecurity prototype that leverages unique elements of emerging 5G technologies to provide secure operations or communications in ways not possible on previous generation networks. This prototype will ultimately develop into a commercializable product solution. Undergraduate and graduate students are encouraged to participate actively on researcher-led teams.

Secure 5G networks will become the backbone to enable IoT, transportation, automated infrastructure, and other autonomous systems of the future. The security of these networks and devices will touch nearly every aspect of people's lives and help drive digital transformation and jobs.

This is a gated, four-phase challenge beginning May 5, 2021. Phases 2-4 will continue from August 2021 into 2022 and culminate in three winning teams selected in December 2022.

4.1.4 Spotlight: Innovate Cyber

The INNOVATE Cyber Challenge program takes a cohort of 20 students from across the Coastal Virginia region and groups them into four teams. Each team is assigned a cybersecurity problem/challenge. The teams use design thinking to come up with unique solutions for this problem. The design-thinking framework – a human-centered method – focuses on creating innovators for creative action that leans heavily on empathy, observation, interviewing, ideation, and brainstorming. A total of 40 students have participated in the program – 20 in the spring 2020 semester and 20 in the fall 2020 semester. The Fall 2020 INNOVATE Cyber Challenge had 20 undergraduate students from Old Dominion University, Christopher Newport University, Norfolk State University, and Paul D. Camp Community College participating in this 11-week program from September to December 2020. Students were divided into five teams and each team was tasked with developing a final cyber-related product or solution related to the education and adoption of cyber hygiene. A virtual showcase was held on November 18, 2020 for the students to pitch their solutions to a diverse group of faculty, administrators, and business contacts. The Fall 2020 projects included:

- Celebrate Cyber Security!
- The Net Pet (Winner: Fall 2020)
- Cyber Hygiene Seminars
- Cyber Hygiene Awareness and Initiative Networking (C.H.A.I.N.)
- THECyberhygeniest.com

In FY22, this highly successful program is being scaled up to be offered to students throughout the entire state.

Chapter 5

Collaborative Partnerships and Projects

5.1 Partnerships

5.1.1 Arlington County Smart Community Pilot

The Arlington County Smart Community Pilot is a program activity to install optical and auditory sensor technology in a designated, commercial zone through a public-private partnership with US-Ignite, Comcast, the Commonwealth Cyber Initiative and Arlington County. The pilot project will help address public safety needs. The goals of the effort are to: 1. improve understanding of pedestrian movements and enhance first responder response time to urgent calls, 2. provide awareness of the county's public safety efforts, and 3. leverage county public assets through a demonstration project designed to benefit residents' public health and safety.

Data collection is via optical, auditory and environmental sensors that view a defined area and capture metadata for just what is defined through the configured algorithm. Pictures, video and audio of individuals will not be captured, only metadata. A limited amount of image processing will occur during the testing phase to validate the sensor's configuration. These images will be stored as sketch images in which individuals and vehicles cannot be uniquely identified.

A Data Privacy Oversight Panel for this activity has been established to provide expert community and independent feedback on all privacy-related aspects of the project. Meetings are held monthly and are open to the public.

Commonwealth Cyber Initiative partnership includes an advisory role to ensure data privacy policies are adhered to in every stage of the pilot. As such, CCI sought faculty members and researchers from Virginia institutions of higher education to help ensure the demonstration pilot meets the cybersecurity, privacy, and data management requirements defined by the County and supports research on pilot results.

Researchers and faculty members at public institutions of higher education in CCI who are deemed eligible by their home institution to serve as a Principal Investigator (PI) on an external grant were eligible to apply.

Two CCI Fellows were selected from the call for proposals to sit on the privacy oversight panel, support the research, and provide their subject matter expertise to the pilot. The selected awardees included Kevin Heaslip, Ph.D., PE, professor, CACI Fellow, Department of Civil & Environmental Engineering, Hume Center for National Security and Technology, Virginia Tech and Nirup M. Menon, Ph.D., professor and associate dean, School of Business with George Mason University.

5.1.2 CyManII

Three Virginia universities participate in Cybersecurity Manufacturing Innovation Institute (CyManII), an inclusive national research Institute with major leading research universities in cybersecurity, smart and energy efficient manufacturing, and deep expertise in research and development, supply chains, factory

automation, and workforce development. Led by The University of Texas at San Antonio and funded by the Department of Energy (DoE), CyManII aggregates the most advanced research institutions in smart and advanced manufacturing, securing automation and supply chains, workforce development, and cybersecurity. The research team brings to bear the most powerful expertise and infrastructure needed to secure the digital transformation that will continue to propel the U.S. in innovated research in manufacturing for decades.

CCI has provided cost sharing funds that enabled VT, VCU, and Mason to play leading roles in CyManII, opening up opportunities for CCI researchers and industry partners to have a major impact in cybermanufacturing.

5.1.3 Industry-led Consortia

O-RAN Alliance

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

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

Next G Alliance

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

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

Open Generation Consortium

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

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

5.2 Correlated Economic Outcomes

In the beginning of FY21, CCI commissioned an economic impact study, conducted by RTI International. Their report, delivered in August 2021, provides a baseline for benchmarking CCI results in future years, as well as early indicators of the economic impact that the initiative has already had. In *Commonwealth Cyber Initiative Economic Impact Assessment, FY2020-FY2021*, 2021, RTI finds that "The CCI hub and four nodes reported significant programmatic outcomes in FY 2020 with even stronger programmatic outcomes in FY 2021." This section summarizes the correlated economic outcomes reported by RTI.

