2015 VASEM SUMMIT REPORT

VOLUME 2 **UNMANNED AERIAL SYSTEMS**

VIRGINIA ACADEMY OF SCIENCE, ENGINEERING, AND MEDICINE

VASEM

CONTENTS

Introduction from the Secretary of Technology 3

UAS Leadership at Sinclair College 4

Cybersecurity for UAS Systems 6

UAS Regulations 8

Research and Industry Incentives for UAS Development 10

Cover photo: Sinclair College
Back cover photo: Jim Stroup

PHOTO: SINCLAIR COLLEGE

MESSAGE FROM THE SECRETARY OF TECHNOLOGY

This is really an exciting moment for technology in the Commonwealth. We are pursuing breakthroughs in a score of fields that have the potential to dramatically improve the quality of life our citizens enjoy. Among them are data analytics, autonomous systems, and cybersecurity. The obstacles are daunting, but the potential rewards are enormous.

The challenges we face in each of these fields are complex, but they are also interrelated. We will not be successful if we pursue them in isolation. The role of my Secretariat is to identify points of intersection, to encourage the relevant stakeholders—industry, academia, as well as government—to join together on common ground, and to work with them to develop a comprehensive strategy.

This approach has already yielded a number of significant successes. In July 2015 Flirtey, Inc., NASA's Langley Research Center, and the Mid-Atlantic Aviation Partnership anchored the team that accomplished the first FAA-approved research package delivery in the nation. And I can testify, having ridden in Virginia Tech Transportation Institute's automated car that the Commonwealth is well positioned to pioneer new forms of safer, more efficient transportation.

That is why I was pleased to speak at the annual VASEM meeting. The caliber and range of expertise VASEM brings to bear topics such as the future of the autonomous systems and cybersecurity is unparalleled. Looking forward, we foresee it playing an integral role in providing authoritative, nonpartisan insight on a wide variety of technological matters.

Sincerely,

Karen R. Jackson
Secretary of Technology

PHOTO: SINCLAIR COLLEGE

UAS LEADERSHIP AT SINCLAIR COLLEGE: NATIONAL UAS TRAINING AND CERTIFICATION CENTER

ANDREW SHEPHERD

Less than 10 years ago, the leadership of Sinclair College in Dayton, Ohio, realized the college had an opportunity to secure a leading position in the quickly emerging field of unmanned aerial systems (UAS) by building on its highly regarded aviation program. Andrew Shepherd, the school's director of unmanned aerial systems, described how Sinclair has moved aggressively in the interim to put itself at the forefront of UAS training. "We set our sights on establishing a national center for UAS training and certification at Sinclair," Shepherd said. "We have made considerable progress in reaching that goal."

Shepherd set the stage for describing these efforts by spotlighting Sinclair. Founded in 1887 by David Sinclair, it is the oldest two-year college still in operation in the United States. Sinclair enrolls 24,000 for-credit students and trains another 13,000 to 14,000 noncredit students annually. It offered its first aviation course in 1911 and has had a formal aviation technology programs for several decades.

In 2008, Sinclair began exploring the development of UAS programs, and in 2013, its Board of Trustees authorized $1.4 million to support their expansion. Total internal investment to date, Shepherd calculated, is more than $5.5 million, and its UAS initiatives have attracted an additional $4 million in state funding.

In August 2015, Sinclair opened the 28,000-square-foot National UAS Training and Certification Center in downtown Dayton. The Center is colocated with Sinclair's manned pilot, flight dispatcher, flight attendant, and aircraft airframe and powerplant mechanic programs, allowing Sinclair to leverage synergies with them. "Students can design their own airfoils and system components, manufacture them using our CNC machines and 3D printers, and test them in the wind tunnel," Shepherd said. Students fly their designs and training systems in Sinclair's 35,000-square-foot UAS Indoor Flight Range, which doubles as the school's field house, and its dedicated UAS Indoor Flying Pavilion, a 3,200-square-foot facility with indoor GPS access that opened in December 2015.

