White Hats, Black Hats, and Grey Matter: Tackling Cybersecurity

By Gordana Goudie, Tara La Bouff, Jacqueline Nemeth, and Mike Terrazas

A secure internet and its applications are now essential to almost every aspect of our daily lives. Yet connected technology has opened the door for criminals and foreign governments to launch cyberattacks with increasing scale and impact.

Today, America's national defense, economic prosperity, and individual freedoms depend upon cybersecurity.

As the storm of demand for cybersecurity solutions and talent grows, Georgia Institute of Technology researchers, faculty members, and students are tackling cybersecurity from multiple angles.

Black, White, and Nuances of Grey

In the realm of cybersecurity, white hats are good-guy defenders and black hats are the adversaries. But it takes both to really put grey matter to work in solving one of the most vexing challenges of our time.

Few universities can approach cybersecurity with the same breadth and depth as Georgia Tech. Few have the cooperation of top-tier academic researchers, plus 500 cybersecurity engineers inside a multimillion-dollar research division that is the Georgia Tech Research Institute (GTRI), and a deep history of supporting classified military, government, and law enforcement operations.

Under this unique combination of resources and skill, Georgia Tech is creating the next wave of cybersecurity solutions. Tech's grey hat hackers study how malicious black hats operate and adapt in order to help the white hats prepare for the next attack.

Seven units and 12 labs across Georgia Tech and GTRI are engaged in cybersecurity. With coordination by the Institute for Information Security & Privacy (IISP), faculty and students across a range of disciplines can connect to tackle new facets of the cybersecurity problem.