CCI's core programmatic and leveraged funding of $52 million directly supported an estimated 207 jobs. These direct impacts supported an additional 137 jobs and $25 million in economic activity in terms of indirect impacts through the local purchases made to support CCI's operational spending and 150 jobs and $24 million in induced impacts resulting from the increase in local incomes attributable to CCI operational and leveraged spending for a total of 494 jobs, earning an estimated $39 million in labor income and $101 million in Virginia economic activity supported by CCI's FY 2021 activities (Table 5.1). These activities

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

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

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

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

generated an estimated $3.2 million in combined state and local government revenues, including an estimated $1.8 million in Commonwealth of Virginia revenues.

These economic impacts come on top of the impact that CCI activities had in FY20. CCI's core programmatic and leveraged funding in FY 2020 of $55 million directly supported an estimated 237 jobs. These direct impacts supported an additional 143 jobs and $26 million in economic activity in terms of indirect impacts through the local purchases made to support CCI's operational spending and 161 jobs and $26 million in induced impacts resulting from the increase in local incomes attributable to CCI operational and leveraged spending for a total of 541 jobs, earning an estimated $41 million in labor income and $107 million in Virginia economic activity supported by CCI's FY 2020 activities (Table 5.2). These activities generated an estimated $3.5 million in combined state and local government revenues, including an estimated $1.9 million in Commonwealth of Virginia revenues.

Chapter 6

Financial Report

6.1 CCI Hub

The budget and expenditures for the CCI Hub in FY21 are shown in Figure 6.1.

The CCI Hub FY21 budget was $7.5M to execute CCI's three mission lines: research, workforce development and innovation. FY21 was a year of growth for the CCI Hub that included the hiring of two research faculty, two testbed directors and four Hub staff members, as well as, establishing two state-of-the art testbeds. Additionally, the Hub sponsored two CCI network research programs and administered five network research programs using Node funding. The seven research programs of FY21 were network-wide, multi-disciplinary, and supported each of our mission lines. The CCI FY21 budget spend plan and the subsequent budget execution on personnel hiring, research programs, projects, and equipment procurement focused on fostering collaboration among the Regional Nodes and researchers from across the Commonwealth to inculcate a whole-of-state philosophy. CCI network wide collaboration and cooperation remains CCI's greatest strength and increases competitiveness across the national and global research and innovation ecosystems. CCI is confident that the FY21 investments moved the Commonwealth closer to achieving its vision of Virginia as a global leader in cybersecurity.

FY21 presented some challenges that impacted the CCI Hub's execution rate. The COVID-19 pandemic continued to significantly impact hiring and eliminated most travel. Common academic, research, and workforce development events such as, seminars, conferences, workshops, camps, and competitions were not conducted in FY21. Additionally, delayed distribution of appropriated funds caused a shortened spending window during the FY. Therefore, the CCI Hub has committed a portion of FY21 funds for programs, projects and research infrastructure procurement that are scheduled to be executed in early FY22.

For FY22, the CCI Hub anticipates more predictability in funding distribution timelines and easing of COVID-19 restrictions allowing for travel and in-person events. CCI has funded research, innovation, and workforce development programs planned throughout FY22 and a spend plan goal of 25% expenditures per quarter. With these measures in place, CCI is confident that the budget execution rate will be more constant throughout the year.

6.2 CCI Nodes

In 2019, the guidance from the Virginia Research Investment Committee (VRIC) was to use FY21 Node funds to focus on recruiting and hiring eminent faculty. However, the restrictions and constraints of the COVID-19 pandemic and the resulting Commonwealth directed hiring freeze drove the CCI Leadership Council to develop an alternate spend plan for FY21. In June 2020, the CCI Leadership Council, after consulting with the leadership of Center for Innovative Technology (CIT), approved an alternate spend plan for the allocation of the FY21 funds ($10,000,000) for the Regional Nodes, summarized in Table 6.1.

For FY21, the CCI Leadership Council directed that the Hub administer and manage network-wide programs in Research, Innovation, and Experiential Learning using $7M of the Regional Node's $10M appropriation. Details regarding these programs are outlined in Chapters 2, 3, and 4 of this report and a

Program	Funding	Objectives
Base Operations	5%	• Fund operations and other discretionary needs
Talent Recruiting	25%	• Attract and retain top tenure-track and research faculty talent to Virginia
Research	40%	• Foster research excellence in the focus area of each Node • Promote inter-node collaboration (funds used for projects that involve researchers from multiple Nodes)
Research Infrastructure	10%	• Promote experimental research that expands and utilizes the shared research infrastructure
Innovation Programs	10%	• Create innovation programs across the Network • Scale up existing innovation programs
Experiential Learning	10%	• Create experiential learning programs across the Network • Fund a second round of the Experiential Learning program funded by the CCI Hub in FY20

Table 6.1: Node spend plan percentages for FY21. The base operations and talent recruiting funds were managed individually by each Node. The remaining programs, totalling $7,000,000, were managed by the Hub on behalf of the entire Network.

CCI Hub Fiscal Year 2021		
FY21 Appropriation: 7,500,000		
Mission	Committed	Expenditure
Operations		
Labor		1,172,248
IT/Phone/Print		24,577
Supplies		6,153
Professional Development		1,624
Communications		6,294
SWVA Node Testbed Infrasturcture	250,000	
Sub Total	250,000	1,210,896
Workforce Development and Innovation		
Arlington County Project		107,115
Operations		115
Experiential Learning Project Extend	100,000	
Sub Total	100,000	107,230
Research		
Labor		707,515
Hub Faculty		833,197
CCI Fellows		450,000
Sanghani Center GRA	55,000	
Arts & Design Research Project		125,000
Mis/Disinformation Research		453,757
Next G Research Project	1,000,000	
High Performance Computing		11,483
Contract Services		287,664
Equipment (HW/SW)		1,041,558
Sub Total	1,055,000	3,910,174
Totals	1,405,000	5,228,300
Total Expenditure & Committed		6,633,300

Figure 6.1: Budget and expenditures for CCI Hub in FY21.

summary of those programs is shown in Figure 6.2.