The strategic framework that Sinclair developed for its National UAS Training and Certification Center determines how these facilities are used to support training and applied research activities. Conceptually, the center is built on three pillars—airspace, curriculum, and modeling and simulation—all supported by data analytics capabilities.

"Because we are a training institution, having access to airspace is critical for us," Shepherd said. Accordingly, the school has 13 certificates of authorization (COAs) and was the first two-year college to receive a Section 333 exemption for commercial UAS operations in the national airspace. It has additional COAs and Section 333 exemption amendments under review. Sinclair's UAS fleet is similarly extensive. It has more than 150 aircraft, ranging in size from small electric systems to large reciprocating and turbo-prop aircraft.

CURRICULUM AND CUSTOM TRAINING

Sinclair's UAS program is an extension of the school's workforce development mission. It focuses primarily on three civil and commercial applications: first responder leadership, precision agriculture, and geospatial information.

Students enter the for-credit programs by completing a one-semester certificate in one of these three focus areas. "We've tied our curriculum to the needs of industry," Shepherd says. "Our goal is to make our students employable after a single semester." After another semester, students qualify for a one-year certificate and can finish the formal two-year degree program in four semesters.

In addition, Sinclair offers a variety of noncredit offerings, from breakfast briefings to multiday and multiweek workshops. Most often, these programs combine online and in-person sessions. It also presents cobranded online sessions with colleges across the country and is the national training partner for the Altavian and Sentara families of UAS and sensor products.

MODELING AND SIMULATION

Simulation provides the foundation for Sinclair's UAS curriculum, giving students the ability to apply what they learn in the classroom and to build the skills they will need to operate UAS under a variety of conditions. Sinclair employs a variety of simulation tools, from RealFlight 7.5, which they use for preflight training, to the more advanced L3, AEgis, and Simlat simulation systems. The high-end programs are extremely immersive, thanks to features like synthetic aperture radar simulation and the ability to connect to Sinclair UAS ground control stations. Sinclair has developed sufficient expertise in UAS simulation that it is collaborating with the Air Force Research Lab to develop software that meets Air Force research and civil training requirements.

DATA ANALYTICS

Shepherd noted that some of Sinclair's UAS flights collect up to a terabyte of data in just 45 minutes. In response, Sinclair's 400-server Network Operations Center has acquired dedicated hardware and software to support UAS data collection, processing, and hosting. It can store and manipulate various data types, including electro-optical/infrared, multispectral, and full-motion video.

To make this information available, Sinclair partnered with experts at Woolpert, a design, geospatial, and infrastructure management firm, to create the Sinclair Google Maps Data Portal, which is open free of charge to the public. Other schools are using this data as a tool in their classrooms.

THOUGHT LEADERSHIP

Sinclair's leaders realized that if the school were to secure a place as a preeminent UAS training and certification center, it had to be a source of thought leadership as well as training. One way it is doing this, Shepherd said, has been to launch the *Journal of Unmanned Aerial Systems*. "We realized that there wasn't a peer-reviewed journal focusing on UAS," he explained. "We wanted to create an open-source publication that would be relevant to researchers, technical staff, and senior managers." The first issue was published online in 2015.

In 2015, Sinclair also launched its inaugural UAS Academic Summit, cohosted with The Ohio State University College of Engineering. More than 80 attendees representing institutions from eight states came to Sinclair to hear 16 speakers highlight the latest advances in UAS training and education, research and development, technology transfer, and commercialization.

One way to measure the success of the school's efforts is the recognition it received this year from federal agencies. Sinclair was accepted as an affiliate member of the Federal Aviation Administration's ASSURE UAS Center of Excellence and as an industry member of the National Science Foundation's Center for UAS.

