

GAINING GROUND IN VIRGINIA

CHALLENGES AND OPPORTUNITIES ACROSS CYBER-PHYSICAL SYSTEMS

ABOUT BHEF

The Business-Higher Education Forum (BHEF) is the nation's oldest membership organization of Fortune 500 CEOs, college and university presidents, and other leaders dedicated to the creation of a highly skilled future workforce. BHEF members collaborate and form strategic partnerships to build new undergraduate pathways; improve alignment between higher education and the workforce; and produce a diverse, highly skilled talent pool to meet demand in emerging fields.

ABOUT CYBERSECURITY IN THE COMMONWEALTH OF VIRGINIA

The Commonwealth of Virginia continues to drive the development of new products, companies, and services in the cybersecurity industry, underscored by its unique and abundant technology resources and leadership throughout the United States. Virginia has developed a world-leading technology ecosystem founded on private industry innovation and public-private partnerships. By incorporating principles of collaboration, coordination, government involvement and investment, and integration across key markets, Virginia has created the best holistic environment for cybersecurity research and development in the United States.

BHEF AUTHORS

L. Isabel Cárdenas-Navia

Director of Emerging Workforce Programs

Janet Chen

Associate Director

Debbie Hughes

Vice President of Higher Education and Workforce

01	Letter from Governor McAuliffe
03	Executive Summary
04	The National Cyber-Physical Systems Challenge
08	Virginia's Leadership in Cyber-Physical Systems
22	The Commonwealth of Virginia Cyber-Physical Systems Summit
24	Challenges and Opportunities in Cyber-Physical Systems
30	Education and Workforce Development in Cyber-Physical Systems
36	The Way Forward
38	References

ACKNOWLEDGEMENTS

BHEF would like to thank the National Governors Association and the Office of Naval Research for their contributions and support. This work is funded by the Center for Innovative Technology and the National Science Foundation under Award DUE-1331063. It is part of a partnership between Cyber Virginia and BHEF.

LETTER FROM GOVERNOR McAULIFFE

Dear Constituents,

Cyber touches everything. It's my goal to make Virginia the cyber capital of the U.S. The states that lead on cyber will not only protect their citizens but will drive the new economy. When I was selected as the 2016–17 chair of the National Governors Association, I chose cybersecurity as my chair's initiative. Cybersecurity is a priority for Virginia, and we are in a unique position to address the threats and serve as a leader in this area.

A focus on cybersecurity is an imperative in the New Virginia Economy workforce initiative. Virginia is the number one recipient of Department of Defense investments and has historically relied on military spending; however, sequestration resulted in a \$9.8 billion reduction in direct defense spending

and a loss of approximately 115,000 jobs, which greatly affected regions such as Northern Virginia and Hampton Roads. The second round of sequestration is yet to come. That's why the New Virginia Economy workforce initiative is so important. The initiative seeks to align education with business needs, diversify the economy, increase postsecondary education and workforce credentials, and secure employment for veterans.

Thus far, Virginia has had a lot of successes. In January 2017, I announced that our seasonally adjusted unemployment rate was 4.1%, which continues to be below the national rate of 4.7%. In addition, Virginia's labor force expanded for the fifth consecutive month, setting a new record high for the state. Since I've been governor, we've had great economic activity, creating

185,100 new jobs and \$14.47 billion in new capital. Because 95% of our customers live outside of America and 81% of our growth over the next 10 years will occur outside the U.S., I have become the most traveled governor and gained great success attracting global businesses back to the state, especially in cybersecurity. Virginia now has 650 cyber companies, which is an increase of 200 since 2011. Employment in Virginia's technology sector is expected to increase 25% through 2022, which surpasses the national growth rate of just over 17%.

Among our many accomplishments, Virginia became the site of the first FAA-sanctioned humanitarian package delivery (medical supplies) by drone in July 2015. I am also very proud that Virginia received national attention as one of four states to stand up a new Air Force cyber unit, the Virginia National Guard's 192nd Fighter Wing cyber operations squadron at Langley Air Force Base, in December 2015. In regards to our budget, we doubled our research and development (R&D) tax credit to help incentivize businesses in cyber. We



TERENCE "TERRY" McAULIFFE

650

CYBER COMPANIES
IN VIRGINIA

25%

INCREASE IN EMPLOYMENT
IN VIRGINIA'S TECHNOLOGY
SECTOR THROUGH 2022

36K+

CYBERSECURITY JOB POSTINGS
IN VIRGINIA
FROM Q3 2015–Q2 2016

86M

CYBER ATTACK ATTEMPTS IN
VIRGINIA IN 2016

also created the Cyber Security Scholarship for Service, which pays for up to two years of a student's education in return for a commitment to work for state government in the field of cybersecurity. I was also proud to be the only governor to speak at the RSA Cyber Conference 2017, the largest information and cybersecurity conference in the world.

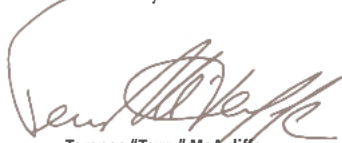
In particular, we are focused on changing our education system. In 2014, there were 17,227 cybersecurity postings. From Q3 2015–Q2 2016, this more than doubled to 36,342 cybersecurity postings in Virginia, showing astonishing growth. Our mission is to improve the education system and fill those jobs. We are making investments and working in a bipartisan way to get this done. We're redesigning STEM courses, providing opportunities for cyber industry experience in high school, and raising awareness of cyber jobs to students as early as fifth grade.

The second big issue is security. In 2016, Virginia had over 86 million attack attempts, equaling three attacks per second, 319 of which became cybersecurity incidents. At the same time, Virginia has blocked over 144,000 pieces of malware and over 832 million spam messages. States have a tremendous amount of records, and there are bad actors trying to steal that data. When I became chair of NGA, I was concerned with establishing a new nationwide program for all 50 governors to address these threats together, which resulted in *Meet the Threat: States Confront the Cyber Challenge*. In this initiative, we created a package with a checklist for all 50 states on the security issue, and the goal is for each state to meet this checklist. With NGA, we've already made tremendous progress, holding a series of regional summits and roundtables on this very issue.

Aligned with this effort, I hosted the first-ever Cyber-Physical Systems (CPS) Summit on September 20–22, 2016, at the Thomas Jefferson National Accelerator Facility in Newport News, Virginia. The goal of the summit was to position Virginia as a leader in CPS education and workforce development, by bringing together CPS stakeholders and highlighting the state's assets, entrepreneurship, programs, and research, with the ultimate aim of achieving economic growth through new jobs, business development, and increased research funding. The following report provides highlights from that summit, and details Virginia's cyber assets, research, and programs. Summits like these ensure that Virginia remains out in front in the cybersecurity field.

We thank all of our partners for Virginia's cybersecurity accomplishments so far, and we look forward to continuing our success and serving as a national leader on this critically important issue.

Sincerely,



Terence "Terry" McAuliffe
Governor
The Commonwealth of Virginia

EXECUTIVE SUMMARY

AS COMPUTERS BECOME EVER FASTER and bandwidth ever cheaper, computing and communication capabilities are embedded within more and more objects and structures in the physical environment. Companies and individuals will benefit, socially and economically, from harnessing these capabilities in real time and across space. Engineered systems, which bridge the cyber world of computing and communications with the physical world, are called cyber-physical systems (CPS).

Recognizing the need to secure CPS both nationally and statewide, Governor Terry McAuliffe and the Commonwealth of Virginia (Virginia), with the support of its partners, hosted the first-ever CPS Summit on September 20–22, 2016, at the Thomas Jefferson National Accelerator Facility in Newport News, Virginia. The goal of the summit was to position Virginia as a leader in CPS education and workforce development by bringing together CPS stakeholders and highlighting the state’s assets, entrepreneurship, programs, and research, with the ultimate aim of achieving economic growth through

new jobs, business development, and increased research funding.

The summit was held as part of Governor McAuliffe’s chair’s initiative for the National Governors Association, *Meet the Threat: States Confront the Cyber Challenge*, which provides all 50 governors the opportunity to collaborate on solutions to the growing cyber threat. During the summit, CPS professionals engaged in roundtable, panel, and plenary sessions on the challenges and opportunities related to three cyber-physical vectors: cyber autonomy, cyber-Internet of Things, and cyber-critical infrastructure.

The summit elicited wide-ranging, productive, and thoughtful discussions that not only addressed challenges and opportunities in each vector but also resulted in recommendations, particularly related to education and workforce development, and highlighted Virginia’s cyber assets, research, and programs.

Engineered systems, which bridge the cyber world of computing and communications with the physical world, are called **cyber-physical systems (CPS)**.

Overall, this report’s recommendations for Virginia include continuing and building upon its current CPS efforts in the following areas:

- **Establishing CPS as a top priority**
- **Aligning the educational system with workforce needs**
- **Building partnerships at all levels and in all sectors**
- **Fostering entrepreneurship and innovation**

Virginia serves in a unique leadership role, and by continuing as well as building upon its current efforts, it will move forward as a national leader in CPS and will inspire other states to follow suit.

THE NATIONAL CYBER-PHYSICAL SYSTEMS CHALLENGE

AS COMPUTERS BECOME EVER FASTER and bandwidth ever cheaper, computing and communication capabilities are embedded within more and more objects and structures in the physical environment. Companies and individuals will benefit, socially and economically, by harnessing these capabilities in real time and across space. Engineered systems, which bridge the cyber world of computing and communications with the physical world, are called cyber-physical systems (CPS).

The expected growth of objects connected to the internet, many of which will be parts of CPS ranging from smaller systems (e.g., meters) to larger systems (e.g., turbines, automobiles), will require an understanding of both the physical system and how to secure it against cyber attacks. This understanding is of particular importance for CPS, for which an attack would not only cause damage once complete but also result in significant and potentially deadly manifestation. It is also important for the state of Virginia, which experienced more than 86

million attack attempts (or three attacks per second), 319 of which became cybersecurity incidents, and blocked more than 144,000 pieces of malware and more than 832 million spam messages from January to December 2016 (Cyber Virginia, 2016d).

Skilled workers are needed to address the threats in CPS. According to a Burning Glass Technologies analysis (2016), the market for cybersecurity jobs and demand for cybersecurity talent is high, particularly in Virginia.

UNLESS OTHERWISE NOTED, ALL STATISTICS IN THE FOLLOWING PAGES ARE FROM BURNING GLASS TECHNOLOGIES (2016).

An aerial view of a city model, likely representing a smart city or cyber-physical system. The model features various buildings, streets, and a river. Overlaid on the image are several glowing blue nodes connected by white lines, suggesting a network or data flow. The background is a blurred image of a city with a river and greenery.

THE MARKET FOR CYBERSECURITY JOBS IS LARGE

From July 2015 to June 2016, **348,975 cybersecurity jobs** were posted nationally.

