ARTIFICIAL INTELLIGENCE AND CYBERSECURITY
The University at Albany (UAlbany) is a comprehensive Research 1 (R1) institution under the Carnegie Classification and one of four research-focused “University Centers” in the State University of New York system. UAlbany is widely recognized for its cutting-edge research programs, student-centered academic and research experiences, and opportunities for research collaboration and industry partnership. UAlbany has a demonstrated history of service to New York’s Capital Region and has been recognized by the Carnegie Foundation’s Community Engagement Classification.

UAlbany offers significant expertise in two rapidly growing and closely related research areas: Artificial Intelligence (AI) and Cybersecurity (CS). AI technologies automate many tasks traditionally performed by humans, such as image or speech recognition, robot-assisted surgery, analysis of large data sets, and simulations of complex social problems. Cybersecurity is a rapidly evolving field dedicated to protecting information systems from intrusion, disruption, or damage by bad actors.

Our AI and CS faculty work across a wide range of disciplines and departments, including Computer Science, Information Security, Mathematics, Electrical Engineering, and Emergency Preparedness. Their research projects are supported by grants from the Department of Defense, the National Science Foundation, the National Institute of Justice, the Department of Energy, Global 500 corporations, and private foundations. We hope that you will be inspired by the many research opportunities available to our students and research partners.

JAMES A. DIAS, PH.D.
VICE PRESIDENT FOR RESEARCH

SATYENDRA KUMAR, PH.D.
ASSOCIATE VICE PRESIDENT FOR RESEARCH
Dr. Chang’s lab is using computer vision and artificial intelligence to develop “smarter” technologies with a wide range of applications. Video analytics can be deployed to identify “fake” media, automate industrial site monitoring, enhance the situational awareness of robots, improve traffic management, and facilitate online learning.

**EXPERTISE**

Computer vision, artificial intelligence, video analytics, machine learning

**ACHIEVEMENTS**

- Developed a deep neural network model for multi-people visual detection and human pose estimation
- Applied state-of-the-art deep neural network and AI techniques to smart transportation for vehicle detection, tracking, counting and re-identification
- Developed deepfake detection algorithms to identify forgery images for media forensics

**PUBLICATIONS**

- **Adaptive RNN Tree for Large-Scale Human Action Recognition**, W. Li, L. Wen, M.-C. Chang, S. Lim and S. Lyu, IEEE International Conference on Computer Vision, Venice, Italy (October 2017).
Dr. Ekenna’s team is working on robust motion planning algorithms that use machine learning techniques to improve the speed and accuracy of autonomous robots and reduce the opportunity for cyber-attacks that exploit situational awareness vulnerabilities. Another project focuses on a metering system to identify weak components in internet of things (IoT) frameworks prior to deployment.

EXPERTISE
Internet of things (IoT) ecology, anomaly detection, reinforcement learning

ACHIEVEMENTS
• Applied reinforcement learning techniques to improve motion planning algorithms for autonomous robot applications in cybersecurity
• Combined cybersecurity research with AI techniques, such as anomaly detection and reinforcement learning, to create a measure of vulnerability to IoT players
• Developed IoT applications to smart city infrastructures

PUBLICATIONS
Robustness is critical to machine learning applications such as computer vision, signal processing, and image processing. Dr. Feng’s research is focused on learning and prediction to account for the “noise” in data sets by exploring the theoretical underpinnings for well-established, but not fully understood, machine learning algorithms. He is also developing novel methods for dealing with noisy high-dimensional data.
Threat assessment and cybersecurity are becoming increasingly critical to the public sector. As a former government intelligence analyst, Dr. Nussbaum is particularly interested in assessing cyber risks and threats at the level of states, regions and municipalities—national security problems at the sub-national level.
Applying machine learning to human-centered data creates reliable models for analyzing and predicting human behavior. These models help us to understand and improve students’ academic performance, make accurate product recommendations, or analyze social networks and community dynamics.

**Expertise**

Machine learning in human-centered applications with multi-view and sparse data, personalization, recommender systems, and educational data mining

**Achievements**

- Developed matrix and tensor factorization models and algorithms to capture learner knowledge gain and forgetting, estimate learning material’s domain knowledge map, and predict students’ future performance
- Developed transfer learning and domain adaptation approaches to model user interests across multiple domains and systems for high quality learner recommendations
- Created factorization and process models to distinguish between efficient and inefficient online learning behaviors, detect procrastination, and study the effects on learning gain and performance