PHOTO: SINCLAIR COLLEGE

THE NEXT STAGE IN OHIO'S AVIATION HISTORY

As Shepherd made clear, there is a great deal of investment and activity behind the momentum of Sinclair's UAS program. "Ohio has a rich aviation history that starts with Wilbur and Orville Wright," he said. "We see UAS as the next evolution in this story." At the same time, he asserted, Sinclair welcomes partners from around the country and the world. "We always welcome opportunities to share information and to collaborate," he said.

Andrew Shepherd, PhD, is director of unmanned aerial systems in the workforce development and corporate services division at Sinclair College in Dayton, Ohio.

CYBERSECURITY FOR UAS SYSTEMS

BARRY HOROWITZ

Before describing his progress in developing secure UAS systems, Barry Horowitz, the Munster Professor of Systems and Information Engineering at the University of Virginia (UVA) and former president and CEO of the MITRE Corporation, highlighted a critical impediment to any successful cybersecurity effort: the difficulty that users and technical experts have communicating with each other. Horowitz recalled making a presentation in the early 1990s to a group of senior Wall Street bankers about defenses against cyber attack. They agreed with virtually everything he had to say, but balked at the prospect of having to meet with their cybersecurity groups. "We just don't speak the same language," they complained.

Horowitz noted another gap: between cybersecurity experts and those designing electromechanical systems. "This is a consequence of the way companies silo their personnel," he observed. "It is also a function of the way we silo the disciplines in our engineering schools."

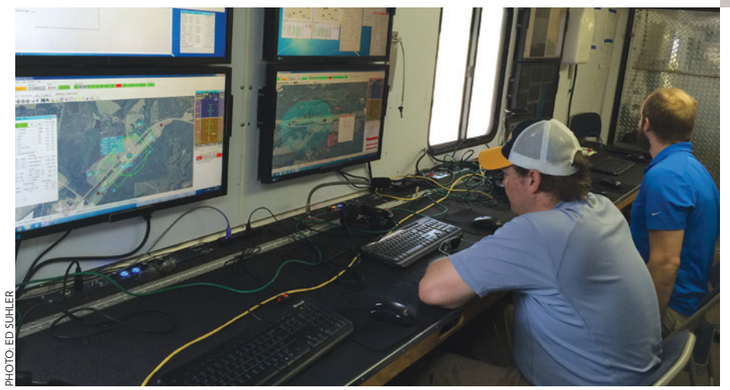

PHOTO: ED SUHLER

A CONCEPTUAL FRAMEWORK FOR UAS CYBERSECURITY

Horowitz has been exploring issues related to UAS cybersecurity for the last five years—and he had a number of observations to make about the challenges experts face in protecting these systems from cyber attack. He highlighted three areas of vulnerability: the manufacturing process, the final product, and the final product in the context of an integrated air/ground system. His research efforts focus on the last of these.

Horowitz noted that developing effective cybersecurity measures for UAS requires a comprehensive, systems-oriented approach. "They must acknowledge policy objectives, particularly safety," he said. "In addition, they must account for process and human factors issues as well as the range of technologies that can be used to mitigate threats, each with its own strengths and limitations."

To illustrate his point, Horowitz compared the cybersecurity measures traditionally used for information systems with those required by physical systems like UAS. His bottom line: protecting a physical system requires a different approach.

For information systems, the standard methods are infrastructural in nature, including network protections and system perimeter protections. There is little emphasis on protecting applications within specific information systems, and, he said, for good reason. "Applications change, are widely distributed, and vary significantly in quality," he noted. "Just the pace of change makes an application-level response difficult." An unfortunate consequence of this situation is that the cybersecurity community does not have experience in securing applications, and in particular the control functions that are a source of vulnerability in physical systems. At the same time, physical system designers do not typically design for better cybersecurity.

Horowitz's group at UVA developed an idea they call System-Aware Cybersecurity. This includes an added layer of security to protect system functions that, as a result of policy considerations, are deemed to present the highest risk. These functions are monitored for illogical behavior, like engine temperature decreasing even as it is supposedly spinning faster. On detection, UAS can be reconfigured. This response should be flexible, either restoring automatic operations or passing control to a human operator. "There are communities that have worked on these issues for many years, in such areas as fault tolerance and automatic control technologies as well as cybersecurity," Horowitz said. "We are bringing them together."

