When Grey Matters: White Hats in Dark Times

Cybersecurity expands at Georgia Tech

Few other universities are tacking cybersecurity research with the breadth and depth of the Georgia Institute of Technology. Few have the aptitude of nationally top-ranked computer science and engineering programs and the potency of a multi-million-dollar, applied research arm with a long history of supporting military, government and industry. Under this unique combination, the Institute for Information Security & Privacy (IISP) is poised to succeed: we foretell how the “white hats” should prepare because we continually witness how the “black hats” adapt.

The IISP – Georgia Tech’s eleventh interdisciplinary research institute – launched in Fall ’15 and since has leveraged the intellectual capital of seven units in profound new ways. Our inaugural year began by dissecting and defining Georgia Tech’s cybersecurity capacity, then creating new experiences for students, faculty and industry to coalesce around solutions. Astounding truths were revealed: cybersecurity research at Georgia Tech spans six critical areas, nine labs, and more than 460 researchers. Nearly $25 million in cyber research is underway. More than 1,100 individuals attended new events organized by the IISP in its first year. Eighteen industry partners were engaged -- global businesses such as British Petroleum, Intel and IBM; Atlanta-based companies, such as Norfolk Southern Railway and The Home Depot, and information security alumni, such as Ionic Security, Pindrop Security, and Damballa. Research faculty secured prominent new positions of influence in national policy and community leadership circles. Nearly 40 Ph.D. candidates entered the workforce, and born from valuable student research, two start-ups are in formation.

Upon completion of a successful first year, the IISP paused to assess how Georgia Tech compares to other academic institutions and to ask industry exactly what they need from a university research partner. We learned that although many universities are expanding cybersecurity activities, few do so with the same advantageous, historical foundation afforded to us by Georgia Tech and the Georgia Tech Research Institute. University research is perceived by industry as more flexible and affordable than other types of consulting. Yet, partnering with universities is often challenging for companies as they navigate copious administrative requirements to set up research engagements. The IISP seeks to serve in this area as well.

It is no exaggeration to state that members of the IISP are approached daily by industry and government in search of cybersecurity solutions. Cybersecurity no longer is just a computer programmer’s problem; it is an urgent concern for disciplines as diverse as public policy, business, defense and ubiquitous computing. For all of the above reasons, we stand ready to advance. The nation is hungry for solutions that will ensure the safety and security of American progress, and Georgia Tech has them.

Wenke Lee
Co-Director of the Institute for Information Security
John P. Imlay Jr. Professor, College of Computing

Bo Rotoloni
Co-Director of the Institute for Information Security
Director, Information and Cyber Sciences Directorate, GTRI
Cybersecurity at Georgia Tech

The Institute for Information Security & Privacy (IISP) at Georgia Tech connects government, industry, and academia to solve the grand challenges of cybersecurity. As a coordinating body for nine information security labs dedicated to academic and solution-oriented applied research, the IISP leverages intellectual capital from across Georgia Tech and its external partners to address vital solutions for national security, economic continuity, and individual privacy and safety. The IISP provides a gateway to faculty, students, scientists, government and industry, and a central location for national and international collaboration. Unbound by system rigidity or over-inflated egos, we’re discovering new solutions that close the innovation gap with immediate application in the real world.

POLICY

How should the private sector use personal information? Should the government be able to access communication in transit or at rest?

RISK

How do we quantify & assess in real time? Who do we watch? What do we look for?

CONSUMER-FACING PRIVACY

How can consumers securely interact with technology? What are the best practices?

TRUST

How should people, machines, and networks establish trust in reliable ways? How does the trust relationship change over time?

ATTRIBUTION

How can we definitively know who is responsible for a cyber breach? What can be done when we cannot attribute the breach?

CYBER-PHYSICAL SYSTEMS

What inputs and outputs should be part of the most fortified embedded and physical systems?
Fast Facts

6,031 students
1,111 event attendees
1,261 friends and followers

930 enrollees (professional education)

20+ year history of cybersecurity solutions

2 start-ups in formation:
FraudScope
ID for Web

7 units represented
1. GTRI
2. College of Computing
3. College of Engineering
4. Scheller College of Business
5. College of Liberal Arts
6. Georgia Tech Professional Education
7. Office of Information Technology

11 professional courses

460+ researchers

1 certification program

$24.1 million in annual research awards supported

200,000 square feet of classified research space

1 master of information security degree

1,111 event attendees
When Virtual Meets Actual
IISP events create new forms of community engagement