Additionally, two of the Nodes hired Program Managers to oversee the day-to-day functions of the Node and assist the Node Director with operations and administration tasks.

The Nodes apportioned their funds into three categories: Operations, Research, and Innovation/Workforce Development. Although the categories are the same and all focused on the cybersecurity field, each Node

FY21 Hub Administered-Node Funded Awards	
Research Project	**Award**
Collaborative Research	
22 x Awards	**3,994,124**
Experiential Learning	
7 x Awards	**966,770**
Experimental Research	
8 x Awards	**399,530**
Research Infrastructure	
4 x Awards	**599,753**
Cybersecurity Innovation Bridge Fund	
7 x Awards	**350,000**
Cybersecurity Challenge	
1 x Award	**181,000**
Misinformation and Disinformation	
3 x Awards	**183,724**
Grand Total	**6,674,901**

Figure 6.2: FY21 network-wide programs.

has the flexibility to plan and execute funds so as to best meet the needs of their region and reinforce the cybersecurity research focus of their region's universities and verticals, namely:

- CVN: Cyber physical systems, autonomous systems, and IoT as they apply to smart cities and communities, as well as medical device security.
- CoVA: The intersection of cyber physical systems and artificial intelligence in maritime, defense, and transportation sectors.
- NoVA: Cybersecurity in national defense, transportation, electric/power distribution, and manufacturing sectors. Also, the impact of human behavior on cyber security and resilience of cyber systems to human behavior.
- SWVA: Cybersecurity related to wireless communications and application domains such as transportation, power systems, manufacturing, autonomous vehicles, and agriculture; cybersecurity and emerging technologies, such as quantum computing; and cryptography.

To foster research collaboration across Nodes was a major CCI goal for FY21, and a total of $4,000,000 in Node funds was allocated to the CCI Cybersecurity Research Collaboration program. This funding program created numerous cross-pollination opportunities for cybersecurity researchers to collaborate across the Commonwealth, bringing multi-disciplinary and multi-vertical expertise to develop a state-wide ecosystem of cybersecurity research excellence.

In FY21, CCI formed the Innovation Committee and the Leadership Council allocated $1,000,000 for programs created by this committee. The committee's charter is to identify and develop opportunities for CCI researchers, faculty, and students to transition experimental technologies, inventions, and intellectual property from the laboratory to the commercial market. The Innovation Committee developed two programs utilizing the Node funds: The Cybersecurity Bridge Fund and the Virginia Cybersecurity Challenge. Each of these programs are detailed in Chapter 4 of the Annual Report.

Workforce development is a principal mission line and purpose of CCI. Building the cybersecurity talent pool within the Commonwealth leads to narrowing the cyber workforce gap, attracts members of the cybersecurity industry to build a presence in Virginia or grow and existing presence, and leads to Virginia being an attractive place to work for recent graduates from the cyber related programs. The Leadership Council allocated $1,000,000 for the Hub to develop and administer a network-wide Experiential Learning program, resulting in seven funded programs across the Commonwealth. Each of these funded programs is outlined in Chapter 3.

In FY21, CCI invested in building and operationalizing two cybersecurity testbeds: The 5G Testbed and the AI Testbed, described in Section 2.4.1. Each testbed was designed and built to enable remote access for researchers from around the state or country to utilize the experimentation capabilities, computing power, data sets, and data storage afforded by the testbeds. The Leadership Council allocated $1,000,000 to a network-wide Experimental Research program. This program funded further testbed development in each of the four Nodes and funded researchers using the CCI to conduct experimental research. Details of the program are outlined in Chapter 2 of the Annual Report.

6.2.1 COVA Node

The budget and expenditures for the CoVA Node in FY21 are shown in Figure 6.3.

6.2.2 CVN

The budget and expenditures for the CVN in FY21 are shown in Figure 6.4.

6.2.3 NOVA Node

The budget and expenditures for the NoVA Node in FY21 are shown in Figure 6.5.

6.2.4 SWVA Node

The budget and expenditures for the SWVA Node in FY21 are shown in Figure 6.6.

6.3 Geographic distribution of the awards from funds contained in HB30

Figure 6.7 shows the distribution of funds by Regional Node.

CCI Coastal Virginia Node Fiscal Year 2021		
FY21 Appropriation: 2,500,000		
Mission	Budget	Expenditure
Operations		
Labor - ITS Engineer	125,000	125,000
Sub Total	125,000	125,000
Workforce Development and Innovation		
Experiential Learning Initiatives	250,000	250,000
Innovation Initiatives	250,000	250,000
Sub Total	500,000	500,000
Research		
Node Faculty Hires	625,000	625,000
Collaborative Research	1,000,000	1,000,000
Infrastructure Related Initiatives	250,000	250,000
Sub Total	1,875,000	1,875,000
Totals	2,500,000	2,500,000
Total Expenditure		2,500,000

Figure 6.3: Budget and expenditures for the CoVA Node in FY21.

CCI Central Virginia Node Fiscal Year 2021		
FY21 Appropriation: 2,500,000		
Mission	Budget	Expenditure
Operations		
Labor and Program Support	125,000	125,000
Sub Total	125,000	125,000
Eminent Faculty		
VCU Eminent Faculty Hire	312,500	312,500
UVA Eminent Faculty Hire	312,500	312,500
Sub Total	625,000	625,000
Workforce Development and Innovation		
Experientail Learning Initiatives	250,000	250,000
Innovation Initiatives	250,000	250,000
Sub Total	500,000	500,000
Research		
Secure, Smart Point of Care Sensors for Lung Health	249,445	249,445
Open source Multi-band, Multi-dimensional Spectrum Access System with Interfaces to Wireless Testbeds and	179,830	179,830
Determination of Safety Limits Against Cyber Threats in Neurodulation Devices Using Maching Learning, Brain Phantoms	200,000	200,000
Enhancing 5G Wireless Network Security with Reconfiguarable Intelligent Sufaces	170,000	170,000
Smart City Infrastructure for Safeguarding Autonomous Vehicles Against Cyber Attacks	200,000	200,000
Sub Total	999,275	999,275
Totals	2,249,275	2,249,275
Total Expenditure		2,249,275

Figure 6.4: Budget and expenditures for the CVN Node in FY21.