A total of **778,402 workers** were employed in the cybersecurity field.

Overall, **2.2 cybersecurity workers** were employed for every opening across the nation. This implies turnover of half the existing workforce every 12 months to fill every role.

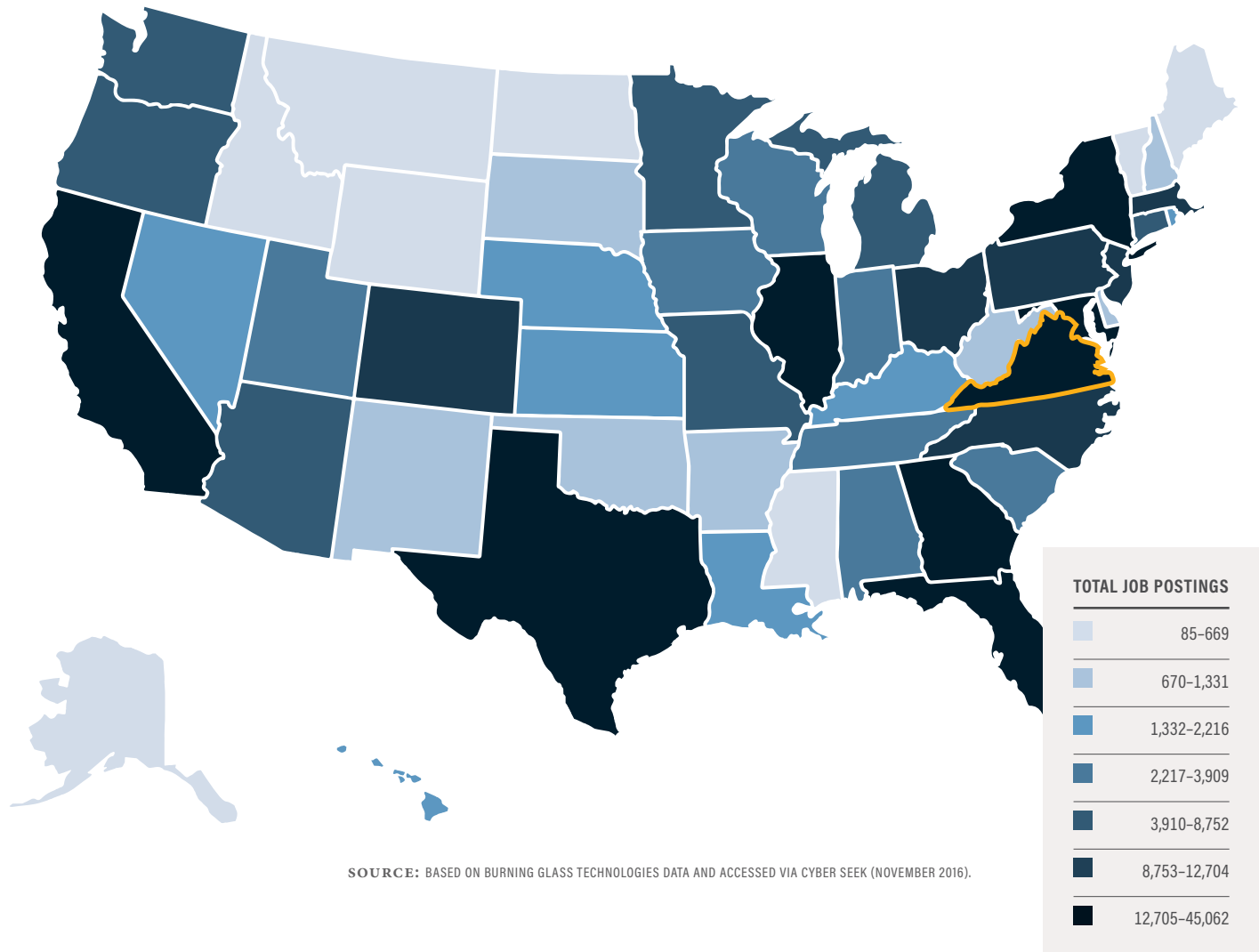
The cybersecurity jobs in highest demand in the United States were cybersecurity analyst/specialist, cybersecurity engineer, and auditor.

DEMAND FOR CYBERSECURITY TALENT IS OUTSTRIPPING SUPPLY

The Certified Information Systems Security Professional (CISSP) certification is the most commonly requested cybersecurity credential, but the demand for CISSP talent dramatically outstrips supply. From July 2015 to June 2016, **U.S. employers attempted to fill 92,802 jobs requiring CISSP certification from a pool of only 69,549 CISSP certificate holders.** (International System Security Certification Consortium, Inc., 2016)

FIGURE 1

CYBERSECURITY POSTINGS BY STATE
JULY 2015-JUNE 2016



SOURCE: BASED ON BURNING GLASS TECHNOLOGIES DATA AND ACCESSED VIA CYBER SEEK (NOVEMBER 2016).

Virginia Leads the Nation in Cybersecurity Demand

- **From July 2015 to June 2016, the D.C.-Maryland-Virginia (DMV) region released 64,602 cybersecurity job postings.**
- **Of these, Virginia released 36,342 cybersecurity job postings, second only to California and 56% of those postings are from the DMV region (see Figure 1).**

OVERVIEW OF CYBERSECURITY JOBS IN VIRGINIA

In 2014, Virginia released **17,227 cybersecurity job postings** (Burning Glass Technologies, 2015). This number more than doubled to 36,342 from July 2015 to June 2016.

A total of **85,982 workers** were employed in the cybersecurity field in Virginia from July 2015 to June 2016.

This is equivalent to a **supply/demand ratio of 2.4**, only slightly higher than the national average of 2.2. In other words, there are 2.4 employed workers for

every job opening in cybersecurity in Virginia—less than the size of the average talent pool for all jobs (5.0 employed workers for every opening).

Virginia is the highest contributor to cybersecurity demand in the DMV region, accounting for 56% of cybersecurity job postings.

The cybersecurity **jobs in highest demand** in Virginia are **cybersecurity analyst/specialist**, **cybersecurity engineer**, and **network engineer/architect**.

30%

OF ALL CYBERSECURITY
JOB POSTINGS REQUIRE
CISSP. **CISSP IS THE MOST
DEMANDED CYBERSECURITY
CERTIFICATION IN VIRGINIA.**

Virginia estimates that employment in its technology sector is expected to increase by 25% through 2022, which surpasses the national growth rate of just over 17% (Virginia Economic Development Partnership, 2016). Addressing the CPS challenge is critical not only across the United States but also in the state of Virginia.

VIRGINIA'S LEADERSHIP IN CYBER-PHYSICAL SYSTEMS

VIRGINIA IS IN A UNIQUE LEADERSHIP POSITION TO ADDRESS THE CYBER-PHYSICAL SYSTEMS CHALLENGES:

Virginia was recognized for its **prioritization of and national leadership in cybersecurity** in a November 2015 Pell Center study, *State of the States on Cybersecurity* (Spidaleri, 2015).

Virginia is **home to more than 650 cybersecurity companies**, which is the most per capita in the nation.

Virginia has **60 data centers**, which are estimated to pass through 70% of the world's internet traffic.

Virginia has **more than 19,000 technology companies** and **280,000 technology workers**.

Virginia is **home to 12 defense contractor headquarters, 19 defense installations**, as well as the Pentagon, Quantico, Defense Advanced Research Project Agency (DARPA), and other federal agency headquarters.

Virginia is home to **20 of the Washington Technology Top 100 federal contracting company headquarters** (Cyber Virginia, 2016f).

Virginia's **federal contract spending increased by almost \$1 billion** from 2013 to 2014, the highest of all states (National Contract Management Association and Bloomberg Government, 2015).

Northern Virginia is considered to be best positioned to become the **next "Silicon Valley" of cybersecurity** (Sorcher, 2015).

Virginia accounted for more than **\$44.6 billion in defense contracts as of FY 2013**, making it the number one state for Department of Defense investment (Virginia Economic Development Partnership, 2014).

Virginia is one of four states to stand up **a new Air Force cyber unit**, the Virginia National Guard's 192nd Fighter Wing cyber operations squadron at Langley Air Force Base (McAuliffe, 2015).

The University of Virginia (UVA) and GrammaTech's automated system, Xandra, won **\$1 million in a first-of-its-kind Cyber Grand Challenge** competition, hosted by DARPA (Mather, 2016).



VIRGINIA HAS BEEN RECOGNIZED FOR SEVERAL CYBER FIRSTS AMONG STATES IN THE NATION:

Adopting the National Institute of Standards and Technology Cyber Framework

Declaring itself an Information Sharing and Assessment Organization (ISAO)

Requiring enhanced security on debit or credit card transactions

Enacting landmark digital identity legislation, now used as the model by other states

Registering apprenticeships for cybersecurity jobs (first in Virginia history)

Establishing a pay-for-performance workforce training program

Signing a memorandum of understanding with the Government of Victoria (Australia) enabling innovation through research and development and the generation of a pipeline of future technologies; promoting sharing of best practices; and enhancing cybersecurity policy

Hosting a Cyber Physical Systems Summit to build awareness of the growing challenges associated with securing autonomous systems, critical infrastructure, and the Internet of Things (Cyber Virginia, 2016d)

IN PARTICULAR, CYBER PLAYS A KEY ROLE in the New Virginia Economy. Established by Governor McAuliffe in 2014, the New Virginia Economy seeks to align education with business needs, diversify the economy, increase postsecondary education and workforce credentials, and secure employment for veterans. One of the goals is to produce 50,000 apprenticeships, associate degrees, certifications, credentials, and licensures in STEM-H (science, technology, engineering, mathematics, and health) to meet Virginia's workforce needs. The state is establishing its cyber leadership and making several key investments in education and workforce development to continue the growth of cyber and meet the demand for cyber talent (Secretary of Commerce and Trade, 2014).

ESTABLISHING LEADERSHIP IN CYBER EDUCATION

15,000+

SCIENCE AND ENGINEERING GRADUATE STUDENTS PURSUING AN ADVANCED DEGREE
AND MORE THAN 1,400 SCIENCE AND ENGINEERING DOCTORATE DEGREES AWARDED
EACH YEAR (CYBER VIRGINIA, 2016F)

407%

ENROLLMENT GROWTH AT THE VIRGINIA
COMMUNITY COLLEGE SYSTEM FROM
FALL 2014 TO FALL 2015

17

OUT OF 23 COMMUNITY COLLEGES
OFFER ONE OR MORE COURSES
ALIGNED TO CYBERSECURITY

8

COMMUNITY COLLEGES IN
VIRGINIA OFFER SECURITY
CERTIFICATES

13

CENTERS OF ACADEMIC
EXCELLENCE AT 11 INSTITUTIONS

35%+

OF VIRGINIANS HAVE AT LEAST
A BACHELOR'S DEGREE, THE
EIGHTH HIGHEST EDUCATIONAL
ATTAINMENT RATE IN THE NATION

44%

INCREASE IN CYBERSECURITY ENROLLMENT AT COMMUNITY COLLEGES SINCE SPRING 2016 AND
668% SINCE THE BEGINNING OF GOVERNOR MCAULIFFE'S ADMINISTRATION

VIRGINIA'S K-12 EDUCATION CYBER INITIATIVES INCLUDE THE FOLLOWING:

CONFERENCE ON CYBER AND EDUCATION.