<table>
<thead>
<tr>
<th>EVENT</th>
<th>ATTENDANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital One Fall '15 Distinguished Lecture</td>
<td>348</td>
</tr>
<tr>
<td>13th Annual Georgia Tech Cyber Security Summit</td>
<td>260</td>
</tr>
<tr>
<td>Spring '16 Cybersecurity Lecture Series</td>
<td>409</td>
</tr>
<tr>
<td>Capital One Spring '16 Distinguished Lecture</td>
<td>56</td>
</tr>
<tr>
<td>Demo Day Finale Spring '16</td>
<td>38</td>
</tr>
</tbody>
</table>

Capital One Fall '15 Distinguished Lecture  Oct. 27, 2015

Famed cryptographer Ron Rivest -- professor at Massachusetts Institute of Technology and inventor of the RSA crypto public key system -- visited Georgia Tech for the IISP’s inaugural Capital One Fall ’15 Distinguished Lecture in a crowded auditorium where students surrounded him to autograph their textbooks. Rivest discussed elections and e-voting security in his talk: “Auditability and Verifiability of Elections.” This winner of the 2002 Turing Award told a captivated audience, “Evidence is the most important word in elections.” He spoke of software independence – when an undetectable bug in election software should not cause an undetectable change in the outcome of the election. “You don’t want your belief in the outcome of the election to be contingent upon your belief that the software is correct and unmodified.”

Georgia Tech Cyber Security Summit  Oct. 28, 2015

The 13th Annual Georgia Tech Cyber Security Summit formally unveiled the IISP to Georgia Tech and the world. A full house of more than 250 guests heard from two outstanding Georgia Tech alumni -- Tom Noonan (ME ‘83), a self-described serial entrepreneur, and Phyllis Schneck (Ph.D. CS ‘99), the U.S. Department of Homeland Security deputy undersecretary for cybersecurity and communications. A rousing panel discussion about privacy challenges included Peter Swire, the Huang Professor of Law and Ethics in the Scheller College of Business, and preceded release of the 2016 Emerging Cyber Threats Report.

Cybersecurity Lecture Series  Weekly, Jan. 29 – April 22, 2016

Under the IISP, the College of Computing’s long-standing Cybersecurity Lecture Series opened its doors for the first time to the public – attracting more than 400 attendees to this weekly series, sponsored by MailChimp in 2015-16. The series welcomed 13 speakers to Georgia Tech from across Atlanta and the country. Students from a variety of majors, faculty, and members of the public attended the series – giving it a 92% approval rating and indicating they would “highly recommend” it to a friend. Surveyed audience members report that their favorite speakers from Spring ’16 were Wenke Lee; John Corliss, a computer scientist from the U.S. Department of Homeland Security, and Tim Junio, a San Francisco-based entrepreneur who discussed how to map device vulnerabilities.
Harvard University’s Latanya Arvette Sweeney, director of the Data Privacy Lab, visited Georgia Tech to deliver the Capital One Spring ‘16 Distinguished Lecture, titled “How Technology Impacts Humans and Dictates Our Civic Future.” She discussed technology and its relationship to society, emphasizing the point that as recording devices become more ubiquitous, century-old policies surrounding personal privacy are continuously challenged. “Technology design is the new policy maker. We live in a technocracy – the rules in how we live our lives are determined by how the technology is designed,” she said. “We don’t train computer science students to actually think about all of the unforeseen consequences of how the technology is supposed to harmonize with society, yet the design decisions that are being made have a profound effect on society.”

The IISP’s inaugural Demo Day Finale awarded two student research projects with venture capital cash. Winning student, Musheer Ahmed (Ph.D. CS ’16), has filed a provisional patent for “FraudScope” to help insurers mine healthcare data and calculate risk among a provider pool. Ahmed and his faculty advisor, Mustaque Ahamad, are continuing translational research to develop a solution that addresses growing healthcare fraud and ensures that more healthcare dollars go to patient care. In addition to keen interest from businesses and entrepreneurs across Atlanta, FraudScope has received $400,000 in funding from the prestigious Wallace H. Coulter Foundation and Georgia Research Alliance. FraudScope also was one of four finalists among 80 competitors in the Technology Association of Georgia’s Biz Launch competition. This work allows Georgia Tech to expand its cybersecurity leadership while addressing rising challenges in healthcare IT, another area where Georgia plans to lead the nation. Meanwhile, the Demo Day “People’s Choice” winner – a new way of presenting one’s public key, called “ID for Web” – received $2,000 and has enrolled in a Tech Square incubator program to explore commercialization.