PHOTO: GTRI

Horowitz and his colleagues have decided to devote their energies to creating a sentinel that monitors the system and securing that, rather than the system itself. "We have seen in our work that the monitors are far simpler and more stable than the systems they protect," he noted. "We can make them very, very secure."

Horowitz's new system, the System-Aware Secure Sentinel, can address insider and supply chain attacks as well as externally generated attacks. It employs reusable design patterns to enable more economical solution development and includes doctrine for operator response to detected attacks. In addition, it incorporates integrated methodology and tools developed to support assessment of both the consequences of attacks and the impact of potential defenses on the cyber attacker's potential selection of attacks.

TEST FLIGHTS IN GEORGIA

In December 2014, Horowitz ran a series of flight tests at Early County Airport in Blakely, Georgia, in collaboration with the Georgia Tech Research Institute (GTRI). Over five days, they replicated likely threat scenarios, which include ground-based cyber attacks, insider-initiated attacks, and supply chain interdictions. As Horowitz explained, ground-based cyber attacks occur when an unauthorized UAS operator attempts to take control of the aircraft. An insider attack is when someone in an organization alters the UAV to bypass security measures. A supply chain attack occurs when an intruder embeds instructions in its electronics during manufacturing to bypass security or make the UAV perform other than as planned.

Horowitz and his team subjected a specially modified Griffon Outlaw ER UAS to a series of attacks designed to change waypoints, alter the camera pointing control system, induce GPS navigation errors, and cause video metadata changes. In each case, the Secure Sentinel technology rapidly detected, informed, and corrected system performance.

The Secure Sentinel contains multiple computer boards, operating systems, and software renditions. Randomly changing the configuration every few seconds makes this monitoring system very difficult to defeat. It monitored both the airborne and ground-based subsystems for continuity. "The actual code required for the monitoring as insignificant," Horowitz said. "It took less than 300 lines of code for each task and the various monitoring tasks are not intertwined."

CONTINUING TO LEARN

By developing systems for different automated systems, Horowitz said, his group is refining its approach to cybersecurity. For the Department of Defense, it looked at human factors issues at Creech Air Force Base, headquarters for a large number of the nation's UAS operational flights. It is also examining the security of an advanced fire control system for Army tanks as well as the Air Force/Army AIMES video exploitation system. For the National Institute of Standards, it analyzed the vulnerabilities of 3D printers. "We are looking at many scenarios and learning from each," he said.

Horowitz noted that securing physical systems from cyber attacks is less complex than protecting information systems. "It's a more contained objective," he said. "The control systems are simpler. There are fewer systems functions, limited access to system controls, and less software. And the systems themselves are bounded by the laws of physics."

He pointed out, however, that the consequences of successful attacks can be dire and an immediate response is often imperative. "Solutions require operators who are trained and ready to react to very infrequent and unprecedented cyber attacks," he said. "This is going to require a change in awareness." Horowitz cited his experience with the Virginia State Police. As part of a project with the organization, he successfully attacked a cruiser, preventing it from getting in gear. "No one thought it was a cyber attack," he said. "They just thought they had a transmission problem."

Barry Horowitz, PhD, is the Munster Professor of Systems and Information Engineering at the University of Virginia and chair of the department. Formerly president and CEO of MITRE Corporation, he is a member of the National Academy of Engineering.

UAS REGULATIONS: THE VIEW FROM THE MID-ATLANTIC AVIATION PARTNERSHIP

JON GREENE

Jon Greene began his presentation by noting wryly that as founding executive director of the Mid-Atlantic Aviation Partnership (MAAP), he had become an expert on UAS regulation, but that it has been well worth the effort. With the encouragement of Virginia Secretary of Technology Karen Jackson, Greene assembled a team of 70 members from Virginia, Maryland, and New Jersey and led by Virginia Tech with the goal of creating a powerful, multifaceted UAS test facility. Together, he noted, they can offer an unparalleled experience and expertise to support the entire UAS product lifecycle from R&D to customer training to operations.