**Publications**

- Detecting Trait vs. Performance Student Behavioral Patterns Using Discriminative Non-Negative Matrix Factorization, M. Mirzaei and S. Sahebi, Proceedings of the Thirty-Third International Florida Artificial Intelligence Research Society Conference, North Miami Beach, FL (May 2020).
The rapid proliferation of “fake news” demands sophisticated methods to mitigate misinformation. Tools for analyzing and authenticating the source and content of news items include natural language processing, machine learning, fusion algorithms, and component and page ranking. Dr. Atrey is combining them in a robust tool that analyzes credibility and provides a “truthfulness score” to consumers.
Topological data analysis (TDA) is useful for imputing missing values and studying the “shape” of large complex data sets. When combined with machine learning, TDA is particularly useful for analyzing manifolds and spaces with manifold strata. This provides a complete set of computable algebraic invariants for a manifold, which is especially useful for epidemiological and biomedical data.
The proliferation of social media has also given rise to online harassment. Machine learning enables fast, accurate detection of cyberbullying, both by alerting offenders to potentially offensive content and by allowing their victims to limit inappropriate contact. This creates safer online communities, particularly for young people who are the frequent targets of cyberbullies.
Intelligent security and privacy analysis are critical to thwarting social engineering attacks. Dr. Masoumzadeh is using automated techniques to analyze the security and privacy behavior of applications without accessing the code. He and his team are also developing a platform that detects social engineering attacks and engages the perpetrators in conversation with the goal of investigating them.

**EXPERTISE**
Modeling, testing and verification of security policies; privacy control, privacy enhancing technologies and data anonymization; machine learning in cybersecurity

**ACHIEVEMENTS**
- Developed machine learning approaches for detecting impersonation and social engineering attacks based on stylometric and communication behaviors
- Proposed machine learning approach for learning access control behavior of web applications without access to application's code
- Developed machine learning algorithms for constructing high-level access control policies from low-level authorization information in systems
- Proposed a computational model of information exposure in online social networks that can be used for privacy awareness and control
- Developed efficient algorithms for anonymizing social and geo-social network datasets

**PUBLICATIONS**
Risk analysis is an effective tool for anticipating and mitigating the consequences of cybersecurity incidents. Impact modeling that considers both internal and external dependencies transforms cyber risk management from a narrow technical issue to a broader business security strategy. This approach creates a common language for technical experts and executive decision makers to collaborate on business continuity planning.

**Unal Tatar**
Assistant Professor
Emergency Preparedness, Homeland Security and Cybersecurity
PhD, Old Dominion University
utatar@albany.edu

**Expertise**
Cybersecurity risk analysis, cyber resiliency, cyber insurance, privacy by design, critical infrastructure protection, cybersecurity education

**Achievements**
- Created an economics-based cyber risk assessment method for acquisition decisions
- Developed a cyber risk quantification method for actuaries and insurance sector
- Assessed cybersecurity risks of maritime critical infrastructure through a novel risk analysis method for the NATO Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
- Developed cyberterrorism and security research and education program for NATO Defense Against Terrorism Centre of Excellence (DAT COE)

**Publications**
User compliance to security policies is a critical component of managing security risks. A good risk management program should have a clearly defined plan for enforcing policy compliance, detecting non-compliance, and addressing non-compliance.
Cybersecurity is critical to our society’s functioning. Organizations need to recognize the importance of cybersecurity and must understand their responsibilities in securing their assets. As a former Application and Security Manager, Critical Care Information Systems, Dr. Yankson is interested in developing privacy and security conscious solutions and teaching the next generation of students who can help organizations build reliable cybersecurity programs and prevent attacks.
From personal assistants, to basic human needs, to the next generation of Semantic Web, graphs play a central role. AI is helping both organize, comb through, and glean insights from such data at unprecedented scales. The challenge is in ensuring that AI solutions are both accurate and constantly evolving, equitable, and tamper-proof.
Dr. Ying’s research group explores the design of new risk measures and efficient optimization algorithms from the novel interaction of statistics, applied mathematics, and machine learning. He and his group have developed robust and efficient ML algorithms for various application domains, such as face verification, anomaly detection, prediction of tumor growth, prediction of wildfires, and privacy protection.
In a rapidly changing world, it is critical that we integrate cutting-edge technologies into our research. Atmospheric Science, in particular, is a prime example of “big data,” and Dr. Sulia is striving to exploit advanced computational techniques, such as data analytics and machine learning and push weather research and development into new frontiers.

KARA
SULIA
PHD, PENN STATE UNIVERSITY
KSULIA@ALBANY.EDU

EXPERTISE
Implementation of novel computational techniques to advance research and development in the Atmospheric Sciences

ACHIEVEMENTS
• Development of advanced visualization software platforms and associated APIs including (1) a mobile app for real-time New York State Mesonet data, (2) web-based interface displaying multi-source air quality measurements and forecasts, and (3) web-based interface for multi-source electrical outage information.
• Determination of the impacts of weather on utility grid outages; development of load, outage, and photovoltaic generation forecasts.
• Development of a database containing millions of type-categorized cloud particle images to characterize weather event microphysics.

PUBLICATIONS
Dr. Goel is currently engaged in cyber security and warfare research and computer security threats such as botnets and malware, risk analysis, security policy development and evaluation, security modeling, and self-organized complex systems. He is leading an effort, launched by IEEE Communications Society and the IEEE Standards Association, to create a vision for the Smart Grid 15 years into the future.
Moral psychology is a burgeoning inter-disciplinary field that investigates human functioning in moral contexts. Drawing on both the empirical resources of the human sciences and the conceptual resources of philosophical ethics, Dr. D’Cruz’s group investigates the trustworthiness of artificial agents, the epistemic value of empathy, moral responsibility for implicit bias, and the rational basis for forgiveness.