Look what's underway…

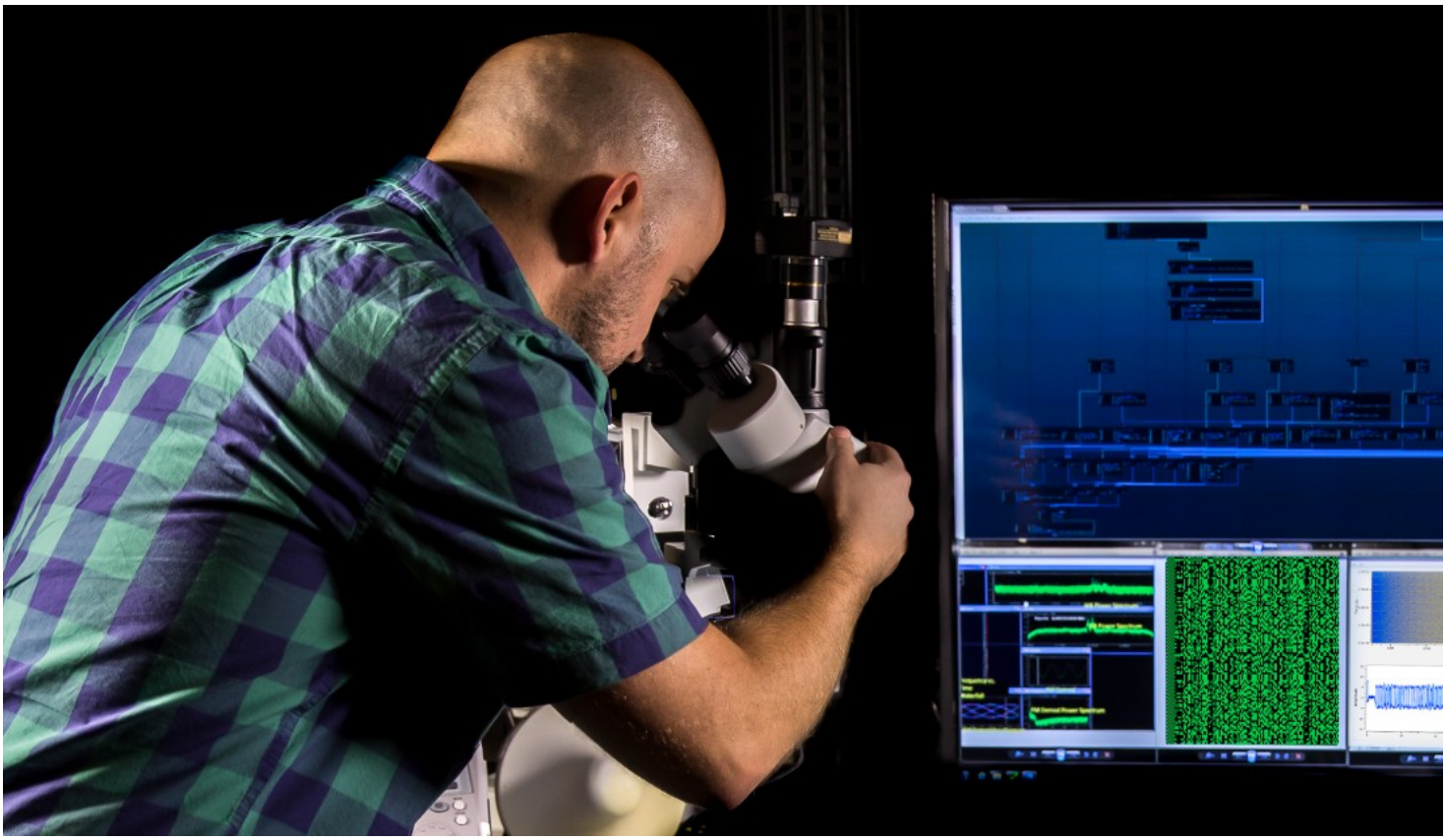
GEORGIA TECH RESEARCH INSTITUTE

Producing more than $86 million in security research each year, GTRI develops the high-risk, high-payoff custom solutions that secure, defend, and respond to threats within our country's information, distribution and network systems.

Research is performed in classified and unclassified spaces for clients seeking the ultimate competitive edge.

Engineers collaborate extensively with Georgia Tech faculty and train numerous students. GTRI's Michael Farrell co-directs the IISP with Wenke Lee from the School of Computer Science to bring academic and applied researchers together.

Cyber Information Protection and Hardware Evaluation Laboratory



CIPHER's work includes technologies in computing, network architectures, signal and protocol analysis, network forensics, custom algorithms for cyber defense and attribution, malware analysis, open source information collection and correlation, insider threat detection and mitigation, hardware and software reverse engineering, and advanced analytics.

Read More

Information and Communications Laboratory

ICL creates secure interactions between networks and devices used for national security, intelligence, emergency response, health analytics, and smart cities.

Known for its geospatial decision tools that support military missions, ICL defines the future of communication through integrated sensors, Internet of Things, and commercial product realization.

Read More

PUBLIC POLICY AND INTERNATIONAL AFFAIRS

Governments engaged in cyber-espionage or cyber-enabled power struggles are now considered among the most pervasive and dangerous threat actors. That's why, at Georgia Tech, even the College of Liberal Arts takes aim at cybersecurity.

Faculty and researchers in the School of Public Policy investigate the policy, legal, and human aspects of cybersecurity — shaping discourse around international practices, shifting cultural norms, challenges to free speech, and intellectual property in the information economy.

Internet Governance Project

Led by professor Milton Mueller, the group examines the methods and international power struggles over an open and secure internet, information routing, and trade – especially where no "court" or governing authority stands above all.

Read More

Policy Research

Research by the School of Public Policy and the Sam Nunn School of International Affairs also addresses technology diffusion and the IT infrastructure needed for national defense – from nuclear arsenals to a sufficient, highly skilled workforce.

Read More

COMPUTING

Researchers at the College of Computing advance cybersecurity by uncovering devastating vulnerabilities between operating systems, hardware, and software; mobile apps; and the machine-learning algorithms that power automated decisions.

Visionary Leaders

The college spearheaded Georgia Tech's entry into cybersecurity academic research in the 1990s with the launch of the Georgia Tech Information Security Center. An annual Cyber Security Summit soon followed.

Since then, Georgia Tech has consistently been one of the top universities represented by research published at the world's most important cybersecurity conferences, and the College of Computing has led the way.

In fact, many of the Institute for Information Security & Privacy's most influential researchers, such as Mustaque Ahamad, Taesoo Kim, Annie Antón, and Sasha Boldyreva, are based in the College's three schools.

With funding from the National Science Foundation, Department of Defense and industry leaders such as Intel and Google, more than two dozen professors are working on the frontiers of cybersecurity. For example, David Bader, Polo Chau, and Le Song are developing new big data analysis algorithms for security analytics as well as new security protection for machine learning.

Economic Influencers

Multiple Atlanta cybersecurity-related startups, such as Pindrop Security and Fraudscope, have been founded from College of Computing student and faculty research.

Former student Chris Klaus is a successful entrepreneur who began to develop his first business at Georgia Tech. He took public and later sold Internet Security Systems Inc. to IBM for $1.3 billion. Today, he continues to mentor Tech students to move great ideas to market through CREATE-X.

BUSINESS

Faculty in the Ernest Scheller Jr. College of Business seek solutions to mitigate risks for business, industry, and for-profit organizations at every level. The scale and sophistication of cyberattacks against businesses has grown from the relatively simple theft of stolen credit card data to operational seizure of hospital systems by ransomware.