The Federal Aviation Administration (FAA) agreed. It selected MAAP as one of six UAS Test Sites in December of 2013. MAAP conducted its first operational test flight at the Virginia Tech Transportation Institute in August 2014.

MAAP has had a number of remarkable successes. Leading the list, in July 2015, MAAP oversaw the first delivery by UAS in the United States. Flirtey, an Australian company with U.S. headquarters in Reno, Nevada, transported pharmaceuticals from Virginia's Lonesome Pine Airport to the Wise County Fairgrounds, the site of the annual Remote Area Medical Clinic. "We are a step ahead of Amazon," Greene said.

THE SAFEST AIRSPACE ON EARTH

Before describing the regulations that governed this and other UAS flights, Greene commented on the pace of UAS regulation: "Although the process has evolved at a rate slower than a lot of us would like, it is important to remember that the FAA has given us not only the busiest but the safest airspace on earth."

Greene pointed out that the fundamental regulation governing UAS flights is rule 14 CFR 91.113, which governs right of way. This reads in part, "When weather conditions permit, regardless of whether an operation is conducted under instrument flight rules or visual flight rules, vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft." In practice, Greene noted, this dictates that a human being must be in the aircraft to ensure safe operation. A camera or direct observation from the ground is not sufficient. "Because UAS are by definition unmanned, every UAS flight requires some sort of waiver to operate in the national airspace," Greene said.

There are a number of ways, Greene said, to secure a waiver. The first, for hobby use, falls under model aircraft operations. Hobbyists must have a visual line of site with the UAS at all times and must restrict the height of the flight to less than 400 feet above ground level. They must be more than five miles from an airport, and their UAS must weigh less than 55 pounds. What is most important, they cannot fly their UAS over people. Greene noted that the American Model Aircraft Association has published guidelines for hobbyists. "If you follow these, you won't get into trouble," he said. [In December 2015, the FAA required hobbyists to register with the agency.]

PHOTO: JIM STROUP

PHOTO: JIM STROUP

UAS users who want to operate their vehicles for public use must secure a certificate of authorization (COA), which allows them to fly a specific aircraft at a specific location. A public entity must certify the airworthiness of the vehicle and that public entity must own or lease the vehicle for a period of not less than 90 days. Greene noted that companies who wish to have MAAP test their UAS could lease the vehicle to the organization. "We perform the airworthiness assessment, provide safety oversight, and fly them using our processes," he said.

The major proviso in seeking a COA is that it must be for the public good. This covers such activities as search and rescue, public infrastructure inspection, and research. This does not cover use in higher education, which is considered a commercial activity, but it may include K–12.

There is an option, however, for commercial operations. Section 333 of the FAA Modernization and Reform Act of 2012 gave the FAA authorization to provide waivers to companies for low-risk commercial operations. More than 2,000 companies and universities currently have Section 333 waivers for such activities as training, agricultural inspection, and infrastructure monitoring. In order to qualify for a Section 333 waiver, the UAS must weigh less than 55 pounds and be operated at low altitude in an unpopulated area. Operators must maintain a visual line of site. Greene noted that it typically takes six months to secure a Section 333 waiver, although there is a fast-track process that can cut this time in half.

Greene acknowledged that many organizations have simply bypassed the waiver system. He noted that the FAA has become increasingly concerned about these violations. The agency noted that interactions with suspected unmanned aircraft have increased from 238 sightings in all of 2014 to 780 through August of 2015. During this past summer, the presence of multiple UAS in the vicinity of wild fires in the western U.S. prompted firefighters to ground their aircraft on several occasions. "The FAA is working with us and others to detect UAS that are flying illegally," Greene said. "It is not that hard." In fall 2015, the agency announced it was seeking a $1.9 million fine from Skypan, an aerial photography company, for scores of flights over some of the country's most congested airspace, New York and Chicago.