CCI Northern Virginia Node Fiscal Year 2021		
FY21 Appropriation: 2,500,000		
Mission	**Budget**	**Expenditure**
Operations		
Operations	124,227	**124,227**
Sub Total	124,227	**124,227**
Workforce Development and Innovation		
Experiential Learning Initiatives	250,000	**250,000**
Innovation Initiatives	250,000	**250,000**
Sub Total	500,000	**500,000**
Research		
NoVa Node Faculty Hires	625,000	**625,000**
User-Centric Privacy Controls for Smart Homes Devices	136,489	**136,489**
RSA-Dc: Building Robust and Self-Adaptive Defense Capability in Cyber Systems	219,839	**219,839**
Enhancing 5G Wireless Network Securitywith Reconfiguarurable Intelligent Surfaces	220,000	**220,000**
Misinformation &Dspatiotemporal G-Code Modeling for Additive Manufacturing Security	176,389	**176,389**
5G Tes5GEM: 5G MED-Enhanced C-V2X for Intersection Management	217,790	**217,790**
Collective and Collaborative Defense for Virginia Regional Cyber Ecosystems	29,493	**29,493**
Infrastructurte Related Initiatives	250,000	**250,000**
Sub Total	1,875,000	**1,875,000**
Totals	2,499,227	**2,499,227**
Total Expenditure		**2,499,227**

Figure 6.5: Budget and expenditures for the NoVA Node in FY21.

CCI Southwest Virginia Node Fiscal Year 2021		
FY21 Appropriation: 2,500,000		
Mission	Budget	Expenditure
Operations		
Personnel		100,112
IT/Phone/Print		2,550
Encumbered Costs		18,300
Sub Total		120,962
Workforce Development and Innovation		
Innovation Programs		85,444
Workforce Programs		436,317
Sub Total		521,761
Research		
Research Collaboration Program		1,000,000
Eminent Scholar	625,000	
Major Thrust Areas		958,885
Research Engagement Program		140,000
Encumbered Costs		545,000
Sub Total		2,643,885
Totals	625,000	3,286,608
Total Expenditure		3,286,608

Figure 6.6: Budget and expenditures for the SWVA Node in FY21.

Node	Number of Awards	Grant Total
Central Virginia	14	$2,389,275
Coastal Virginia	15	$2,548,546
Northern Virginia	13	$2,304,590
Southwest Virginia	18	$2,646,523
Total	**60**	**$9,888,934**

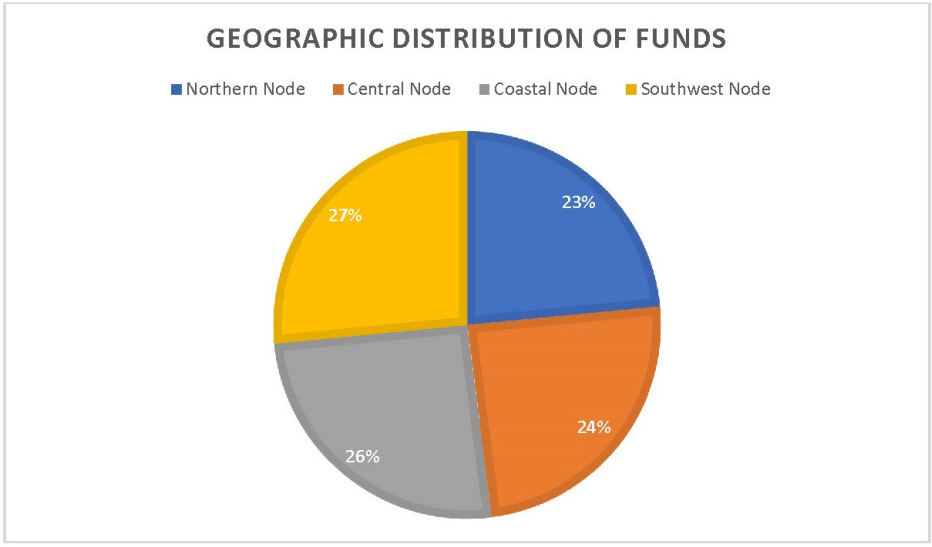


Figure 6.7: Geographic distribution of FY21 Node funds.

Chapter 7

Looking Ahead: FY22

FY21 saw the establishment of the key structures in CCI and the recruitment of administrators and researchers in the initiative. It also saw a vast expansion in the 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 FY21. In this chapter, we outline the main activities and programs planned for FY22.

The investments and early success of CCI in areas including 5G security, Artificial Intelligence (AI) Assurance, and securing cyber-physical systems, positions us particularly well to contribute to federal investments in these key areas, including the goals of the United States Innovation and Competition Act of 2021, which at the time of the writing of this report is being discussed in Congress.

As it starts to be feasible to meet in person, CCI is planning several events for the coming year, including an all-hands CCI symposium, a kick-off workshop for our program on the role of cybersecurity in curbing the spread of misinformation and disinformation (scheduled to be held in Charlottesville in October 2021), and meetings of researchers in each of the four CCI Nodes. CCI was also selected to host the 2022 edition of the Virginia Academy of Science, Engineering, and Medicine (VASEM) Annual Summit.

