

# 2019 SAIC National Security Education Program Colloquium

## The Weaponization of Information and Artificial Intelligence

Hosted by

Hume Center for National Security and Technology and the  
Virginia Tech Integrated Security Destination Area

Sponsored by



April 16, 2019

The Inn at Virginia Tech and Skelton Conference Center  
Blacksburg, Virginia

# Hume Center & the Integrated Security Destination Area

The mission of the Ted and Karyn Hume Center for National Security and Technology is to cultivate the next generation of national security leaders by developing and executing curricular, extracurricular, and research opportunities to engage students. Education programs principally engage undergraduates through curriculum development, extra curricular programs, internship and career opportunities in the national security sector, and scholarships.



**HUME CENTER FOR NATIONAL  
SECURITY AND TECHNOLOGY**  
VIRGINIA TECH™

The Hume Center leads Virginia Tech's research, education, and outreach programs focused on the challenges of cybersecurity, autonomy, and resilience in the context of national and homeland security. Education programs provide mentorship, internships, scholarships, and seek to address key challenges in qualified US citizens entering federal service. Current research initiatives include cyber-physical system security, orchestrated missions, and the convergence of cyber warfare and electronic warfare.

It is important to recognize that the core mission of the Hume Center is student-focused. Research activities support the student ecosystem, and as such, all research activities include student participation.



The Integrated Security Destination Area focuses on understanding and fostering a world in which individuals, institutions, and nations are secured by technology and social systems that follow ethical principles and promote values of social justice.

Faculty working together in this area are bringing a transdisciplinary approach to the complex range of human and systems security challenges. Work in this area also embraces equity in the human condition by seeking the equitable distribution and availability of physical safety and well-being, psychological well-being, respect for human dignity, and access to crucial material and social resources throughout the world's diverse communities.

This Destination Area further addresses policymaking and policy analysis, collaborating at the intersection of scientific evidence, governance, and analyses to translate scholarship into practice.

# Agenda

\*\*All Sessions in Latham Ballroom A except where noted

9:00 a.m.	<b>Welcome, Col. Paul Mele, Commanding Officer of the Virginia Tech Army ROTC</b>
9:10 a.m.	<b>Student Team Presentation</b> - Hack RFML Attack & Resilience teams
9:40 a.m.	<b>Day of Remembrance Moment of Silence</b> (9:43 a.m.) Led by Madison Dillow; Cadet Sergeant, Corps of Cadets
9:45 a.m.	<b>Artificial Intelligence: Opportunities and Threats for the Intelligence Community</b> Dr. Jonathan Black, Aerospace & Ocean Systems Lab Director (Moderator) Sarita B., Federal Bureau of Investigation Jasen Halmes, CACI Kirk Jenne, Aveshka, Inc. Karen Metzler, Northrop Grumman
10:45 a.m.	<b>Networking Break and Refreshments</b>
11:00 a.m.	<b>Student Team Presentation</b> - CyberLeaders Teams 1 & 2
11:30 a.m.	<b>Student Team Presentation</b> - SAIC team
12:00 noon	<b>Lunch</b> (Latham Ballroom B)
1:00 p.m.	<b>Workforce Development for Emerging National Security Technologies</b> Caroline Frampton, SAIC (Moderator) Mike B., Central Intelligence Agency Deborah Golden, Deloitte Dr. Patty Finch, Northrop Grumman Kent Pride, Raytheon
2:00 p.m.	<b>Student Team Presentation</b> - CACI team
2:20 p.m.	<b>Break</b>
2:30 p.m.	<b>Technical and Policy Considerations of Cyber Influence Operations</b> Chris S. Anderson, National Security Agency (Moderator) Christopher C., Federal Bureau of Investigation Phil Harvey, Raytheon Dr. Chad Levinson, Virginia Tech School of Public and International Affairs Dr. David Raymond, Virginia Cyber Range
3:30 p.m.	<b>Student Team Presentation</b> - Northrop Grumman Team
3:50 p.m.	<b>Concluding Remarks</b> , Ehren Hill, Outreach Associate Director
4:00 p.m.	<b>Student Poster Session and Reception</b>
6:00 p.m.	<b>Poster Winners Awarded</b> , Dr. Alan Michaels, Electronics Systems Lab Director
	<b>Keynote Address</b> , Dr. T. Charles Clancy, Hume Center Director <i>"Disruptive Technologies and their impact on National Security"</i>