A LOOK TO THE FUTURE

In February 2015, the FAA proposed a framework of regulations that would allow routine commercial use of UAS under 55 pounds, while maintaining its flexibility to accommodate future technological innovations. The rule would limit flights to daylight and visual-line-of-sight operations. It also addresses height restrictions, operator certification, optional use of a visual observer, aircraft registration and marking, and operational limits. The agency received more than 5,000 comments during the comment period, which ended in April.

Although the FAA is hoping to release final rules by June 2016, Greene noted that many are not optimistic about achieving that date. "In addition to 2016 being an election year," he said, "there are a number of difficult issues that must be resolved, and the rules must be reviewed by a series of agencies, from the Department of Transportation to the Office of Management and Budget." Among the open questions are systems for certifying pilots and aircraft.

But as Greene pointed out, these rules cover a small portion of the envisioned uses for UAS. For Amazon to realize its vision of home delivery, it has to fly over people, something expressly forbidden in the proposed rules. Weight is another issue. Sensors exist that could greatly increase the utility of UAS, but they weigh more than 55 pounds. Finally, there is the line-of-sight issue. Greene noted that most business models that involve using UAS are for beyond-line-of-site applications. "The small UAS rules will be a step forward for the industry," he concludes, "but they are necessarily just a first step."

A former naval officer, Jon Greene is the founding executive director of the Mid-Atlantic Aviation Partnership and associate director for strategic planning and development of Virginia Tech's Institute for Critical Technology and Applied Science.

PHOTO: SINCLAIR COLLEGE

RESEARCH AND INDUSTRY INCENTIVES FOR UAS DEVELOPMENT

SCOTT KORDELLA, TONY COLE, RICK GORDON, JIM FLOWERS

The annual meeting concluded with a panel discussion that focused on steps that Virginia could take to become a nationally recognized leader in UAS. It featured four experts with a deep understanding of the public and private efforts needed to build and sustain a competitive advantage in an emerging technology.

SCOTT KORDELLA

Scott Kordella began the panel's remarks by noting that he worked primarily at the federal level and that the VASEM meeting had brought together a number of familiar faces who worked in federal technology programs. He commented that it was important for Virginia to tap into the comprehensive expertise the federal government assembles on technology issues. "I believe it is in everyone's interests," he said, "to make this transition happen as quickly and as efficiently as possible."

Kordella believes that some of the lessons learned from working with the National Space Program for MITRE Corporation could apply to the UAS sector. He noted that both the White House's National Space Policy and its National Space Transportation Policy make clear that that federal government has no intention of being the only operator in space. State governments, industry, and universities have been working together to take advantage of this opportunity, which has resulted in a number of individual projects. As an example, Kordella cited Minnesota's demonstration that the use of hyperspectral satellite imagery to manage the water quality in its many lakes would enable it to perform this task faster, more accurately, and less expensively than before.

While these individual projects are promising, Kordella noted, they should be complemented by state-level discussions about the opportunities that space offers. He asserted that the same kind of dialogue would help Virginia develop its UAS resources strategically.

Scott Kordella, PhD, is director of the National Space Program portfolio at the National Security Engineering Center at MITRE Corporation.

TONY COLE

The next panelist, Tony Cole, shared insights on incubators and accelerators from his work as vice president and global government CTO at FireEye. He believes Virginia and the United States have a great opportunity to drive innovation in UAS, but only if they act quickly. "I'm concerned that if we don't get in front of it very quickly, we will instead be consumers of this technology rather its creator," he said.

Cole noted that other areas have used tax incentives to encourage technology startups. He cited Beersheba, Israel, home of Ben-Gurion University, as a place where tax incentives have helped establish a flourishing cybersecurity industry. These incentives have given startups the breathing room they need to develop their ideas, helping them attract venture capital. Cole noted that Microsoft Ventures has invested in several companies in the area, and that tax policy is being considered for similar purposes in South Korea, Japan, and Australia.