7.1 Refreshing our Research Themes

From its inception, CCI has identified two research themes, 5G Security and AI Assurance, which have guided many of our investments. This year we are reviewing these themes for a refresh that reflects the latest workforce development needs and research opportunities.

The research themes must: (i) align with CCI's focus on the intersection of cybersecurity, autonomy, and intelligence, and with our mission lines of research, innovation, and workforce development; (ii) contribute to our goal of establishing Virginia as a global leader in cybersecurity; (iii) have high potential for innovation; and (iv) be forward-looking. The process to arrive at the new research themes is to gather input from our Technical Advisory Board (TAB), all CCI researchers, and key stakeholders. We are conducting regional workshops with CCI researchers in the Summer and Fall 2021. We expect to announce the new themes in FY22 and produce collateral, including a video and brochures, disseminating and enforcing those themes.

7.1.1 Securing NextG

One area of clear investment by federal agencies and industry is in building the vision for the next generation of communication networks, usually referred to as NextG or 6G. Leadership in setting this vision is a national priority, and the timing is right for CCI to contribute to this effort, and in particular to develop the solutions needed to secure NextG networks.

We have identified NextG security as an area of investment by CCI in FY22, and will devote approximately $ 1,000,000 in Hub funds to a CCI program whose objectives include: to produce seminal contributions to secure NextG networks; to establish a CCI vision of NextG network security; to position CCI researchers to be competitive for government and industry funding of NextG research; and to contribute to workforce

development for NextG. Projects to be funded in this program will be selected through our usual peer review process, and all CCI researchers are eligible to participate.

To provide a path for research in this area to impact standards and product development, we have joined the Next G Alliance, a North American consortium led by ATIS (atis.org). CCI researchers participate in working groups and contribute to the Alliance with ideas and technical advice.

7.1.2 Inter-Node Collaboration

In FY22 we are continuing to devote resources to incentivize collaboration among researchers in different CCI Nodes. About 10% of Node funds in the coming fiscal year are dedicated to supporting these collaborations.

7.2 Research Infrastructure: Roadmap for the CCI Testbeds

Both of our testbeds continue to grow in scope and accessibility. We are evolving towards a testbed that can support experimentation in securing the Next Generation of networks, often referred to as 6G. Our investments in a 5G compliant end-to-end network that relies on open source components, and on an AI testbed, position us especially well to support experimentation in 6G.

7.2.1 5G and Next Generation Testbed

The roadmap for the 5G and Next Generation testbed in 2021-2022 is summarized in Figure 7.1. Major accomplishments in the roadmap include:

- A fully open-source end-to-end 5G network relying on srsRAN software for the UE and RAN and an open source network core.
- The integration of the O-RAN RIC and our open source 5G implementation, based on srsRAN.
- A mmWave network operation at 28 GHz integrated with our sub-6GHz 5G network.
- A prototype CBRS base station operating in General Authorized Access (GAA) spectrum.

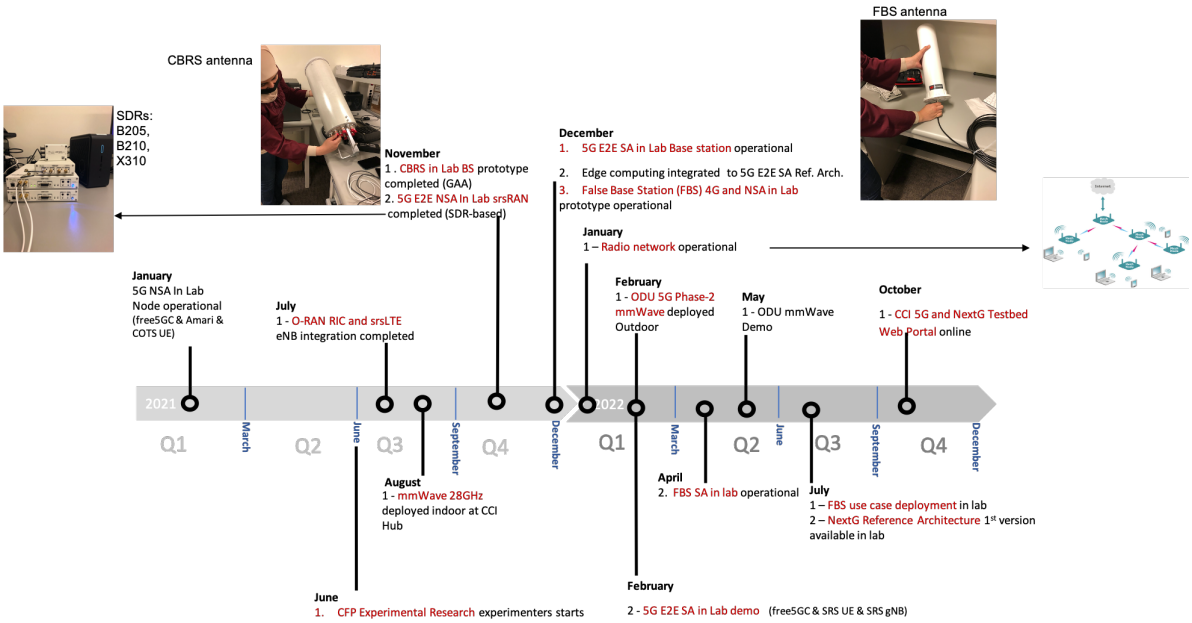


Figure 7.1: CCI 5G and Next Generation testbed roadmap.

This expansion of the testbed in the CCI Hub will be complemented by major new deployments in the Nodes.