Participating as judges were venture capitalists and business leaders:

- Robin Bienfait
  Chief enterprise innovation officer, Samsung

- Paul Conley
  Managing director, Paladin Capital Group

- Sig Mosley
  Managing partner, Mosley Ventures

- Glenn McGonnigle
  General partner, TechOperators

- John Lee
  Senior associate, Osage Partners
Georgia Tech to Dismantle Pervasive Cyberattacks in 10 Seconds or Less

A multi-disciplinary team from the College of Computing and GTRI's Information & Cyber Sciences Directorate received $2.9 million to mitigate low-volume distributed denial of service (DDoS) attacks. Under project name ROKI, researchers will develop continuous analysis algorithms to compare a packet’s effect on system performance, then produce instructions to nullify a cyberattack and encode the finding into a network interface card in 10 seconds or less.

Low-volume attacks—while generally receiving less attention from scholars and media outlets—account for a significant percentage of all DDoS assaults. They can take down a website and be as damaging, but may use less bandwidth, are often shorter in duration, and may be designed to distract a security team.

**Sponsor:** U.S. Defense Advanced Research Projects Agency (DARPA)
**PI:** Taesoo Kim, assistant professor, School of Computer Science

SEISE Tool Uses Semantic Gaps to Detect Website Promotional Attacks

By detecting semantic inconsistencies in content, researchers have developed a new technique for identifying promotional infections of websites operated by government and educational organizations. Such attacks use code embedded in highly-ranked sites to drive traffic to sketchy websites - selling fake medicines, counterfeit handbags and plagiarized term papers, or installing drive-by malware.

**Sponsor:** U.S. National Science Foundation, Natural Science Foundation of China
**PI:** Raheem Beyah, Motorola Foundation Professor, School of Electrical & Computer Engineering

Device “Fingerprints” Could Help Protect Power Grid, Other Industrial Systems

Researchers are using the same principle as individually recognizable human voices to identify devices on electrical grid control networks, using their unique electronic “voices” – fingerprints produced by the devices’ individual physical characteristics – to determine which signals are legitimate and which signals might be from attackers.

**Sponsor:** U.S. National Science Foundation
**PI:** Raheem Beyah, Motorola Foundation Professor, School of Electrical & Computer Engineering
TOP CYBER TRENDS OF 2016

1. Consumers continue to lose their privacy as companies collect more data.

2. The shortfall in skilled security workers puts companies in peril.


4. Information theft and espionage show no signs of abating.

5. More companies consider cybersecurity threats an executive-level problem, and directors and officers are paying more than just cursory attention to cyber risks.

At the core of our mission is educating students with a curiosity and capacity to solve cybersecurity’s grand challenges. Supporting Georgia Tech’s educational mission is the first priority of the IISP’s research strategy. We spark economic growth and societal benefit by building the leaders who can competently create innovation.

<table>
<thead>
<tr>
<th>Degree Production</th>
<th>Enrolled (Fall 2015)</th>
<th>Graduated (Spring 2016)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bachelor’s, Computer Science</td>
<td>1,729</td>
<td>219</td>
</tr>
<tr>
<td>Master’s, Information Security</td>
<td>51</td>
<td>2</td>
</tr>
<tr>
<td>Master’s, Computer Science</td>
<td>1,822</td>
<td>132</td>
</tr>
<tr>
<td>Ph.D., Computer Science</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Bachelor’s, Electrical Engineering</td>
<td>880</td>
<td>136</td>
</tr>
<tr>
<td>Bachelor’s, Computer Engineering</td>
<td>582</td>
<td>72</td>
</tr>
<tr>
<td>Master’s, Electrical &amp; Computer Engineering</td>
<td>967</td>
<td>240</td>
</tr>
<tr>
<td>Ph.D., Electrical &amp; Computer Engineering</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Professional Education</td>
<td>930</td>
<td>NA</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>6,961</strong></td>
<td><strong>840</strong></td>
</tr>
</tbody>
</table>
Launching Big Ideas into Big Careers

Thirty-nine doctoral students graduated in Spring ’16 from the schools of Computer Science and Electrical & Computer Engineering, and are headed to a variety of sectors. Among them:

Musheer Ahmed – entrepreneur, FraudScope
Byoungyoung Lee – faculty, Purdue University
Shouling Ji – faculty, Zhejiang University
Yacin Nadji – post-doc and entrepreneur, NetRisk
Chengyu Song – faculty, University of California – Davis

Ph.D. graduates Byoungyoung Lee (second from left) and Chengyu Song (second from right) are pictured here with advisors Wenke Lee and Taesoo Kim after winning $100,000 from Facebook for identifying 11 previously unknown browser flaws. The graduates will both pursue academic careers and continue their research for Facebook.
Information security research underway or completed at Georgia Tech during 2015-16 is presented here. This conservative sampling represents more than $24 million in activity led by four units and involving several more.