## Student Research Poster Titles

Poster	Title
U 1	Transfer Learning with Google MobileNets for Street Sign Multiclass Classification
U 2	Autonomous Geolocation of an RF Transmitter
U 3	Counterterrorism Strategies in the G5 Sahel
U 4	Hezbollah's Network in Latin America
U 5	Predictive Satellite Analysis using brewlytics
U 6	An Analysis of the Rohingya Refugee Crisis
G 1	The Social Networking of Automobiles
G 2	Working Memory: An Incremental Predictor of Learning and Task Performance
G 3	Helmholtz Cage Development for CubeSat Testing
G 4	Diving Deeper into Fuzzing Performance
G 5	250 kHz Three-Component Velocity Measurements using TRDGV
G 6	3D Printing Maple Seeds as a Covert Surveillance Vehicle
G 7	Blind FHSS Signal Separation
G 8	PRNG-based Key Derivation Function
G 9	Predicting High Density Server Load Variability to Subcool Data Halls
G 10	Accelerating Fault Attacks with Deep Learning
G 11	Machine Learning Object Recognition
G 12	Anomaly Detection in Wind Tunnel Experiments Using PCA
G 13	Adversarial Competition Between US and China
G 14	OpenCL Experimentation
G 15	Designing a rideshare-based fire detection constellation using DISCO-Tech
G 16	Co-Channel Underlay-Based Watermark Authentication
G 17	Radicalization on the Internet: Virtual Extremism in the US from 2012-2017

G - Graduate Student

T - Undergraduate / Graduate TEAM

U - Undergraduate Solo

## Student Research Poster Titles

Poster	Title
G 18	Random Aggregate Spectrum Generation on an FPGA
G 19	A Defense-in-Depth Security Architecture for Software Defined Radios
G 20	Evaluating Adversarial Evasion Attacks Against RFML
G 21	Network Robustness & Resiliency
G 22	Humanitarian Disaster
G 24	Mitigation of Electromagnetic Interference (EMI) for High Power EW Applications
G 25	HPA Predistortion for Spread Spectrum Waveforms
T 1	Analysis of Compression Wave Propagation through Non-Linear Viscoelastic Material
T 2	Systems and Pipelines for Semantic Interaction
T 3	Fake News Detection via Sentiment Analysis
T 4	Insider Threat Detection and Management
T 5	GPS Spoofing Detection via Satellite Fingerprinting
T 6	MDP Path Planning on UAS with ROS and Optitrack
T 7	Fake news detection with BERT
T 8	Cyborg Datasets for Improving RFML
T 9	Autonomous Space Domain Sensor Tasking
T 10	Counting Jeeps: CACI Hume Project
T 11	Improving Warfighter Operations with IoBT
T 12	Future of Spacecraft Electronic Warfare
T 13	HackRFML: Adversarial Threats to RFML Spectrum Sensing
T 14	Quantifying Degradations of Convolutional Neural Networks in Space Environments
T 15	Quallect Machine Learning

G - Graduate Student

T - Undergraduate / Graduate TEAM

U - Undergraduate Solo

## Keynote Speaker and Panelist Biographies

### Keynote Address

**Dr. Charles Clancy** is the Bradley Professor of Cybersecurity in the Department of Electrical and Computer Engineering at Virginia Tech, and is Executive Director of the Ted and Karyn Hume Center for National Security and Technology. With 85 faculty and staff, the Hume Center leverages \$10M to \$15M in annual grants and contracts to engage over 400 students in research and experiential learning focused in national security and technology. Additionally, Dr. Clancy leads efforts in developing and expanding the university's role in cybersecurity research and education. Dr. Clancy is an internationally-recognized expert on topics at the intersection of wireless, cybersecurity, and artificial intelligence, and has testified to Congress on telecommunications security issues.

Prior to joining Virginia Tech in 2010, Dr. Clancy spent seven years working for the National Security Agency in a variety of research, engineering, and operations roles. The majority of his time was spent as a researcher with the Laboratory for Telecommunications Sciences, based at the University of Maryland. There he led government research programs in wireless communications, with an emphasis on software-defined and cognitive radio. His research focused on efficient use of commodity processors for software-defined radio, and security implications involved in military use of cognitive radio technologies. During this time, Dr. Clancy was also heavily involved in wireless authentication and authorization protocol standardization, and held leadership positions within the Internet Engineering Task Force.

Dr. Clancy received his BS in Computer Engineering from the Rose-Hulman Institute of Technology in 2001, his MS in Electrical Engineering from the University of Illinois, Urbana-Champaign in 2002, and his PhD in Computer Science from the University of Maryland, College Park, in 2006. His studies focused on information-theoretic foundations of communications and security.

Dr. Clancy is a Senior Member of the Institute for Electronics and Electrical Engineers (IEEE) and holds leadership positions within IEEE's Communications and Signal Processing Societies. He has previously served as an editor for IEEE Transactions on Cognitive Communications and Networking and IEEE Transactions on Information Forensics and Security. In 2015, Dr. Clancy was elected to be a member of the prestigious AFCEA Intelligence Committee.