Cole believes that centers of excellence, combining federal, state, and industry support, would also make a difference. Finally, he would like to see more educational initiatives—even video games about making video games—that expose children at an early age to the excitement of science, technology, engineering, and math (STEM). "We need a broader swath of kids in STEM programs than we have today," he said.

Tony Cole is vice president and global government CTO at FireEye. He helps government agencies, corporations, and systems integrators understand today's advanced threats and their potential impact.

RICK GORDON

Rick Gordon understands what it takes to support startups in an emerging area of technology. Gordon is the managing partner of MACH37™, a cybersecurity accelerator developed by Virginia's Center for Innovative Technology. "I think our experience may shed light on what can be done to nurture UAS entrepreneurs," he said.

The Commonwealth recognized that the state's substantial intellectual capital in cybersecurity wasn't leading to the formation of new companies. It created MACH37 in 2013 to remedy that situation. "By teaching technologists or would-be entrepreneurs to build tech companies, we help put them in a position to attract an angel investor or venture capitalist who can then play a role in their success," Gordon said.

In addition to training, MACH37 provides each company admitted to the program with $50,000 in seed capital. "While the typical entrepreneur in Palo Alto or Boston is a 20-something with nothing to lose, our entrepreneurs have families and real economic obligations like mortgages," Gordon says. "It was a commitment on our part to cover some of their opportunity costs during the 14-week training period."

This investment has proven an attractive inducement for entrepreneurs. Gordon noted that MACH37 has received applications from around the world. It has also produced value. Since it opened, the majority of its companies have secured seed funding. Gordon estimates that every dollar MACH37 invested will yield a fourfold return. "Building an accelerator that seeds innovators and creates sustainable enterprises works," he said.

Rick Gordon is managing partner of MACH37™, a cybersecurity market-centric accelerator developed by Virginia's Center for Innovative Technology.

JIM FLOWERS

The executive director of VT Knowledge Works, Jim Flowers, returned to a theme that both Scott Kordella and Tony Cole raised: the need for strategic government support for communities creating centers of excellence in emerging technological fields. "Places like Beersheba are not unusual around the world," he said, citing investments that Singapore has made in its quest to become the medical gateway to Asia, "nor is the government commitment that contributes to their success."

At the same time, Flowers noted that local communities must take a dispassionate look at their own strengths and resources and select an area of technology that can capitalize on them. "Communities were created for economic reasons—whether they were located near a navigable river or a coal deposit—but in many cases, these reasons become less compelling with time," Flowers said. "If those communities are going to survive and prosper, they must find new reasons to matter economically."

But that is just a first step, Flowers said. They must also create policies and practices that encourage startups that complement their strengths. And they must make an investment of their own. "If the movers and shakers in the local community don't buy in, nothing will change, despite everyone's best intentions," Flowers said. He concluded by proposing that the government develop a block grant tool to match the money that local funders raise to support startups.

Jim Flowers is executive director of VT KnowledgeWorks, which enables creative entrepreneurship through innovative curriculum, local business resource centers, and a global network of cooperating regions.

VASEM
School of Engineering and Applied Science
University of Virginia
P.O. Box 400743
Charlottesville, VA 22090-0743
www.VASEM.org

VASEM

VIRGINIA ACADEMY OF SCIENCE, ENGINEERING, AND MEDICINE

The Virginia Academy of Science, Engineering, and Medicine is a nonprofit organization comprising members of the National Academy of Science, National Academy of Engineering and Institute of Medicine who reside or work in Virginia.

VASEM's mission is to assist the Commonwealth of Virginia by serving as an intellectual resource to inform and educate agencies on issues for which science, engineering, and medicine affect decisions on policy, on the economy, and on the quality of life. The organization will promote research, foster interchange between individuals and organizations, and recognize and honor individuals in the Commonwealth who have made major achievements in science, engineering, and medicine.

Senator Mark Warner is the honorary chair of the VASEM board of directors.