Whether it's the pre-release of stolen creative works (experienced by Sony Pictures) or the heist of complete personal data on 143 million Americans (at Equifax), it's now clear that organizations in every market vertical are at risk.

Business Guidance

The Institute for Information Security & Privacy's Associate Director Peter Swire — a professor, attorney, and nationally regarded expert who served in the White House, studies emerging business issues as global companies try to navigate conflicting data regulations, privacy, and cybersecurity laws.

Risk Management Research

Spearheaded by Sudheer Chava, financial professor and associate director of the IISP, researchers address minimizing risk from cyberattacks, methods for quantifying financial and reputational impact after a breach, and incentives for cooperation among all stakeholders when responding to or preventing an attack.

Read More

Technology Association of Georgia FinTech Report

Data Analytics/Big Data in Financial Services

DOWNLOAD THE REPORT

PROFESSIONAL EDUCATION

Business leaders and organizations know that it's not just management at the top who need to understand cyber risk and technologies, but every layer of the workforce.

Which is why demand has skyrocketed 93 percent in recent years for Georgia Tech Professional Education cybersecurity courses.

Cyber Security Certificate

Georgia Tech Professional Education offers more than 100 courses about essential topics for business professionals and military operators. This is one of GTPE's signature offerings, combining applied research, expert instruction, and interactive learning.

Courses are taught by research faculty from Georgia Tech and GTRI, some of whom are former military or government intelligence personnel from the United States or its allies with experience in nation-state cyberwarfare response.

Read More

Admiral James "Sandy" Winnefeld (Ret.)

Cybersecurity Leadership Program

In 2016, GTPE and The Sam Nunn School of International Affairs hosted Georgia Tech's Cybersecurity Leadership Program — the first of its kind in Atlanta.

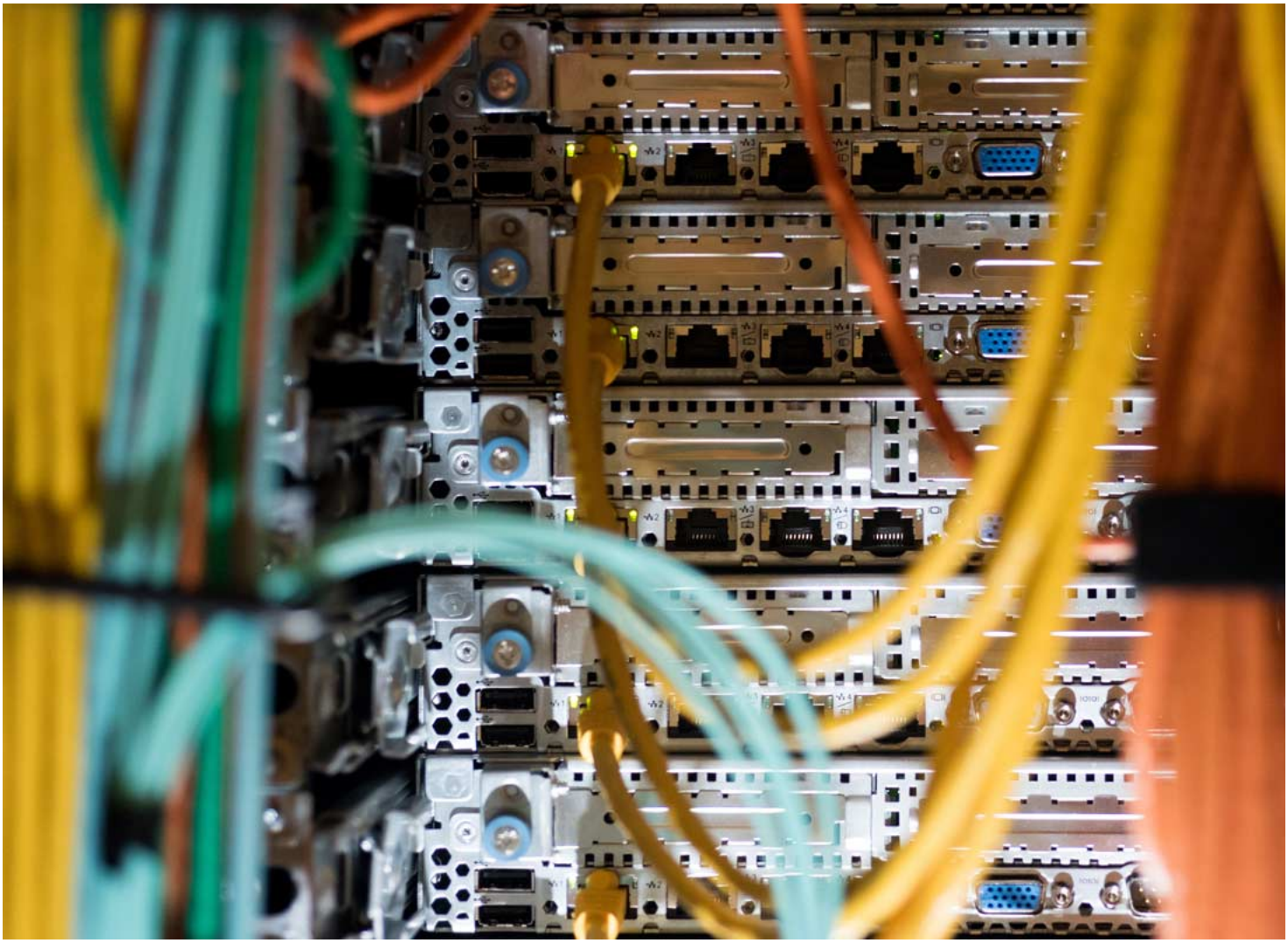
The program was developed by Admiral Sandy Winnefeld (Ret.) to build cybersecurity technical understanding and leadership capabilities among public, private, and nonprofit organizations.