Testbed Evolution in the Central Virginia Node

Significant expansion is planned in FY22 for the Medical Security Device lab in CVN. The laboratory will have six tagged VLANs dedicated to different research and administrative needs:

- A smart city IoT VLAN to be used for sensing and IoT devices that communicate with the smart city as part of the hospital building.
- A secure-by-design development VLAN for FPGA and IoT projects.
- An offensive security VLAN where the pen testing environment will be housed for commercial devices and devices from other research groups ready for testing.
- A "user" VLAN for multipurpose workstations on the network.
- A "wireless" VLAN for wireless work stations.
- An "administrative" VLAN for Domain Name System (DNS), packet sniffing intrusion detection server, authentication and key generation server, etc.

The Medical Device Security lab will support research focusing on cyber resiliency to include mission-aware multi-level safety and monitoring impacting devices whose failure may impact patient health or can cause serious safety issues. The devices in the Medical Device Security lab will be used to create a network of stationary and wearable devices for collecting human data that than can be stored in a database and: 1) analyzed locally for anomalies that may indicate sudden medical emergencies such as dangerous glucose spikes or heart attacks, 2) compiled for review by a physician during consultation for a more complete picture of health issues, and 3) used as part of the Open City testbed to simulate environmental interaction with occupants, specifically simulated telehealth or long-term care scenarios. Collected patient data can also be used for analytics purposes to create programs for increasing the veracity of electronic medical records.

7.3 Workforce Development

Workforce development programs planned for FY22 include:

- **CCI Cyber Camp.** in this virtual camp, run in July/August 2021, a selected cohort of undergraduate students from throughout the Commonwealth complete cybersecurity challenges designed by experts from industry, government, and academia, who also serve as camp counselors. Students also go through career training, including resume writing workshops provided by UVA, VT, and Northern Virginia Community College, and mock interviews with cybersecurity practitioners and experts.
- **CCI Internship Fair.** Whether virtual or traditional, internships and apprenticeships offer essential work experience and are a must-do for students who want to explore different fields and organizations within industry, government, academia, and startup programs. In the CCI Internship Fair, to be held in early October 2021, students will have the opportunity to learn about more than 50 internships and apprenticeships available to them. Representatives from the following sponsoring organizations will be on hand to detail available opportunities: Amazon Web Services, Appteon, CivilianCyber, Commonwealth STEM Industry Internship Program, Deloitte, Microsoft, MI Technical Solutions, Palo Alto Networks, Sentara Heathcare, U.S. Department of Health and Human Services, Virginia Space Grant Consortium, WR Systems. Students will be able to ask program leaders questions and learn more about their organizations, how to apply, job expectations, and more. These top programs are recruiting students within the STEM and cybersecurity fields of study but are open to students in other disciplines as well.

- **VMI/CCI CyberFusion.** This invitation-only event combines a collegiate cyber competition with learning and career opportunities that emphasize Cyber Fusion. Commonwealth Cyber Fusion is co-hosted by Virginia Military Institute, Senator Mark R. Warner, the Commonwealth Cyber Initiative, and the Virginia Cyber Range. It will take place in Lexington, VA, in February 2022.
- **Experiential Learning Program.** To date, CCI has created 13 new experiential programs in cybersecurity in Virginia, in topics ranging from a drone race to data poisoning in satellite reconnaissance, for a total of $1.7 million in funding. We will issue the third annual call for proposals in this program in Spring 2022.
- **CCI Affiliates Program.** We will carry out the design and recruitment phase of an affiliates program for CCI that focuses on workforce development, with the objective of launching the program in the second half of 2022.

7.4 Innovation

Innovation programs planned for FY22 include:

- **Innovation Program Focusing on Student Inventors** In the past two years, CCI has launched multiple programs supporting the translation of cybersecurity research into products and startups. In the coming fiscal year, we aim at increasing participation in these programs by CCI students.
- **INNOVATE Cyber** The CoVA Node will form the third cohort for the INNOVATE Cyber program, which provides students with training in design thinking and hands on experience in ideation and product development in response to a cybersecurity problem. The highly successful first two cohorts included students from the Coastal Virginia region, and the program is now expanding to entire Commonwealth.
- **Access to Intellectual Property** CCI's Innovation Committee is working on improving access by industry to intellectual property generated by CCI researchers. This efforts includes identifying IP with high potential for licensing, and devising models of industry involvement that may provide industry partners with preferred access to relevant IP.

Appendices

Appendix 1

Extramural Funding, CCI Hub Faculty

Project Title	PI	Lead Institution	Funding Amount	Funding Agency
Collaborative Research: CPS: Medium: Timeliness vs. Trustworthiness: Balancing Predictability and Security in Time-Sensitive CPS Design	Dr. Tam Chantem & Dr. Ryan Gerdes	Virginia Tech	$1,200,000	NSF
SEcure DIstributed IoT ManagemENT for 5G (SEDIMENT	Dr. Haining Wang	Virginia Tech	$457,659	DARPA
A Special Workshop on AI Safety	Dr. Wenjing Lou	Virginia Tech	$25,000	ARO
SII Planning: National Center for Wireless Spectrum Research	Dr. Wenjing Lou	Virginia Tech	$299,996	NSF
Maven Test & Evaluation Research - Determining the Sufficient Test Dataset for Algorithm Acceptance	Dr. Laura Freeman	Virginia Tech	$500,000	DoD
MITRE UIX: AI Model Certification in Operational Environments	Dr. Laura Freeman	Virginia Tech	$66,000	MITRE
Metrics for Evaluation of Human-Agent Teaming	Dr. Laura Freeman	Virginia Tech	$29,669	MITRE
DoD Cyber Scholarship Program 2020	Dr. Laura Freeman	Virginia Tech	$775,189	NSA
SMC Cyber Institute	Dr. Laura Freeman	Virginia Tech	$1,474,997	NSA
SERC Center for Acquisition Excellence (CAE)	Dr. Laura Freeman	Virginia Tech	$699,999	DOD (OSD)
AI Model Certification in Operational Environments	Dr. Laura Freeman	Virginia Tech	$536,085	DOD (USDI/ARL)
Top-down 5G Networks Security Design and Implementation in Zero-Trust Network Architecture	Dr. Laura Freeman	Virginia Tech	$400,000	Deloitte
Graduate Student Research Program on Artificial Intelligence Enabled Technologies	Dr. Laura Freeman	Virginia Tech	$375,000	Deloitte
Mission Engineering	Dr. Laura Freeman	Virginia Tech	$239,000	DARPA
Total			**$7,078,594**	