Hosted by the Cyber Security Commission in December 2015, this conference engaged educators, employers, and government leaders on cybersecurity issues (Cyber Virginia, 2015a). As a result, the Virginia Department of Education:

- Established cybersecurity as a career pathway in middle and high school career and technical education programs
- Created Virginia's Cyber Security and Cyber Forensics Infusion Units, which identified 85 tasks and competencies for incorporation into existing STEM courses
- Provided grant funds for 32 cyber camps in 2016

GENCYBER. Supported by the National Security Agency (NSA) and the National Science Foundation (NSF), the GenCyber program is a cybersecurity boot camp for Virginia educators. Its goal is to provide awareness and education to K-12 students, teaching methodologies to computer science teachers, and resources for teaching and learning curricula in cybersecurity (GenCyber, 2017).

NATIONAL SECURITY AGENCY DAY OF CYBER. Sponsored by the NSA, the Day of Cyber is designed to introduce and inspire the students in schools and colleges across the nation to pursue STEM careers and connect them to this in-demand digital workforce. Participating Virginia students can engage in a free, interactive, self-guided, and fully automated cybersecurity career experience (LifeJourney, Inc., 2017).

STANDARDS OF LEARNING CURRICULUM.

In May 2016, Governor McAuliffe signed legislation to incorporate computational thinking, computer coding, and computer science into the state's Standards of Learning Curriculum. The measure will help prepare students for technology jobs (Llovio, 2016).

STEM ACADEMIES. STEM Academies, such as Virginia's George C. Marshall Governor's STEM Academy and Chantilly Governor's STEM Academy, provide students with opportunities to earn high-demand STEM credentials for the 21st century (Virginia Department of Education, 2017).

VIRGINIA'S HIGHER EDUCATION CYBER INITIATIVES INCLUDE THE FOLLOWING:

TWO-YEAR COLLEGE TRANSFER GRANT

PROGRAM (CTG). Passed into Virginia law in 2007, CTG allows qualifying students who have completed their associate's degree at a Virginia two-year public college and transferred to a participating Virginia four-year college or university to receive a \$1,000 CTG award per year if enrolled in STEM programs, such as information technology and cybersecurity.

CYBER SECURITY SCHOLARSHIP FOR

SERVICE. The State Council on Higher Education in Virginia offers the Cyber Security Scholarship for Service, which pays for a student's education in return for a commitment to work in state government in the cybersecurity field. In the 2016-2017 academic year, \$500,000 was appropriated for this program.

NATIONAL CENTERS OF ACADEMIC EXCELLENCE (CAE). Sponsored by NSA and the Department of Homeland Security, CAE in Information Assurance and Cyber Defense (IA/CD) programs reduce vulnerability in the national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise. Virginia has 14 CAEs at 12 institutions. Recently, Northern Virginia Community College became a CAE Regional Resource Center, supporting both two- and four-year institutions seeking CAE designation in the central Eastern region, including Delaware, the District of Columbia, Kentucky, Maryland, Tennessee, Virginia, and West Virginia (The Information Assurance Directorate, 2016). Virginia plans for all of its community colleges to become CAE designated.

VIRGINIA CYBER RANGE. In September 2016, Virginia launched its cyber range, which is designed to be a state-of-the-art platform for cybersecurity education that provides hands-on, industry-relevant advanced cybersecurity training exercises for high school and college students to prepare them for the cybersecurity workforce. Managed by Virginia Polytechnic Institute and State University (Virginia Tech), the range is currently available to Virginia students at any of its CAE schools (Virginia Cyber Range, 2016).

VIRGINIA SPACE GRANT CONSORTIUM (VSGC). In partnership with the Virginia Community College System (VCCS), NASA Langley Research Center, and NASA Wallops Flight Facility, the VSGC offers the STEM Takes Flight at Virginia's Community Colleges. STEM Takes Flight consists of programs for Virginia community college students pursuing STEM majors (exclusive

of allied health and business) and faculty in STEM disciplines statewide (Virginia Space Grant Consortium, 2016).

VETERANS' PORTAL. VCCS will launch a veterans' portal demonstrating how college credit is awarded for military experience, which will serve the more than 800,000 veterans in Virginia.

GEORGE MASON UNIVERSITY (GMU) VETERANS PATHWAY PROGRAM IN CYBERSECURITY. GMU offers a veterans pathway program in cybersecurity, which allows veterans to transfer through guaranteed admissions to a bachelor of applied science in cybersecurity at GMU after completing an associate's degree at a Virginia community college.

COMMONWEALTH CYBER FUSION 2017 AND INAUGURAL VIRGINIA CYBER CUP CHALLENGE. Cyber Fusion is the organized integration of data and tools from disparate sources to support a secure and resilient system lifecycle. Co-chaired by Governor McAuliffe and Senator Mark Warner, Cyber Fusion 2017 features an inaugural Virginia collegiate cybersecurity competition with Jeopardy-style teams using the Virginia Cyber Range called the Virginia Cyber Cup Capture the Flag. The invitation-only event includes a cyber job fair, keynote speaker, and panel discussions. Hosted by Virginia Military Institute and sponsored by the Virginia Secretary of Technology and Senator Warner, the Cyber Fusion emphasizes the integration of technology with policy and intelligence. Ten colleges competed in the inaugural event in February 2017 at the Virginia Military Institute in Lexington, Virginia (Cyber Virginia, 2017).

ESTABLISHING LEADERSHIP IN CYBER WORKFORCE DEVELOPMENT

10%

OF VIRGINIA'S PRIVATE-SECTOR WORKFORCE ARE EMPLOYED IN TECHNOLOGY, WHICH IS THE LARGEST CONCENTRATION OF HIGH-TECH WORKERS IN THE NATION (TECHAMERICA FOUNDATION, 2011)

~19%

OF ITS PAYROLL STEMS FROM TECHNOLOGY COMPANIES IN 2014 (VIRGINIA DEPARTMENT OF EDUCATION, 2016)

67,850+

VIRGINIANS WORK IN CYBERSECURITY

18,000

PEOPLE SEEK CIVILIAN EMPLOYMENT AFTER LEAVING VIRGINIA MILITARY BASES ON AN ANNUAL BASIS (CYBER VIRGINIA, 2016F)

#3

VIRGINIA IS RANKED THIRD FOR COMPUTER SYSTEMS DESIGN AND RELATED SERVICES JOBS, AS WELL AS FIFTH IN ENGINEERING SERVICES (COMPTIA, 2015)

\$20 MILLION

NSF GRANT FOR CYBER WORKFORCE DEVELOPMENT AND INNOVATIVE SCIENTIFIC PARTNERSHIPS RECEIVED BY VIRGINIA TECH (HPN NEWS DESK, 2016)

VIRGINIA'S CYBER WORKFORCE INITIATIVES INCLUDE THE FOLLOWING:

K-20 PIPELINE FOR CYBERSECURITY

WORKFORCE. Funded by the Department of Energy, Norfolk State University is leading a \$25 million collaborative effort to develop a K-20 pipeline for the cybersecurity workforce (Virginia Department of Education, 2016).

CYBER VETERANS INITIATIVE. Announced by Governor McAuliffe on Veteran's Day 2016, Cyber Vets Virginia provides veterans with access to cybersecurity training and resources to enter the Virginia cybersecurity workforce. In January 2017, Governor McAuliffe announced an expansion of the initiative to include cybersecurity training through the SANS VetSuccess Immersion Academy (AlexandriaNews, 2017).

CYBER JOBS. Virginia's Cyber Jobs website connects the state's cyber professionals to the state's cyber jobs.

NEW ECONOMY WORKFORCE CREDENTIAL GRANT FUND AND PROGRAM.

The New Economy Workforce Credential Grant Fund and Program supports students who pursue high-demand workforce credentials such as information technology and cybersecurity. It is a first-of-its-kind, pay-for-performance model designed to create and sustain a supply of credentialed workers who meet business needs (State Council of Higher Education for Virginia, 2016).

CYBERSECURITY APPRENTICESHIP

PROGRAM. Announced by Governor McAuliffe in June 2016, Virginia businesses can now develop registered apprenticeships for cybersecurity occupations. Approved by the Virginia Apprenticeship Council, three new registered cybersecurity apprenticeship occupations include information security analyst-computer forensics analyst, information security analyst-cybersecurity analyst, and information security analyst-incident response analyst. Virginia's first partnership is in Hampton Roads between Tidewater Community College and Peregrine Technical Solutions (Coy, 2016a).

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE).

Coordinated by the National Institute of Standards and Technology at the Department of Commerce, NICE is a national effort to advance cybersecurity education and training opportunities for career preparation. Composed of federal departments and agencies, industries, and academic institutions, NICE has 13 affiliates in Virginia, including seven academic institutions (Cyber Virginia, 2016f).

These Virginia investments ensure that cyber remains a priority and that the state's education and workforce development systems address the state's cyber needs.

VIRGINIA IS ALSO LEADING IN CYBER POLICY

Executive Order #8 launched **Cyber Virginia** and the **Cyber Security Commission**.

Executive Directive #5 mandates a clear path to **secure consumer transactions using authentication technology**, such as "chip and pin."

Executive Directive #6 **improved cyber protocols**, expanded cyber-related risk management activities, and conducted inventory of the state's critical and sensitive systems.

HB1946/SB919 **sealed administrative subpoenas** for electronic communications and social networking data.

SB1121 **defined IT responsibilities** of agency directors.

HB1562/SB814 **addressed electronic identity management standards** and liability.

SB1307 **clarified language for search warrants** for seizure, examination of computers, networks, and other electronic devices.

SB1109 **secured Freedom of Information Act (FOIA) exemptions** for meetings and discussions that include sensitive information regarding cybersecurity vulnerabilities.

SB1129 **secured FOIA exemptions for plans, information, or responses to terrorism** regarding cybersecurity threats and vulnerabilities.

HB924 **allowed providers to verify the authenticity of reports** or records with an affidavit from the custodian of the records (Cyber Virginia, 2016d).



ADDITIONAL VIRGINIA CYBER POLICY INITIATIVES INCLUDE THE FOLLOWING:

CYBERSECURITY COMMISSION AND CYBER VIRGINIA.