ENGINEERING

The cybersecurity challenges addressed by faculty in the School of Electrical and Computer Engineering are as diverse as the field itself.

Research spans how to detect cyberattack in wireless networks, spot malware signs in novel places, protect cyber infrastructure for industrial facilities and power grids, and perform cyber forensics.

Identifying Cyber Attackers



Along with the GTRI, assistant professor Manos Antonakakis is working to establish new science around the ability to identify virtual actors behind cyberattacks, a technique known as "attribution."

Read More

The group recently developed new, malware-independent detection strategies that help network defenders spot security breaches in a timely manner.

Researchers Counter a New Class of Coffee Shop Hackers

Associate professor Alenka Zajic is studying emissions from computers that aren't connected to Wi-Fi and has developed a metric for measuring the strength of such leaks – known as "side-channel signals." Side-channel signals emitted by computers and cellphones could provide hackers with another way to see what the devices are doing.

By analyzing the low-power electronic signals emitted by these devices – even when they're not transmitting on the Internet or cellular networks – hackers can obtain information about computer operations and even track passwords.

Read More

She also leads a team that is developing a new way to wirelessly monitor IoT devices for malicious software without affecting their operations.

Fortifying Cyber-Physical Systems and Utilities

Motorola Foundation Professor and ECE Interim Steve W. Chaddick School Chair Raheem Beyah aims to protect cybersecurity infrastructure for industrial facilities, building-management systems, and power grids.

The interests of Georgia Power Distinguished Professor Santiago Grijalva lie in developing a cyber-physical security assessment tool that considers the interdependencies of power systems and cyber and communication network components. His CPSA module could be integrated with utility management systems to support real-time control and operation, and what-if scenario analysis.

Georgia Power Distinguished Professor Sakis Meliopoulos, associate director of cyber-physical systems for the IISP, develops methods to detect and block cyberattacks on the power grid in real time. His work has been demonstrated with several utility companies.

Read More

Cyber Forensics Innovation Laboratory

Assistant Professor Brendan Saltaformaggio heads the Cyber Forensics Innovation Laboratory to research advanced cybercrimes.

The lab examines, analyzes, and prevents next-generation malware attacks — particularly in mobile and Internet of Things environments.

PROTECTING GEORGIA TECH

Rounding out Georgia Tech's cybersecurity approach is the team that protects the Institute's faculty, staff, students, and resources from potential attacks.

Georgia Tech Cyber Security works with campus units to identify and neutralize attacks on campus IT resources and data, educate users to cyber threats, and ensure compliance with information security laws and policies.

Georgia Tech is investing millions of dollars to improve cybersecurity infrastructure for its 34,000 users, including next-generation firewalls, vulnerability upgrades, and system replacements.

LEARN MORE

- Explore more cybersecurity research at Georgia Tech, the Georgia Tech Research Institute, or begin a research project with us.
  Institute for Information Security & Privacy
- As of this fall, the School of Public Policy offers a Master of Science in Cybersecurity degree – jointly with the College of Computing — with a track dedicated to policy.
  Master of Science in Cybersecurity
- Sign up for email alerts about public cybersecurity events.
  Subscribe to Cyber News