Appendix 1

Extramural Funding, CCI Fellows

Project Title	PI	Lead Institution	Funding Amount	Funding Agency
Advancements in low-latency, resilient and energy-efficient 5G network for smart warehouse	Dr. Sachin Shetty	Old Dominion University	$13,000,000 ODU= $850,000	DoD
Cyber Risk and Resilience Analytics	Dr. Sachin Shetty	Old Dominion University	$400,000	FTI
Advanced Instrumentation Technology Spectrum Risk Assessment	Dr. Sachin Shetty	Old Dominion University	$276,000	Circadence
Center of Excellence in AI/ML	Dr. Sachin Shetty	Old Dominion University	$1,750,000	DoD
Achieving Cyber-Resilience for Power Systems using a Learning Model-Assisted Blockchain Framework	Dr. Kevin Heaslip	Virginia Tech	$3,000,000	DoE (SETO)
Support for Smart Thermal Processing	Dr. Kevin Heaslip	Virginia Tech	$100,000	Honeywell Aerospace
CCRI Planning: Towards Building a Community Data Infrastructure for Cybersecurity Research	Dr. Jack Davidson	University of Virginia	$100,000	NSF
Scrubbing PCI from Email	Dr. Duminda Wijesekera	George Mason University	$36,000	DHS
Crocodilian: Space University Small Research Project	Dr. Duminda Wijesekera	George Mason University	$20,000	Lockheed-Martin
Safety Evaluations of Metro North Railroad and Long Island Rail Road	Dr. Duminda Wijesekera	George Mason University	$663,000	Federal Railroad Administration
Safety Evaluations of New Jersey Transit Rail Road	Dr. Duminda Wijesekera	George Mason University	$186,000	Federal Railroad Administration
CyManII	Dr. Duminda Wijesekera	George Mason University	$950,000	DHS/UTSA
Hardening Cybersecurity for mmWave Massive MIMO 5G Networks at Physical Layer	Dr. Kai Zeng	George Mason University	$386,929	ARO
CyberCorps Scholarship for Service: Preparing Future Cybersecurity LeADERS through Applied Learning Experiences	Dr. Hongyi Wu	Old Dominion University	$3,901,236	NSF
Old Dominion GenCyber: JROTC Students and Teachers Interactive Learning in Cyber Defense	Dr. Hongyi Wu	Old Dominion University	$125,000	NSA / ONR
Advanced Data Analytics Toolbox and Sensitivity Analysis in Support of Smart High Precision Experiments and Data Management	Dr. Milos Manic	Virginia Commonwealth University	$200,000	Battelle Energy Alliance
Cyber Physical Anomaly Detection for Wind	Dr. Milos Manic	Virginia Commonwealth University	$75,000	Battelle Energy Alliance
Protective Relay Master Fault Detector AI Algorithm	Dr. Milos Manic	Virginia Commonwealth University	$75,000	Battelle Energy Alliance
Advanced Persistent Threats (APT) Summer Research Apprenticeship Program (APT Summer RAP) Recruitment	Dr. Frank Hu	Norfolk State University	$14,575	DoD
Total			**$13,108,740**	

Appendix 2

Collaborative Research Grants by Node

Central Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Secure, Smart Point of Care Sensors for Lung Health	Dr. Rebecca Heise	Virginia Commonwealth University		$249,445
Open-Source, Multi-Band, Multi-Dimensional Spectrum Access System with Interfaces to Wirelesss Testbeds and Network Simulation Software	Dr. Cong Shen	University of Virginia		$179,830
Determination of safety limits against Cyber Threats in Neuromodulation Devices using Machine Learning, Brain Phantoms and Neural Pathways	Dr. Ravi Hadimani	Virginia Commonwealth University		$200,000
Developing and Open Architecture Testbed and Learning-based Management for Smart Cities (OpenCity)	Dr. Sherif Abdelwahed	Virginia Commonwealth University		$170,000
Smart City Infrastructures for Safeguarding Autonomous Vehicles Against Cyber Attacks	Dr. Felix Lin	University of Virginia		$200,000

Coastal Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Secure and Privacy Preserving 5G Network for Connected Vehicles	Dr. Sachin Shetty	Old Dominion University		$200,000
Backdoor Detection and Mitigation in Deep Neural Networks	Dr. Hongyi Wu	Old Dominion University		$200,000
DeepPOSE: Securing Transportation Systems from GPS Spoofing Attack	Dr. Chunsheng Xin	Old Dominion University		$200,000
A Systematic Evaluation of Smart City Security and Privacy	Dr. Adwait Nadkarni	William & Mary		$194,850
Virginia State Investments in Port of Virginia: A simulation-based framework for Identifying, Assessing, and Mitigating Systemic Cybersecurity at the operational Technology Layer	Dr. Rafael Diaz	Old Dominion University		$200,000

Appendix 2

Collaborative Research Program – Grants by Node

Northern Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
User-Centric Privacy Controls for Smart Home Devices	Motti	George Mason University		$136,489
RSA-DC: Building Robust and Self-Adaptive Defense Capability in Cyber Systems	Chen	George Mason University		$219,839
Enhancing 5G Wireless Network Security with Reconfigurable Intelligence Surfaces	Dr. Kai Zeng	George Mason University		$220,000
Spatiotemporal G-Code Modeling for Additive Manufacturing Security	Prins	James Madison University		$176,389
5GEM: 5G MEC-Enhanced C-V2X for Intersection Management	Dr. Duminda Wijesekera	George Mason University		$217,790