Virginia established the Cyber Security Commission and Cyber Virginia by Executive Order (EO8) in February 2014 (Commonwealth of Virginia Office of the Governor, 2014). The commission brings together public- and private-sector experts to make recommendations to position Virginia as a leader in cybersecurity. In August 2015, the commission released its first report with recommendations to expand Virginia's cyber leadership (Cyber Virginia, 2015b). Cyber Virginia is focused on developing a strong cyber workforce. The commission ended its work in 2016 (Cyber Virginia, 2016a).

SENATE CYBERSECURITY TASK FORCE.

Launched in January 2016 and led by Senator Warner, the task force is composed of experts from the federal government and the private sector to not only facilitate discussion but also produce concrete deliverables. Within six months, the task force accomplished the following:

- **Promoting Value Based Defense Procurement Act.** Lowest Price Technically Acceptable (LPTA) is typically used in a source selection process when requirements are well defined, the risk of unsuccessful contract performance is minimal, and price is a significant factor. Given the LPTA's lack of applicability to cybersecurity, the task force successfully proposed legislation that would limit the use of LPTA for cybersecurity in the Department of Defense (Warner, 2016).

- **Senate Cybersecurity Caucus.** Launched in June 2016 by Senators Mark Warner and Cory Gardner, the caucus informs senators and their staff on major policy issues and developments in cybersecurity. In two months, 16 members signed up to join the caucus.
- **Federal Cyber Collaboration Channel.** The channel provides a platform for federal agencies to post difficult cyber-related problems and for private-sector companies to post solutions. All the federal agency chief information officers (CIOs) participate, which provides many opportunities for joint solutions between federal agencies and private-sector companies.
- **Automated Cloud-Based Compliance.** Amazon Web Services and Telos Corporation collaborated to expedite security compliance of cloud systems through automation. The task force sent a letter to federal agency CIOs recommending the approach as a way to streamline the security compliance process (Telos Corporation, 2016).
- **Cyber Reserve Training Corps.** In collaboration with the Partnership for Public Service, the task force is developing a Cyber Reserve Training Corps, which, similar to the military's Reserve Officers' Training Corps program, will recruit private-sector and National Guard cyber professionals to serve at the ready in the event of a national network emergency.

These initiatives demonstrate Virginia's leadership at both the federal and state levels.

NATIONAL GOVERNORS ASSOCIATION INITIATIVE MEET THE THREAT

Virginia is focused on how to address the cyber threat nationwide through Governor McAuliffe's National Governors Association (NGA) 2016-2017 chair's initiative, *Meet the Threat: States Confront the Cyber Challenge*. This initiative is designed to provide all 50 governors with the opportunity to collaborate on solutions to the growing cyber threat, including the development of a cybersecurity checklist for states, a website of resources, and a series of regional summits and roundtables. **The initiative's primary goal is to strengthen state cybersecurity strategies and practices regarding critical infrastructure, economic and workforce development, education, energy, health care, IT networks, safety, and transportation.** Virginia will conclude the initiative with a National Summit on State Cybersecurity to share best practices and lessons learned among representatives from each state, commonwealth, and territory (National Governors Association, 2017a).

Among the *Meet the Threat* initiatives is the NGA Cyber Policy Academy, which provides five states (Connecticut, Illinois, Louisiana, Nevada, and Oregon) with the opportunity to collaborate on comprehensive strategies to address cyber threats and assist in cyber education, prevention, and response across multiple fields. Governor McAuliffe and Governor Rick Snyder (Michigan) will lead the academy, along with partners from academia, federal agencies, the private sector, and research institutions.

THUS FAR, MEET THE THREAT EVENTS INCLUDE THE FOLLOWING:

JULY 16, 2016

Governor McAuliffe Named NGA Chair, Unveils Cyber Initiative.

At the Closing Session of the 2016 NGA Summer Meeting, Governor McAuliffe was named NGA chair and Governor Brian Sandoval (Nevada) was named vice chair. Governor McAuliffe also announced his chair's initiative, *Meet the Threat*.

JULY 19, 2016

First Cyber Roundtable.

Held at the INOVA Center for Personalized Health, Governor McAuliffe's first official meeting for *Meet the Threat* convened health care CEOs to address the intersection of cybersecurity and health care.

JULY 29, 2016

C-SPAN Newsmakers Interview.

For its weekly program "Newsmakers," C-SPAN interviewed Governor McAuliffe from the Democratic National Convention in Philadelphia. Governor McAuliffe discussed his role as NGA chair and his *Meet the Threat* initiative.

SEPTEMBER 7, 2016

Second Cyber Roundtable.

Governor McAuliffe hosted an education and workforce cyber event at Northern Virginia Community College. The event convened 40 cyber and education experts, including college presidents, education organization leaders, and cybersecurity industry CEOs, to discuss ways that states, universities, and the private sector can enhance workforce development, promote cybersecurity education, and protect valuable intellectual property.

SEPTEMBER 20, 2016

CPS Summit Roundtables.

Governor McAuliffe hosted this first-ever CPS Summit at the Thomas Jefferson National Accelerator Facility in Newport News, Virginia. Roundtable sessions convened cyber professionals to discuss the challenges and opportunities within three cyber-physical vectors: cyber autonomy, cyber-critical infrastructure, and cyber-Internet of Things.

OCTOBER 5-7, 2016

First Regional Summit.

Governor McAuliffe hosted the first regional summit on state cybersecurity in Boston, Massachusetts, which convened officials from 26 states and territories and seven federal agencies. Plenary and panel sessions discussed workforce development initiatives and explored cybersecurity in relation to critical infrastructure, health care, higher education, and public safety.

DECEMBER 8, 2016

Small Business Cyber Roundtable.

Hosted by the Northern Virginia Chamber of Commerce, Governor McAuliffe and small business owners discussed how to improve their cybersecurity posture. This was the governor's fourth roundtable.

FEBRUARY 25, 2017

2017 NGA Winter Meeting.

At this meeting, led by NGA chair, Governor McAuliffe, and NGA vice chair, Governor Brian Sandoval (Nevada), the nation's governors gathered in Washington, D.C. to discuss cyber challenges at a plenary session. The session included a panel discussion—led by Homeland Security and Public Safety Committee chair, Governor Asa Hutchinson (Arkansas), and vice chair, Governor Kate Brown (Oregon)—during which Adam Clayton Powell III from the University of Southern California Annenberg Center, Mary Galligan from Deloitte & Touche, John P. Carlin from Morrison Foerster, and Vint Cerf from Google spoke on critical cybersecurity issues (National Governors Association, 2017b).

OTHER VIRGINIA CYBER INITIATIVES INCLUDE THE FOLLOWING:

CYBERSECURITY INFORMATION PORTAL.

This public website provides information on best practices and standards in cyber for businesses, citizens, and government organizations (Cyber Virginia, 2016e).

COMMONWEALTH SECURITY AND RISK MANAGEMENT (CSRM) DIRECTORATE. Part of the Virginia Information Technologies Agency (VITA), the CSRM Directorate protects Virginia's citizen data and provides a safe, secure technology environment. To do this, the CSRM Directorate develops and manages an evolving portfolio of processes and tools that protect Virginia's data and systems (Virginia Information Technologies Agency, 2016).

INFORMATION SHARING AND ANALYSIS ORGANIZATION. Virginia will establish a Mid-Atlantic Information Sharing and Analysis Organization as a forum for information sharing across industries on the cyber threat among companies, government, and universities.

RESEARCH AND DEVELOPMENT (R&D) TAX CREDIT. The state has doubled its R&D tax credit to incentivize businesses to continue their work in this area. Businesses may claim a tax credit equal to 15% of the first \$234,000

in Virginia-qualified R&D expenses incurred during the taxable year. The tax credit increases to 20% if the qualified research was conducted in conjunction with a Virginia college or university.

VIRGINIA CYBER SECURITY PARTNERSHIP (VCSP). In partnership with the FBI, Virginia established the VCSP in 2012. The VCSP is a trusted community of public- and private-sector cyber professionals that collaborate to address cyber threats. It has more than 220 active members and has held more than 35 events throughout the state.

VIRGINIA STATE POLICE HIGH TECH CRIME DIVISION (HTCD). Formed in 2009 by the Department of State Police, the HTCD uses leading technologies to provide specialized law enforcement services to the Department. The Virginia Assembly funded 10 additional positions for the HTCD in 2016.

CYBER GUARD PRELUDE. Designed to test state-level cyber response procedures, Cyber Guard Prelude 2015 engaged state agency partners along with federal, local, and private-sector stakeholders in a tabletop exercise. A functional exercise is being planned for Cyber Guard Prelude 2016 (Cyber Virginia, 2016f).

VIRGINIA IS A LEADER IN CYBER and committed to cyber initiatives and investments to continue its success in the field. Moving forward, Virginia plans to increase capacity and attract even more cyber jobs and investment. In Virginia's 2017–18 budget bill, cyber initiatives include an increased number of Cyber Centers of Excellence, the Virginia Scholarship for Service Program, the Veterans Pathway Program in Cybersecurity at GMU, the Virginia Cyber Range, IT Security Service Center (VITA), Information Sharing and Analysis Organization, Virginia Fusion Center, and the HTCD (Cyber Virginia, 2016b).

In addition, Virginia is aligned with and envisions itself as a key partner in the federal government's investment and initiatives in cybersecurity. President Obama allocated \$19 billion for cybersecurity in the Fiscal Year 2017 budget and developed a Cyber Security National Action Plan (CNAP) to provide an additional \$3.1 billion to address outdated IT infrastructure. The CNAP gives \$62 million to cybersecurity personnel, including those at Virginia's National Centers for Academic Excellence Cybersecurity Program locations (The White House, 2016a). Virginia hopes to serve as a home for the new technology partnerships outlined in the CNAP, such as the National Center for Cybersecurity Resilience and the Cyber Security Assurance Program, and to continue as a leading voice in partnerships on this effort.

THE COMMONWEALTH OF VIRGINIA CYBER-PHYSICAL SYSTEMS SUMMIT

IN RESPONSE TO THE CYBER CHALLENGE and building on its unique leadership position, Governor McAuliffe and the Commonwealth of Virginia, with the support of its partners, hosted the first-ever CPS Summit on September 20-22, 2016, at the Thomas Jefferson National Accelerator Facility in Newport News, Virginia. The goal of the summit was to position Virginia as a leader in CPS education and workforce development by bringing together CPS stakeholders and highlighting the state's assets, entrepreneurship, programs, and research, with the ultimate aim of achieving economic growth through new jobs, business development, and increased research funding. The agenda featured more than 35 speakers, including Governor McAuliffe and Senator Warner, and attracted more than 250 attendees (Cyber Virginia, 2016c).