<table>
<thead>
<tr>
<th>Project</th>
<th>PI</th>
<th>Unit</th>
<th>CoC</th>
<th>ECE</th>
<th>Scheller</th>
<th>Ivan Allen</th>
<th>GTRI</th>
<th>GTPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SATC-EDU: EAGER: Broadening Cyber Security Education Beyond Computing</td>
<td>Mustaque Ahamad</td>
<td>CS</td>
<td></td>
<td></td>
<td>$300,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TWC: Medium: Collaborative Exposing and Mitigating Cross-Channel Attacks</td>
<td>Mustaque Ahamad</td>
<td>CS</td>
<td></td>
<td></td>
<td>$900,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hosted Master's of Science in Information Security II</td>
<td>Mustaque Ahamad</td>
<td>CS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>An Early Warning System Against Cyber Attacks</td>
<td>Manos Antonakakis</td>
<td>ECE</td>
<td></td>
<td></td>
<td>$300,000</td>
<td></td>
<td>$2,356,684</td>
<td></td>
</tr>
<tr>
<td>Standardizing Botnet Enumeration</td>
<td>Manos Antonakakis</td>
<td>ECE</td>
<td></td>
<td></td>
<td>$455,744</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2P Security Analysis and Modeling</td>
<td>Manos Antonakakis</td>
<td>ECE</td>
<td></td>
<td></td>
<td>$70,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploring the Possibility for a Secure and Scalable Identity Management</td>
<td>Manos Antonakakis</td>
<td>ECE</td>
<td></td>
<td></td>
<td>$70,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ShareSafe: A Framework for Researchers and Data Owners to Help Facilitate Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA)</td>
<td>Manos Antonakakis</td>
<td>ECE</td>
<td></td>
<td></td>
<td>$777,010</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applying Behavioral Economics to Improve Cyber Security Behaviors</td>
<td>Faiborz Farahmand</td>
<td>ECE</td>
<td></td>
<td></td>
<td>$1,199,999</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Manufacturing Sector 1) PLC Honey pot</td>
<td>Dave Huggins</td>
<td>CTISL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$79,881</td>
<td></td>
</tr>
<tr>
<td>SATC-EDU: EAGER: Big Data and Security: Educating the Next-Generation</td>
<td>Taesoo Kim</td>
<td>CS</td>
<td></td>
<td></td>
<td>$300,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BFT++ Attack Tolerance in Hard Real-Time Systems</td>
<td>Taesoo Kim</td>
<td>CS</td>
<td></td>
<td></td>
<td>$1,245,720</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ConsoLite: Testing to Improve Software Security</td>
<td>Taesoo Kim</td>
<td>CS</td>
<td></td>
<td></td>
<td>$89,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource-Oriented Computation</td>
<td>Taesoo Kim</td>
<td>CS</td>
<td></td>
<td></td>
<td>$2,587,364</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embeddedasploit: A Pen-Test in a Box for Industrial Control Systems</td>
<td>Wenke Lee</td>
<td>CS</td>
<td></td>
<td></td>
<td>$1,250,351</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THEIA: Tagging and Tracking of Multi-Level Host Events for Transparent Compilers</td>
<td>Wenke Lee</td>
<td>CS</td>
<td></td>
<td></td>
<td>$4,193,126</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TWC: Medium: Privacy Preserving Computation in Big Data Clouds</td>
<td>Ling Liu</td>
<td>CS</td>
<td></td>
<td></td>
<td>$1,199,999</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Retail Sector 1) Infosec Program Analysis</td>
<td>Ben Medlin</td>
<td>CTISL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$525,000</td>
<td></td>
</tr>
<tr>
<td>(Transportation Sector 1) PEN Test</td>
<td>Ben Medlin</td>
<td>CTISL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$54,196</td>
<td></td>
</tr>
<tr>
<td>(Oil &amp; Gas Sector 2) Master Services Agreement</td>
<td>Steve Moulton</td>
<td>CTISL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$0</td>
<td></td>
</tr>
<tr>
<td>SHF: Small: New Frontiers in Constraint-based Program Analysis</td>
<td>Mayur Naik</td>
<td>CS</td>
<td></td>
<td></td>
<td>$450,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAGER: Collaborative: Leveraging Graph Databases for Incremental...</td>
<td>Alessandro Orso</td>
<td>CS</td>
<td></td>
<td></td>
<td>$100,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Oil &amp; Gas Sector 2) Prototyping</td>
<td>Valerie Taylor</td>
<td>CTISL</td>
<td></td>
<td></td>
<td>$176,741</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Oil &amp; Gas Sector 2) Insider Threat</td>
<td>Valerie Taylor</td>
<td>CTISL</td>
<td></td>
<td></td>
<td>$100,000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insider Threat (Financial Sector 1)</td>
<td>Noah Tobin</td>
<td>CTISL</td>
<td></td>
<td></td>
<td>$219,135</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA)</td>
<td>Seth Walters</td>
<td>CTISL</td>
<td></td>
<td></td>
<td>$4,900,000</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Totals                                                                  |                        |       |      |      | $13,287,536 | $2,448,523 | $0     | $0    | $6,054,953 | $2,356,684 |