Southwest Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
O-RAN Compliant User Driven RAN Resource Management System for Next-generation Mobile and C-VX2 Communications	Shah	Virginia Tech		$133,500
Evaluation of Lattice-Based Candidates in the NIST Post-Quantum Cryptography Standardization Process in Terms of Security and Performance in Hardware	Morrison	Virginia Tech		$200,000
C3-5GPG: Cybersecure Communications and Control for 5G-enabled Power Grid	Mehirizi-Sani	Virginia Tech		$200,000
Sensor Degradation Detection Algorithm for Automated Driving Systems	Chaka	Virginia Tech		$200,000
Enhancing the Privacy and Reliability of Massive-scale Bluetooth Contact Tracing	Yao	Virginia Tech		$200,000
SmallSat Cybersecurity and Resiliency	Dr. Jon Black	Virginia Tech		$66,500

Appendix 3

Arts and Design Program – Grants by Node

Central Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Moving Choreography to a New Universe: AI Driven Privacy Automation Approach	Dr. Kate Siccio	Virginia Commonwealth University	Dr. Yan Lu / VCU Dr. Sachin Shetty / ODU	$25,000

Coastal Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Develop a Gamified Mobile Application for Cybersecurity Education and Assessment via User Centered Design Process	Dr. Kevin Moberly	Old Dominion University	Dr. R. Patton / VCU Dr. D. Draper / ODU Dr. J. Pittges/ Radford Mr. B. Keener / CivCyber	$25,000

Northern Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Undeleted	Dr. Michael McDermott	George Mason University		$25,000

Southwest Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
A Self-Calibrating, Network-Based, Portable High-Density Loudspeaker Array for Evaluation of Cybersecurity Data and Artistic Expression	Mr. Tanner Upthegrove	Virginia Tech	Dr. M. Roan / VT Dr. R. Patrick / VT	$25,000
Exploring AI and 5G Capabilities for Enabling Online, Real-Time Network Music Collaboration	Mr. Tanner Upthegrove	Virginia Tech	Dr. V. Shaw / VT	$25,000

Appendix 4

The Role of Cybersecurity in the Spread of Disinformation and Misinformation – Grants by Node

Central Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Machine Learning based Disinformation Detection and Its Human Trust in Autonomous Vehicle Systems	Dr. Haiying Shen	University of Virginia	Dr. M. Gorman / UVA	$65,000

Coastal Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Question Under Discussion Framework to Analyze Misinformation Targeting Security Researchers	Dr. Sachin Shetty	Old Dominion University	Dr. T.K. Kissel / ODU	$65,000
The Acceptance and Effectiveness of Explainable AI-Powered Credibility labeler for Scientific Misinformation and Disinformation	Dr. Jian Wu	Old Dominion University	Dr. J. Still / ODU Dr. J. Li / ODU	$63,790

Northern Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Designing Tools for Proactive Counter-Disinformation Communication to Empower Local Government Agencies	Dr. Hemant Purohit	George Mason University	Dr. A. Anastasopoulos /GMU Dr. T. Neaves / GMU Dr. h. Rangwala / GMU	$64,971
Artificial Intelligence Based Analysis of Misinformation and Disinformation Efforts from Mass Media nd Social Media in Creating Anti-U.S. Perceptions	Dr. Hamdi Kavak	George Mason University	Dr. S. Karahan / ODU Dr. H. Wu / ODU Dr. K. Perez / TCC	$64,996

Southwest Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Exploring the Impact of Human-AI Collaboration on Open Source Intelligence (OSINT) Investigations of Social Media Disinformation	Dr. Kurt Luther	Virginia Tech	Dr. A. Brantly / VT Dr. D. Hicks / VT	$65,000
Fast Deployment of AI-Based Disinformation Detector	Dr. Ruoxi Jia	Virginia Tech	Dr. J.B. Huang / VT Dr. A. Ivory / VT	$65,000

Appendix 5

Experimental Research in CCI Testbeds – Grants by Node

Central Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Ultra-thin Smart Coating of Polymer Composite of Novel Magnetic Nonoparticles for High Frequency and Broad-Band Electromagnetic Shielding	Dr. Ravi Hadimani	Virginia Commonwealth University	Dr. R. Barua / VCU	$50,000
Experimenting Aggregated IoT 5G Communication through IMSI Sharing	Dr. Eyuphan Bulut	Virginia Commonwealth University		$50,000

Coastal Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Beamforming Optimization for 5G and Beyond	Dr. Chunseng Xin	Old Dominion University	Dr. H. Wu / ODU	$50,000
Investigating Robustness and Uncertainty of AI Algorithms in Cyber Physical Systems	Dr. Rui Ning	Old Dominion University	Dr. J. Li / ODU Dr. X. Deng / VT Dr. L. Freeman / VT Dr. Y. Hong / VT	$49,906

Northern Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Lightweight Resource-and Workload-aware Malware Detection in IoT Networked Devices	Dr. Sai Dinakarrao	George Mason University		$49,624

Southwest Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Overshadowing Attacks in 5G Systems: Launching and Detecting	Dr. Lingjia Lou	Virginia Tech	Dr. Y. Pan / VT	$50,000
Enabling Trustworthy Base Station as-a-Service in 5G Networks	Dr. Mohammed Azab	Virginia Military Institute	Dr. M. Eltoweissy / VMI Dr. M. Abdel-Malek / VT	$50,000
Cybersecurity of Utility Electric Systems (CUES)	Dr. Ali Mehrizi-Sani	Virginia Tech	Dr. J. Reed / VT	$50,000

Bibliography

Commonwealth Cyber Initiative Economic Impact Assessment, FY2020-FY2021 (tech. rep.). (2021). RTI International.

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/