PHOTO BY MICHAEL WHITE / GOVERNOR'S OFFICE

The summit convened CPS professionals to engage in roundtable, panel, and plenary sessions on the challenges and opportunities related to three cyber-physical vectors:

CYBER AUTONOMY

This vector addresses the intersection between cyber-physical systems and autonomy. Drawing on fields such as artificial intelligence and robotics, autonomous physical systems can determine courses of action and/or solve problems with little to no human involvement using various algorithms and/or software system architectures. Examples of autonomous systems include drones and driverless cars.

CYBER-INTERNET OF THINGS (IOT)

This vector addresses the intersection between cyber-physical systems and the IoT. The IoT refers to the network of interconnected physical devices embedded with electronics, software, sensors, and/or actuators that enable the collection and exchange of data. The IoT encompasses technologies such as intelligent transportation and smart cities.

CYBER-CRITICAL INFRASTRUCTURE

This vector addresses the intersection between cyber-physical systems and critical infrastructure. The Department of Homeland Security reports that the assets, systems, and networks of 16 sectors are so vital that their destruction or incapacitation would have a debilitating effect on national economic security, national public health or safety, and/or security. These sectors include the defense industrial base sector and the nuclear reactors, materials, and waste sector (U.S. Department of Homeland Security, 2016).



PHOTO BY MICHAEL WHITE / GOVERNOR'S OFFICE

On the first day, summit participants could participate in two sessions of roundtables on the summit's three cyber-physical vectors. Facilitated by BHEF and NGA, the roundtables were held in conjunction with Governor McAuliffe's NGA chair's initiative *Meet the Threat: States Confront the Cyber Challenge*, and findings were used to inform both the Virginia and NGA agendas for the next year. BHEF also distributed three case studies at the convening that highlighted successful CPS efforts in Virginia to help inform discussions.

The CPS Summit elicited wide-ranging, productive, and thoughtful discussions that highlighted Virginia's cyber assets, research, and programs. The discussions not only addressed challenges and opportunities in each vector but also resulted in recommendations, particularly related to education and workforce development. The consensus among summit participants was that Virginia is in a unique leadership role for the nation around CPS and should continue as well as build upon its current efforts, inspiring others to follow suit.

CHALLENGES AND OPPORTUNITIES IN CYBER-PHYSICAL SYSTEMS

CHALLENGES

Summit participants shared a variety of challenges and threats related to each cyber-physical vector. For example, in cyber-autonomy, the Consumer Technology Association estimates that 700,000 drones were sold in the United States alone in 2015 (Consumer Technology Association, 2015). The market for drones can be divided into three categories: professional commercial user, nonprofessional commercial user, and casual recreational user. Because they may not be aware of or trained in best practices for protection, the latter two users represent a major threat to the system as a whole.

Threats in the cyber-autonomy space can also be divided into three categories:

THREAT FROM THE PLATFORM.

The Federal Aviation Administration (FAA) reported that nearly 600 drones flew too close to airports and airplanes from August 22, 2015 to January 31, 2016 (Federal Aviation Administration, 2016). Furthermore, according to a review of 921 cases involving drones and manned aircraft from December 2013 to September 2015, Bard College reported that airplane pilots took evasive action to avoid flying into a drone 28 times (Bard College, 2015). These data demonstrate that users can now remotely control a potential attack surface, which presents a new cyber threat.

THREAT TO THE VEHICLE.

Autonomous vehicles still rely heavily on communications systems to transmit data and information as well as GPS devices to assist with navigation, both of which are highly vulnerable to remotely executed attacks.

THREAT TO THE USER.

When users download an app and/or software to interface with a drone, the amount of metadata shared through the interface is a black box to the user and poses a major vulnerability.

Regarding cyber-critical infrastructure, summit participants described several significant events that demonstrate the threats in this sector, including those from nation-states:

AURORA GENERATOR TEST. In 2007, the Idaho National Laboratory demonstrated how a cyber attack could physically destroy an electric grid. Using a computer program, the experiment rapidly opened and closed a diesel generator's circuit breakers out of sync with the rest of the grid, causing it to explode (YouTube, 2007).

SAUDI ARAMCO HACK. In 2012, Saudi Aramco, one of the world's largest oil companies, suffered the worst hack in world history. Within hours, 35,000 computers were partially wiped or completely destroyed, forcing the company to function without the internet until a newly secured computer network and expanded cybersecurity team were in place months later (Pagliery, 2015).

UKRAINE POWER GRID HACK. In 2015, more than 230,000 people lost power in the Ivano-Frankivsk region of Western Ukraine due to a suspected Russian hack. The hack was the first confirmed to take down a power grid (Zetter, 2016).

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER RANSOMWARE ATTACK. In 2016, Hollywood Presbyterian Medical Center became the first known hospital in the United States to be targeted with a ransomware attack. The hospital paid a \$17,000 ransom in bitcoin to obtain the decryption key and regain control

of the hospital's computer systems from the hacker (Winton, 2016). The attack demonstrated how important industrial control systems and supervisory control and data acquisition systems can be to maintaining operations in critical infrastructure sectors such as health care.



Ongoing challenges in cyber-critical infrastructure include increased vulnerability due to the IoT, private ownership of public assets, a lack of information sharing and individuals experienced in assessing or responding to cyber threats, and a lack of comprehensive security measures to address potential threats.

Gartner projects that 20.8 billion “things” within the IoT will be in use by 2020 (Van der Meulen, 2015). In a 2014 study, researchers from Hewlett Packard's Fortify on Demand division discovered that 6 out of 10 common IoT devices that provide user interfaces were vulnerable to a

range of issues, including persistent cross-site scripting vulnerabilities and weak credentials. In addition, 70% of devices used unencrypted network services, exposing their connections to cloud services and mobile apps to attacks, and 80% failed to require passwords of sufficient length or complexity. On average, the study identified 25 vulnerabilities per device (Hewlett Packard Enterprise, 2014).

Summit participants agreed that today's cybersecurity problems are not just a technology problem. These problems stem from the greatest, most complex IT infrastructure in the history of mankind, and the appetite for advanced technology is rapidly exceeding the ability to protect it. Summit participants emphasized that cyber operates “below the water line,” which means that people may be unaware of problems because they are not necessarily manifested in the physical world (e.g., system shuts down). However, the director of the NSA, General Keith Alexander, warned that cyberattacks are causing the “greatest transfer of wealth in history” and cited a McAfee estimate that the global cost of cybercrime is \$1 trillion, which is about a one-fourth of the nation's gross domestic product (Maas and Rajagopalan, 2012). The nation's innovation, investments, and military training, tactics, and technology are being stolen, which is a serious economic and national security issue. On a more personal level, acquired assets are being targeted through an aggregation of the personally identifiable information collected on individuals through IoT.

OPPORTUNITIES

Some major opportunities exist among the challenges and threats in CPS. In particular, the data collected through the IoT provide an information-rich environment that can be analyzed through the cloud. Cloud infrastructure allows for the analytics and computation of massive amounts of data simply and affordably without requiring a major capital acquisition. The cloud has the potential to enhance the nation's security capabilities and to address the increasingly complex issues stemming from the IoT. Summit participants also discussed the importance of partnerships at all levels to address the challenges in CPS and agreed that they could learn from and work together with other industries, universities, government agencies, as well as international partners to form solutions.



PHOTO BY MICHAEL WHITE / GOVERNOR'S OFFICE

Other topics discussed included improving communication between the IT and operational technology parts of an organization, the importance of a top-down approach to establish cybersecurity as a core organizational commitment, the need for a common language in cyber, the value of knowing one's network better than anyone else in order to protect it, and the emerging role of information sharing analysis centers and information sharing analysis organizations. In particular, summit participants recognized the importance of a cultural change in organizations to ensure that every member is aware of cyber's importance and effect on their daily activities and operations, thereby creating an environment wherein everyone is trained in good

cyber hygiene as well as equipped to identify and address cyber threats.

In addition, summit participants were encouraged to persuade policymakers that regulation is necessary to secure the IoT, including industrial control systems and supervisory control and data acquisition systems. Although there has been some progress with the issuance of standards for driverless cars by former Secretary of Transportation Foxx (U.S. Department of Transportation, 2016), policymakers still need to be convinced of the real threat to the cyber-physical world to benefit from investments in the necessary research and technology to ensure that cybersecurity is built into devices and products from the start.

Summit participants also shared recommendations for governors. As part of Governor McAuliffe's *Meet the Threat: States Confront the Cyber Challenge* initiative, NGA released a white paper with six recommendations in critical infrastructure:

1. **Work with other governors and lawmakers** to evaluate costs and benefits of regulation to determine whether regulations make sense.
2. **Institutionalize regular contacts between relevant officials and state utilities**, which will be critical in the event of a significant cyber incident.
3. **Audit existing rules and practices** to determine compliance and the need for additional standards.
4. **Focusing on resiliency**, because implementing strong cybersecurity in all utilities will take many years.
5. **Explore public-private partnerships** between state regulators and the private sector to leverage world-class expertise to ease the burden on state regulators in assessing utilities' compliance with security standards.
6. **Ensure that all stakeholders are involved** so that any statewide cybersecurity initiatives or plans account for all utilities. (National Governors Association, 2016)

CYBER AUTONOMY

At the same time, summit participants praised Virginia's current leadership in CPS, citing achievements in all three of the cyber-physical vectors. In cyber autonomy, summit participants highlighted the following examples:

MID-ATLANTIC AVIATION PARTNERSHIP (MAAP). Virginia Tech was selected by the FAA to be one of six unmanned aircraft systems research and test site operators across the country. Formed in 2013, the MAAP makes Virginia a world leader in the field of unmanned systems (Virginia Polytechnic and State University, 2017b).

FIRST FAA-APPROVED DRONE DELIVERY. Virginia is home to the first official drone package delivery of medical supplies in the country—completed with the assistance of Virginia Tech. Conducted in July 2015, the delivery is considered a milestone flight (Vanian, 2015).

CHIPOTLE DRONE DELIVERY TESTING. Virginia Tech has collaborated with Google to test drone deliveries of Chipotle burritos. In September 2016, Project Wing from Google's X lab began testing drone deliveries, and resulting data and information will be used to improve drone operations and expand drone use (Addady, 2016).

CYBER-CRITICAL INFRASTRUCTURE

In cyber-critical infrastructure, summit participants highlighted Virginia's "all-hazards" approach to disaster preparedness. A primary mission of the Office of the Secretary of Public Safety and Homeland Security is to maintain the security and resilience of Virginia's critical infrastructure, and central to this effort is Virginia's ability to collaborate with critical infrastructure owners and operators. Virginia has made several significant strides in realizing this mission:

VIRGINIA FUSION CENTER (VFC). The VFC serves as Virginia's focal point for the analysis, collection, dissemination, and receipt of timely and actionable threat intelligence between the federal government and local, private-sector, and state partners. The VFC produced 43 products related to potential cyber threats and cybersecurity in 2014, and hired four additional employees with funding from the Virginia General Assembly in 2016 (Virginia Fusion Center, 2016).