Grand Total: $24,147,696
Partnering with Industry to Lead

The External Advisory Board of the Institute for Information Security & Privacy is a select group of representatives from leading organizations who help to create research and educational programs that address the grand challenges of cybersecurity. Members of the Board steward the IISP by providing advice about the foundational research that is most needed, the direction of technology in development, tech transfer and startup environments, and financial support for events and activities. Membership is offered by invitation to experienced leaders in public or private industry, entrepreneurs, and venture capitalists.

Board Members 2015-16

Daniel Barriuso, British Petroleum
Marty Battaglio, Norfolk Southern Railway
Scott Buck, Intel Corp.
Tom Cross, Drawbridge Networks
David Dewey, Pindrop Security
Jamil Farshchi, The Home Depot
Adam Ghetti, Ionic Security Inc.
Karl Guntow, CyberPoint International
John Marshall, AirWatch
Michael O’Rierdan, Comcast Corp.
Barney Sanchez, IBM
David Scholtz, Damballa Inc.
Monirul Sharif, Google
Tony Spinelli, Capital One
Arjun Thusu, Worldpay
Joe Uhl, MailChimp
Johnson Wu, Acalvio
Bob Varnadoe, NCR Corporation
Second Steps Begin

Looking Ahead to Year Two

Peering into Year Two for the Institute for Information Security & Privacy, bold new strategies already are underway to ensure national security, personal safety and economic continuity. Exciting degree expansions and scholarship opportunities are in motion to expose more students to cybersecurity careers. Esteemed organizations such as RSA, the French Embassy and the U.S. Federal Reserve are proactively approaching us for highly public engagements. Research awards secured in the first month of Fiscal Year 2017 already exceed last year’s totals by more than 32 percent.

There is limitless potential that can only be constrained by hours in the day and unexpected, but welcome, diversions from more who need our help. Our core objectives remain clear:

- Increase by 50% the volume of cybersecurity research by 2020
- Expand pathways into the Master’s in Information Security degree
- Produce 60 Ph.D. candidates in the next five years
- Develop at least five commercial start-ups from academic or applied research

Market Indicators Point to Growth

We know that university research is perceived by industry as more flexible and affordable than other types of consulting. Universities are critical for offering deep domain expertise, innovative solutions, and hypothesis testing when companies must instead keep employees focused on a narrow window of quarterly profits.

The number of institutions conferring master’s degrees in computer and information systems security has nearly doubled between 2010 and 2014, from 26 to 50 institutions nationally. Among Georgia Tech’s 23 benchmarked peer institutions, six specifically offer master’s degrees in information security, cybersecurity, or related areas. Nationally, the number of master’s degrees conferred in this field has increased from 560 in 2010 to 1,804 in 2014, suggesting growing demand.

Prospective buyers of information security and privacy research tend to engage with local institutions with which they have partnered with in the past. Local, in-person relationships between university researchers and industry are critical to success. Structured partnership programs, such as those offered by Carnegie Mellon University’s CyLab and Purdue University’s CERIAS, are organized consortium models that offer companies access to research, faculty, and staff in exchange for an annual or multi-year financial investment. These programs require extensive administrative support and on-going relationship building, but also create symbiotic relationships that would otherwise be unrecognized.

Growth Builds from Investment in Organizational Structure

The IISP has the potential to be the “front door” to Georgia Tech’s information security and privacy researchers, allowing companies to seamlessly engage with talented faculty and students while cultivating long-term relationships that provide researchers with access to real-world data and challenges.

To move forward, the IISP will need to continue its research trajectory and funding while supporting its talent. The IISP will need take steps to reinforce areas that will most strongly contribute to the IISP’s success. This may require additional financial and administrative support, as well as broader efforts both internally and externally to educate stakeholders about the IISP’s capabilities.

Nearly 20 years ago, Georgia Tech’s strengths in technology and policy warranted it to take a leading role in improved security research, education and more reliable computing. Today, the IISP advances from that success with revolutionary steps. We are truly creating the next gateway for faculty, students, scientists, government and industry – the place for national and international collaboration to solve cybersecurity’s grandest challenges.