SECURE COMMONWEALTH PANEL (SCP). Composed of 33 members, the SCP is an advisory board in the executive branch of state government. The SCP monitors and assesses the implementation of statewide prevention, preparedness, response, and recovery initiatives and, where necessary, reviews, evaluates, and makes recommendations relating to the emergency preparedness of all levels of government in Virginia. Additionally, the SCP facilitates cabinet-level coordination among the various state government agencies related to emergency preparedness and facilitates private-sector preparedness and communication (Secretary of Public Safety and Homeland Security, 2016).

VIRGINIA NATIONAL GUARD. In partnership with the Virginia National Guard's Data Processing Unit, Virginia is using local assets to strengthen the state's cyber infrastructure. Thus far, the partnership has conducted cyber assessments on infrastructure within at least five localities to identify gaps or opportunities to increase Virginia's cyber resilience, and expects to conduct several more in the future (Virginia National Guard, 2016).

CYBER ENTREPRENEURSHIP AND INNOVATION

Summit participants also highlighted Virginia's support for entrepreneurship and innovation to address the next generation of security needs from the rise of IoT devices:

CENTER FOR INNOVATIVE TECHNOLOGY (CIT). Headquartered in Herndon, Virginia, CIT is a nonprofit that is focused on creating technology-based economic development strategies to advance innovation and the next generation of technology companies (Center for Innovative Technology, 2017a). CIT created a web-based portal called the Commonwealth Innovation and Entrepreneurship Measurement Systems that tracks the performance of Virginia startup companies, lowering the barriers of engagement for interested investors and other stakeholders (Center for Innovative Technology, 2017c).

MACH37 ACCELERATOR. Founded by Virginia's CIT and funded by the Virginia General Assembly, Mach37 Accelerator is an intensive 90-day program created to launch cyber startups. It is designed to facilitate creation of next generation cybersecurity product companies with an emphasis on

validation of product ideas and relationship development to produce an initial customer base and investment capital. Since April 2016, Mach37 Accelerator has had two private-sector investors, General Dynamics Mission Systems and Amazon Web Services, and has graduated 35 new cyber companies (MACH37 Cyber Accelerator, 2016).

COMMONWEALTH RESEARCH AND COMMERCIALIZATION FUND (CRCF).

The CRCF advances solutions to critical state, national, and international problems through technology research, development, and commercialization, thereby moving Virginia's economic growth and innovation forward. For FY2017, CRCF had a \$2.8 million solicitation (Center for Innovative Technology, 2017b).

Throughout the discussions, summit participants acknowledged the critical need for education and workforce development in CPS to address the challenges and opportunities across all three cyber-physical vectors. The final section below provides highlights, and particularly recommendations, from those discussions.



PHOTO BY MICHAEL WHITE / GOVERNOR'S OFFICE



PHOTO BY MICHAEL WHITE / GOVERNOR'S OFFICE

EDUCATION AND WORKFORCE DEVELOPMENT IN CYBER-PHYSICAL SYSTEMS

BACKGROUND

The demand for cyber and the use of data science and analytics (DSA) and artificial intelligence (AI) are expanding throughout government, non-profits, and business. However, current talent development models cannot meet those demands, relying on poaching rather than on developing new talent. In addition, research in leading-edge fields, including cyber, DSA, and AI, are inadequate for addressing long-term challenges.

Nevertheless, Computing Research Association survey data reveal certain positive trends that can help address these talent needs if smartly calibrated strategies and tactics are used (Zweben and Bizot, 2016). Many computer science and computer engineering students are not currently exposed to cyber and DSA, which presents an opportunity to introduce new skills. Additionally, an explosion of enrollments among majors and non-majors results in new talent but may exclude non-majors from popular courses (e.g., AI and machine learning). Lastly, non-majors in computer science courses increase the diversity of relevant skills (cyber, DSA, AI, and T-shaped), the diversity of perspectives (non-STEM majors from a range of disciplines), and the diversity of backgrounds (socioeconomic status, gender, race and ethnicity).

K-12 EDUCATION

Summit participants discussed the importance of beginning the pipeline for cyber early. Summit participants encouraged the use of incentives as early as K-12 to increase the awareness of underrepresented groups, such as women and minorities, of cyber and/or STEM. Summit participants also suggested leveraging the IoT to raise awareness of the IoT among K-12 students by creating targeted advertisements through social networks.

Summit participants suggested requiring a cyber-related course, just like a math or English course, in K-12 education. For example, schools could make computer science a requirement and/or dedicate a period to cyber topics, such as cyber hygiene, and complementary skills such as communication and teamwork. Summit participants emphasized the importance of including internet security in the curriculum, adding that teachers must be well-versed in cyber to implement such a curriculum.

Summit participants highlighted the following best practices in K-12 education:

CYBERPATRIOT. This National Youth Cyber Education Program is centered on the National Youth Cyber Defense Competition. Teams of middle and high school students assume the position of newly hired IT professionals responsible for managing the network of a small company. In a series of rounds, teams receive virtual images of operating systems and look for cybersecurity vulnerabilities, simultaneously hardening the system while maintaining critical services over the course of six hours. The top teams advance to the National Finals Competition in Baltimore, Maryland, for the opportunity to earn national recognition and scholarship money. In 2016, about 3,300 schools and 15,000-20,000 students participated (Air Force Association, 2017).

HAWAII STATE DEPARTMENT OF EDUCATION'S STEM INTEGRATION IN K-12 EDUCATION. To prepare students for the 21st century global economy, the Hawaii State Department of Education is purposefully integrating STEM into K-12 education. The goals are to increase the number of STEM teachers, provide students with a solid STEM foundation, increase the number of public school graduates who pursue STEM either

academically or professionally, especially those from underrepresented backgrounds, and cultivate community partnerships for access to diverse, high-quality STEM opportunities (Hawaii State Department of Education, 2016).

VERIZON WIRELESS FOUNDATION'S MINORITY MALE MAKERS PROGRAM. The Verizon Wireless Foundation is collaborating with historically black colleges and universities (HBCUs) to recruit rising minority seventh- and eighth-grade male students from surrounding communities into a STEM training program on HBCU campuses. In summer 2015, Verizon collaborated with four HBCUs (Jackson State University, Kentucky State University, Morgan State University, and North Carolina A&T University) to train more than 700 minority, middle school males (Lewis, 2015).

JUNIOR ACHIEVEMENT. This program is a volunteer-delivered, K-12 program that fosters entrepreneurship, financial literacy, and work-readiness skills as well as uses experiential learning to inspire and prepare students for success in a global economy. The program serves more than 4.8 million students per year in 209,651 classrooms and after-school locations and is a model for teaching basic skills such as cyber (Junior Achievement USA, 2016).

HIGHER EDUCATION

Regarding higher education, summit participants emphasized the importance of exposing non-cyber students to cyber through a related course before graduation, including combining cyber education with privacy education (e.g., privacy engineering) or teaching technology and ethics. They suggested several best practices such as new programs or degrees, internships, scholarships, and key partnerships to ensure that cyber is included as part of the overall experience. For example, students could gain early exposure to the field through an internship in the fall of the freshman or sophomore year. Students may also benefit from IoT user training (e.g., IoT developer, IoT designer) throughout the pipeline, more cross-pollination of different fields, and, given the fast pace of change in cyber, a focus on hands-on classes to accelerate the pace of learning. Summit participants shared the desire for every engineering student, especially at the undergraduate level regardless of major, to learn about security in addition to timing and performance.

Summit participants highlighted the following best practices in higher education:

ADVANCED CYBERSECURITY EXPERIENCE FOR STUDENTS (ACES) PROGRAM. Offered by the University of Maryland Honors College, the ACES program is the first and only honors undergraduate program in cybersecurity. With the help and support of its partners, such as Northrop Grumman and BHEF, the program was launched in fall 2013 and includes a living-learning program for freshman and sophomores as well as an advanced minor for juniors and seniors (University of Maryland Honors College, 2016).

GEORGE MASON UNIVERSITY BACHELOR'S DEGREE IN CYBERSECURITY ENGINEERING. Among many other cyber-related programs, GMU offers a bachelor's degree in cybersecurity engineering to teach students how to build cyber resilient systems, which include physical as well as computer and network systems (George Mason University, 2017). In two years, the program has increased enrollment to a total of more than 180 students and serves as a model for other programs in this area.

VIRGINIA TECH INTEGRATED SECURITY DESTINATION AREA. Currently in development, one of Virginia Tech's five Destination Areas is Integrated Security, which is focused on advancing and assuring the security of the country's social, political, and financial networks while balancing the needs and expectations of governmental oversight and privacy. Transdisciplinary teams will support these Destination Areas through research, education, and engagement, enabling Virginia Tech to become an international destination for talent, partnership, knowledge, and outcomes (Virginia Polytechnic Institute and State University, 2017a).

NORTHROP GRUMMAN'S COOPERATIVE EDUCATION OPPORTUNITY (CO-OP). Northrop Grumman provides a co-op that combines academic and work experience. Students engage in a structured learning system where they alternate between working at Northrop Grumman and taking classes, and simultaneously receive college credit and work experience (Northrop Grumman Corporation, 2016).

NATIONAL SECURITY AGENCY

COOPERATIVE EDUCATION PROGRAM. This program rotates students between alternating semesters of full-time co-op work and study until graduation. Students are required to complete a minimum of 52 weeks of the co-op, and the work experiences are designed to expose students to potential future career paths (National Security Agency, 2016).

CYBERCORPS: SCHOLARSHIP FOR

SERVICE (SFS). CyberCorps: SFS is intended to increase and strengthen the talent in federal information assurance that protects the government's critical information infrastructure. Funded through grants awarded by the NSF, this program provides scholarships to full-time students attending a participating institution, including tuition and education and related fees. Stipends of \$22,500 for undergraduate students and \$34,000 for graduate students are also provided (U.S. Office of Personnel Management, 2016).

THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION (NRECA) HIGHER EDUCATION PARTNERSHIPS.

Although not focused on cyber, NRECA has established several key higher education partnerships, including one with Carnegie Mellon University, that serve as an example for other organizations interested in building strong and mutually beneficial relationships with higher education (America's Electric Cooperatives, 2016).

BUSINESS-HIGHER EDUCATION FORUM'S STRATEGIC BUSINESS ENGAGEMENT

MODEL. BHEF's Strategic Business Engagement Model serves as the foundation for building successful partnerships between

business and higher education. This model moves the two sectors from transactional relationships to strategic partnerships through five strategies: engage corporate leadership; focus corporate philanthropy on undergraduate education; identify and tap core competencies and expertise; facilitate and encourage employee, faculty, and staff engagement; and expand the focus of funded research to include undergraduate education (Business-Higher Education Forum, 2016).

Summit participants also believe that higher education is ripe for innovation. Although 4-year programs may be suitable for traditional, 18- to 22-year-old students, at least 73% of students are now nontraditional (Choy, 2002). In addition, while higher education has a defined endpoint, the nation needs people who are eager to take the next step in their learning due to the rapid pace of technological change. In response, summit participants suggested that students should have the option to pay a set amount for education that could continue for a longer time period (e.g., 20 years or more), ensuring ongoing learning opportunities to mid-career adults that could be supported by both the public and private sector. Training programs such as Silicon Valley bootcamps as well as certifications should also be considered. Summit participants also emphasized the need to resume discussion and dialogue between higher education and the states. They suggested that governors invest in personnel across the country, providing a mix of academic and hands-on, real-world opportunities to build a culture of continuous learning beyond the traditional higher education system of credentials (e.g., four-year programs).

WORKFORCE DEVELOPMENT

Summit participants discussed expanding the description of a cyber-professional to include not only technical cyber skills but also communication, teamwork, and critical thinking skills. These skills characterize T-shaped professionals who possess both deep disciplinary knowledge as well as an ability to collaborate across disciplines. Given the rapid pace of change in cyber, summit participants did not identify a baseline skill for cyber, considering it a moving target. However, they identified a variety of desired skills including AI, big data, biometrics, communication, critical thinking, data governance, design thinking, systems thinking, and an understanding of rule sets and system of systems. They emphasized the importance of creating teams whereby each member could contribute different skills, as necessary.

To expand the workforce with this depth and breadth of skills, summit participants suggested utilizing existing professionals to cross-train them in cyber (e.g., cross-pollination with specialists) and providing cyber training for a company's functional areas (e.g., human resources case studies and exercises, public relations communication module). They encouraged companies to combine the IT and OT parts of their business and to train IT for cyber. They specified health care as an industry needing a combination of both IT and bio. Summit participants described the potential for training individuals with liberal arts backgrounds who may apply different perspectives or approaches to problems than those trained in traditional cyber-related fields. Educating not only the IT staff but also the business staff on cybersecurity and building a common language to address cybersecurity issues throughout the development lifecycle is critical.

Summit participants highlighted the following best practices in workforce development:

INTELLIGENCE AND NATIONAL SECURITY SUMMIT.

The third annual Intelligence and National Security Summit provided participants with opportunities to discuss workforce management, how the cyber world was changing, and the need for talent to quickly adapt to changes (AFCEA International and the Intelligence and National Security Alliance, 2016).

TIDEWATER COMMUNITY COLLEGE

APPRENTICESHIP INSTITUTE. The institute serves as an example for organizations interested in an apprenticeship model. The institute works with Hampton Roads employers to tailor apprenticeship programs based on desired workforce outcomes. In

Virginia, apprentices receive an average starting salary of \$50,000, and the apprenticeship model provides an efficient pathway to meet demand for the 550,000 new Virginia jobs that are expected to require advanced training and postsecondary education by 2022 (Tidewater Community College, 2016).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBERSECURITY FRAMEWORK.

In response to Executive Order 13636 in 2013, Improving Critical Infrastructure Cybersecurity, NIST worked with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. Created in collaboration with industry and government, the framework consists of standards, guidelines, and practices to protect critical infrastructure, and its approach helps owners and

operators of critical infrastructure manage cybersecurity-related risk (National Institute of Standards and Technology, 2017).

TECHHIRE. An initiative powered by Opportunity@Work in partnership with the Department of Education, TechHire builds tech talent pipelines in communities across the country and provides an alternative pathway that successfully targets underrepresented populations. For example, \$150 million dollars in Department of Labor TechHire grants were used to support 39 public-private partnerships for workforce training, providing workers with a pathway to the middle class and employers with the skilled workers needed. In particular, \$24 million went to partnerships that help disadvantaged groups overcome barriers to

employment, including people with criminal records, disabilities, or limited English proficiency as well as veterans (The White House, 2016b).

COLUMBUS COLLABORATORY. The Columbus Collaboratory consists of seven cross-industry founding member companies and public and private partners focused on delivering rapid innovation in the areas of advanced analytics and cybersecurity. By working collaboratively on common complex challenges, it develops solutions that transcend industries, enhance operational efficiencies, and improve customer service. In doing so, it is also expanding and upskilling the IT workforce in Columbus, Ohio (Columbus Collaboratory, 2017).

GIVEN ITS CURRENT CYBER ACHIEVEMENTS, assets, investments, and initiatives, Virginia plays a unique leadership role in cyber, and the recommendations following will further inform the state's approach to advancing cyber education and workforce development.

THE WAY FORWARD

TO MOVE FORWARD IN CYBER-PHYSICAL SYSTEMS, BHEF and NGA recommend that Virginia continue as well as build on its current efforts in the following areas:



ESTABLISH CPS AS A TOP PRIORITY

CPS must remain a priority to ensure critical actions such as advancements in research, investments in technology, and implementation of standards and regulations for national and economic security. All people and organizations are vulnerable to cyber threats, and therefore should prioritize strategies and changes in culture, practice, and/or policy to mitigate threats and protect those at risk. Governor McAuliffe's and Senator Warner's state and federal leadership for Virginia, respectively, are prime examples of the accomplishments and successes that can result when CPS is made a top priority.



ALIGN THE EDUCATIONAL SYSTEM WITH WORKFORCE NEEDS

The demand for skilled CPS workers is high both nationally and in the state of Virginia. To address the CPS challenges, the educational system must align with workforce needs, providing the skilled workers necessary to meet the continually growing demands in this field. In turn, employers must recognize and respond to new talent sources as they develop. Virginia has already made significant strides to align its educational system and workforce needs, and by continuing to do so is solidifying its leadership position in CPS.

CAPITALIZING ON ITS ASSETS AND LEADERSHIP

in innovation and technology, Virginia is creating a thriving cyber ecosystem that other states and nations can follow. By continuing as well as building on its current efforts, Virginia will move forward as a national leader in cyber and, in turn, will inspire others to follow suit.



BUILD PARTNERSHIPS AT ALL LEVELS AND IN ALL SECTORS

Addressing the CPS challenges requires a team effort. Partnerships at all levels (e.g., local, regional, national, and international) and among all sectors (e.g., academia, public, private, and nonprofits) are critical. These partnerships should encourage transparency and information sharing, including best practices and resources, as well as collaboration to produce the best solutions. Virginia is establishing key partnerships, building a base of knowledge and experience that it can share, and contributing to larger efforts in the field.



FOSTER ENTREPRENEURSHIP AND INNOVATION

An effective response to the rapid pace of change in CPS is predicated on an environment of constant innovation. Virginia's achievements in this area are highlighted in the 2016 report *Virginia's Innovation Ecosystem: The Trusted Leader in Growing Cyber Security Solutions* (Cyber Virginia, 2016g). By establishing a nurturing environment for entrepreneurship and innovation, Virginia serves as a home for next generation solutions, allowing for quick and efficient responses to change.

REFERENCES

- Addady, M. (2016). *Chipotle is Delivering Burritos by Drone at This College Campus*. Fortune. <http://fortune.com/2016/09/09/chipotle-alphabet-drone-burrito>
- AFCEA International and the Intelligence and National Security Alliance. (2016). *Intelligence & National Security Summit*. <http://events.jspargo.com/inss16/public/enter.aspx>
- Air Force Association. (2017). *CyberPatriot: The National Youth Cyber Education Program*. <https://www.uscyberpatriot.org>
- AlexandriaNews. (2017). *Governor McAuliffe Announces Cyber Vets Virginia Training Initiative Partnership with SANS Institute's VetSuccess Academy*. <http://www.alexandrianews.org/2017/01/governor-mcauliffe-announces-cyber-vets-virginia-training-initiative-partnership-with-sans-institutes-vetsuccess-academy>
- America's Electric Cooperatives. (2016). *NRECA Wins DOE Grant to Advance Cybersecurity Solution to Market*. <http://www.electric.coop/nreca-wins-doe-grant-advance-cybersecurity-solution-market>
- Burning Glass Technologies. (2015). *Report on Cybersecurity Jobs in Virginia and the DMV*. [PowerPoint slides].
- Burning Glass Technologies. (2016). *Report on Cybersecurity Jobs in Virginia and the DMV*. [PowerPoint slides].
- Business-Higher Education Forum. (2016). *Build Partnerships*. <http://www.bhef.com/our-work/build-partnerships>
- Center for Innovative Technology. (2017a). *Center for Innovative Technology*. <http://www.cit.org/>
- Center for Innovative Technology. (2017b). *Commonwealth Research and Commercialization Fund*. <http://www.cit.org/initiatives/crcf>
- Center for Innovative Technology. (2017c). *Commonwealth Innovation and Entrepreneurship Measurement System*. <http://www.cit.org/initiatives/iems/measurement-system>
- Choy, S. (2002). *Nontraditional Undergraduates*. NCES. <https://nces.ed.gov/pubs2002/2002012.pdf>
- Columbus Collaboratory. (2017). <http://columbuscollaboratory.com>
- Commonwealth of Virginia Office of the Governor. (2014). *Executive Order Number Eight: Launching "Cyber Virginia" and the Virginia Cyber Security Commission*. <https://governor.virginia.gov/media/3330/eo-8-launching-cyber-virginia-and-the-virginia-cyber-security-commission.pdf>
- CompTIA. (2015). *Cyberstates 2015*. <https://www.comptia.org/resources/cyberstates-15?tracking=resources/2015-cyberstates>
- Consumer Technology Association. (2015). *New Tech to Drive CE Industry Growth in 2015, Projects CEA's Midyear Sales and Forecasts Report*. <https://www.cta.tech/News/Press-Releases/2015/July/New-Tech-to-Drive-CE-Industry-Growth-in-2015-Proj.aspx>
- Coy, B. (2016a). *Governor McAuliffe Announces Expansion of Cybersecurity Apprenticeships*. <http://governor.virginia.gov/newsroom/newsarticle?articleId=15727>
- Cyber Seek. (2016). *Cybersecurity Supply/Demand Heat Map*. <http://cyberseek.org/heatmap.html>
- Cyber Virginia. (2015a). *Commonwealth Conference on Cyber and Education 2015*. <http://cyberva.virginia.gov/cce2015>
- Cyber Virginia. (2015b). *Commonwealth of Virginia Cybersecurity Commission: First Report, August 2015*. <http://technology.virginia.gov/media/4396/cyber-commission-report-final.pdf>
- Cyber Virginia. (2016a). *Cyber Commission Final Report*. <http://cyberva.virginia.gov/media/8139/cyber-commission-final-report.pdf>
- Cyber Virginia. (2016b). *Cyber Initiatives Included in the 2017-18 Budget Bill*. <http://cyberva.virginia.gov>
- Cyber Virginia. (2016c). *Cyber-Physical Systems Summit*. <https://cyberva.virginia.gov/cyber-physical-summit>
- Cyber Virginia. (2016d). *Cyber Vigilance: The Virginia Way*. http://cyberva.virginia.gov/media/8138/cyber_12-2-16.pdf
- Cyber Virginia. (2016e). *Cyber Security Information Portal*. <https://cyberva.virginia.gov/portal>
- Cyber Virginia. (2016f). *Virginia's Cyber Security Approach: Leadership Through Diversity*. https://cyberva.virginia.gov/media/6424/virginiacybersecurity_printfinal-83116.pdf
- Cyber Virginia. (2016g). *Virginia's Innovation Eco-System: The Trusted Leader in Growing Cyber Security Solutions*. <https://cyberva.virginia.gov/media/2163/cyberreport.pdf>
- Cyber Virginia. (2017). *Commonwealth Cyber Fusion 2017*. <http://cyberfusion.virginia.gov/>
- Federal Aviation Administration. (2016). *UAS Sightings Report*. https://www.faa.gov/uas/resources/uas_sightings_report
- GenCyber. (2017). *Inspiring the Next Generation of Cyber Stars*. <https://www.gen-cyber.com>
- George Mason University. (2017). *Cyber Security Engineering, BS*. <https://volgenau.gmu.edu/program/view/20490>
- Hawaii State Department of Education. (2016). *Science, Technology, Engineering & Math (STEM)*. <http://www.hawaiipublicschools.org/TeachingAndLearning/StudentLearning/Stem/Pages/home.aspx>
- Hewlett Packard Enterprise. (2014). *Internet of Things Research Study*. <http://go.saas.hpe.com/fod/internet-of-things>

- HPN News Desk. (2016). *Virginia Tech Awarded \$20 Million Grant for Cyber Workforce Development*. <https://homelandprepnews.com/government/19417-virginia-tech-awarded-20-million-grant-cyber-workforce-development>
- International System Security Certification Consortium, Inc. (2016). <https://www.isc2.org>
- Junior Achievement USA. (2016). <https://www.juniorachievement.org/web/ja-usa/home>
- Lewis, T. (2015). *Minority Male Makers: Verizon Invests in STEM Education for Minority Boys*. <http://www.verizon.com/about/news/minority-male-makers-verizon-invests-in-stem-education-for-minority-boys>
- LifeJourney, Inc. (2017). *National Security Agency Day of Cyber*. <https://nsadayofcyber.com>
- Llovio, L. (2016). *Governor Signs Legislation to Make Computer Science Part of SOL Curriculum*. *Richmond-Times Dispatch*. http://www.richmond.com/news/local/education/districts/article_36fel085-9da0-59f5-b3d0-732a5ada5eb1.html
- Maas, P., and Rajagopalan, M. (2012). *Does Cybercrime Really Cost \$1 Trillion?* ProPublica. <https://www.propublica.org/article/does-cybercrime-really-cost-1-trillion>
- MACH37 Cyber Accelerator. (2016). <https://www.mach37.com>
- Mather, E.T. (2016). *UVA Computer Scientists Win \$1 Million in National Cybersecurity Challenge*. <https://www.news.virginia.edu/content/uva-computer-scientists-win-1-million-national-cybersecurity-challenge>
- McAuliffe, T. (2015). *Governor McAuliffe Announces Virginia Air National Guard to Stand Up New Cyber Unit*. <http://governor.virginia.gov/newsroom/newsarticle?articleId=13673>
- National Contract Management Association and Bloomberg Government. (2015). *Annual Review of Government Contracting 2015 edition*. <http://www.ncmahq.org/docs/default-source/default-document-library/pdfs/exec15---ncma-annual-review-of-government-contracting-2015-edition>
- National Governors Association. (2016). *Cybersecurity and Critical Infrastructure*. Meet the Threat: States Confront the Cyber Challenge. <https://ci.nga.org/files/live/sites/ci/files/1617/docs/1610CybersecurityCriticalInfrastructure.pdf>
- National Governors Association. (2017a). *Meet the Threat: States Confront the Cyber Challenge*. <https://ci.nga.org/cms/home/ci1617/index.html>
- National Governors Association. (2017b). *NGA Winter Meeting Shines Spotlight on Bipartisanship, Governors' Priorities*. <https://www.nga.org/cms/home/news-room/news-releases/2017--news/col2-content/nga-winter-meeting-shines-spotli.html>
- National Institute of Standards and Technology. (2017). *Cybersecurity Framework*. <https://www.nist.gov/cyberframework>
- National Security Agency. (2016). *Cooperative Education Program*. <https://www.intelligencecareers.gov/icstudents.html?Agency=NSA>
- Northrop Grumman Corporation. (2016). *Cooperative Education*. <http://www.northropgrumman.com/Careers/StudentsAndNewGrads/Pages/CooperativeEducation.aspx>
- Pagliery, J. (2015). *The Inside Story of the Biggest Hack in History*. CNN. <http://money.cnn.com/2015/08/05/technology/aramco-hack>
- Secretary of Commerce and Trade. (2014). *New Virginia Economy*. <https://commerce.virginia.gov/media/3501/new-virginia-economy-12052014.pdf>
- Secretary of Public Safety and Homeland Security. (2016). *Secure Commonwealth Panel*. <https://pshs.virginia.gov/initiatives/secure-commonwealth-panel>
- Sorcher, S. (2015). *The Race to Build the Silicon Valley of Cybersecurity*. <http://passcode.csmonitor.com/goldrush>
- Spidaleri, F. (2015). *State of the States on Cybersecurity*. Pell Center for International Relations and Public Policy at Salve Regina University. <http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf>
- State Council of Higher Education for Virginia. (2016). *New Economy Workforce Credential Grant*. <http://www.schev.edu/index/institutional/grants/workforce-credential-grant>
- TechAmerica Foundation. (2011). *Cyberstates 2011: The Definitive State-by-State Analysis of the U.S. High-Tech Industry*. <http://www.techamericafoundation.org/cyberstates>
- Telos Corporation. (2016). *Telos and Amazon Web Services (AWS): Accelerating Secure and Compliant Cloud Deployments*. Ashburn, VA. <https://www.telos.com/assets/Telos-AWS-white-paper.pdf>
- The Information Assurance Directorate. (2016). *NSA/DHS Current National CAE Designated Institutions*. https://www.iad.gov/nietp/reports/current_cae_designated_institutions.cfm
- The White House. (2016a). *Fact Sheet: Cybersecurity National Action Plan*. <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>
- The White House. (2016b). *TechHire Initiative*. <https://www.whitehouse.gov/issues/technology/techhire>
- Tidewater Community College. (2016). *TCC Apprenticeship Institute*. <https://www.tcc.edu/about-tcc/apprenticeship-institute>
- University of Maryland Honors College. (2016). *Advanced Cybersecurity Experience for Students*. <http://www.aces.umd.edu/>
- U.S. Department of Homeland Security. (2016). *Critical Infrastructure Sectors*. <https://www.dhs.gov/critical-infrastructure-sectors>
- U.S. Department of Transportation. (2016). *Federal Automated Vehicles Policy*. <https://www.transportation.gov/AV>

REFERENCES

- U.S. Office of Personnel Management. (2016). *CyberCorps: Scholarship for Service*. <https://www.sfs.opm.gov>
- Van der Meulen, R. (2015). *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent from 2015*. Gartner, Inc. <http://www.gartner.com/newsroom/id/3165317>
- Vanian, J. (2015). *Drone Makes First Legal Doorstep Delivery in Milestone Flight*. Fortune. <http://fortune.com/2015/07/17/faa-drone-delivery-amazon>
- Virginia Cyber Range. (2016). *Virginia Cyber Range*. <https://virginiacyberrange.org>
- Virginia Department of Education. (2016). *Virginia's 21st Century Career Pathway: Cybersecurity*. http://www.doe.virginia.gov/administrators/superintendents_memos/2016/040-16a.pdf
- Virginia Department of Education. (2017). *Governor's STEM Academies*. http://www.doe.virginia.gov/instruction/career_technical/gov_academies
- Virginia Economic Development Partnership. (2014). *Virginia Advantages: Aerospace*. <http://www.yesvirginia.org/Content/pdf/Industry%20Profiles/VA%20Aerospace%20Profile%202014.pdf>
- Virginia Economic Development Partnership. (2016). *Virginia's Cybersecurity Industry*. <http://www.yesvirginia.org/content/pdf/industry%20profiles/va%20cybersecurity%20summary%202016.pdf>
- Virginia Fusion Center. (2016). *Virginia Fusion Center*. <http://www.vsp.state.va.us/FusionCenter>
- Virginia Information Technologies Agency. (2016). *Security*. <https://www.vita.virginia.gov/security>
- Virginia National Guard. (2016). *Data Processing Unit*. <http://vanguard.dodlive.mil/category/armyguard/91sttc/data-processing-unit>
- Virginia Polytechnic Institute and State University. (2017a). *Integrated Security*. <http://provost.vt.edu/destination-areas/da-security.html>
- Virginia Polytechnic Institute and State University. (2017b). *Mid-Atlantic Aviation Partnership*. <https://www.maap.ictas.vt.edu>
- Virginia Space Grant Consortium. (2016). *STEM Takes Flight at Virginia's Community Colleges*. <http://www.vsgc.odu.edu/STEMtakesFlight>
- Warner, M.R. (2016). *Warner, Rounds, Beyer, Wittman Act to Encourage Competition & Innovation in DoD Cyber Procurement*. http://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=A4D27777-C176-4924-970A-C72128D00A60
- Winton, R. (2016). *Hollywood Hospital Pays \$17,000 in Bitcoin to Hackers; FBI Investigating*. Los Angeles Times. <http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html>
- YouTube. (2007). *Staged Cyber Attack Reveals Vulnerability in Power Grid*. Frgrd.com. <https://www.youtube.com/watch?v=fJyWngDco3g>
- Zetter, K. (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid>
- Zweben, S., and Bizot, B. (2016). *2015 Taulbee Survey: Continued Booming Undergraduate CS Enrollment; Doctoral Degree Production Dips Slightly*. <http://cra.org/wp-content/uploads/2016/05/2015-Taulbee-Survey.pdf>



CYBERVIRGINIA

P.O. Box 1475
p: 804.786.2211

Richmond, VA 23218
cyberva.virginia.gov



Creating Solutions. Inspiring Action.

© 2017 Business-Higher Education Forum / 2025 M Street NW, Suite 800 / Washington, DC 20036
p: 202.367.1189 / info@bhef.com / www.bhef.com