### Welcome

**Colonel Paul Mele** was commissioned as a Second Lieutenant in the U.S. Army through the Reserve Officer Training Corps (ROTC) program at The Virginia Military Institute in 1989. An Aviation Officer, his recent assignments include serving as The J5 (Plans Officer) with the Joint Special Operations Command Air Component, Commander of an Attack Aviation Reconnaissance Battalion in 1st Infantry Division, The G3 (Operations Officer) for the U.S. Army Special Operations Aviation Command, and Commander of the Combat Aviation Brigade in the 7th Infantry Division. Most recently he served as the Chief of Staff for the 1st Cavalry Division completing one year in Fort Hood, Texas and the second year in Bagram, Afghanistan during the division's deployment in support of Operation Freedom's Sentinel. He has been the Professor of Military Science for the Virginia Tech and Radford ROTC programs since August of 2017. Colonel Mele is a graduate of The Virginia Military Institute and Virginia Tech where he earned a bachelor's and master's degree in mechanical engineering respectively. He also has master's degrees in national security and strategic studies from The Naval War College and The Army War College. His awards are representative of his years of service and experiences. He has also earned the Ranger Tab, Parachutist Badge, and Master Aviator Badge. Colonel Paul Mele and his wife Julie have been married for 24 years. They have two children, Virginia who is 19 years old and Jake who is 14.

### Artificial Intelligence Panel

**Dr. Jonathan Black** is a Professor in the Kevin T. Crofton Department of Aerospace and Ocean Engineering at Virginia Tech (VT), the Director of the Aerospace Systems Lab of the Ted and Karyn Hume Center for National Security and Technology, a member of the Center for Space Science and Engineering Research (Space@VT), and the Northrop Grumman Senior Faculty Fellow in C4ISR. Prior to joining VT, Dr. Black served as a faculty member in the Aeronautics and Astronautics department at the Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, Ohio. There he was the founding Director of the Center for Space Research and Assurance. As Director, Dr. Black focused the center's efforts on the execution of cutting-edge space technology development and scientific space experiments; managed and executed the annual \$2 million center research portfolio; supervised a diverse group of 20 consisting of research faculty, program managers, laboratory and administrative staff, graduate students, and summer interns; briefed senior Department of Defense and Intelligence Community leadership advising national strategy; and cultivated research and educational relationships inside and outside AFIT. He served as PI or Co-PI on five spaceflight experiments. At VT, Dr. Black works across academic departments and multiple research centers at the intersection of mission platforms and mission payloads. His research focuses on the ability to analyze sensor inputs onboard in low-SWAP, heterogeneous computing environments, such that the payload can autonomously identify objects in its environment; the ability for high-level mission priorities to drive low-level technical processes in real time with the human out of the tactical loop but rather operating in a strategic control role; and the ability to manage payload resources according to mission goals in a distributed manner across several self-organizing nodes. Dr. Black's research interests include space and atmospheric vehicle dynamics, linear and nonlinear control theory, autonomous vehicle design, structures, structural dynamics, advanced sensing technologies, space systems engineering, and novel orbit analysis for a wide variety of military and intelligence applications including large lightweight space structures, micro UAV development, and taskable satellites.

**Sarita B.** works as an analyst for Federal Bureau of Investigation. Sarita has been working with the FBI for the past 9 years. For the first part of her career at the bureau Sarita worked on Counterterrorism matters at the Washington Field Office. Currently she is working on Counterintelligence matters at FBI Headquarters. Prior to her bureau career with the FBI, Sarita worked with the founder of Alternative Behaviors a counseling center in Virginia assisting families on the implementation of written behavioral intervention plan and addressing behavioral issues in young children. Sarita has a Master's in Statecraft and International Relations from Institute of World Politics and a Bachelors in International Relations with minor in Sociology from Drake University in Des Moines, Iowa.

**Jasen Halmes** is the Director of Artificial Intelligence for CACI, Inc. He has worked as a member of the National and Cyber Solutions (NCS) Business Group for over a decade in support of U.S. Intelligence and Defense communities. His past roles have included software developer, software architect and big data analytics developer. Jasen is currently responsible for applications of Artificial Intelligence, Machine Learning, and Deep Learning across CACI. He currently supports research and development efforts in areas such as Computer Vision, Natural Language Processing, and Cyber Defense applications utilizing Machine Learning and Deep Neural Networks. Mr. Halmes received his Bachelor of Science degree in Computer Science from Montana Tech in 1996 and his Master of Engineering degree in Computer Science from the University of Colorado in 2008.

**Kirk E. Jenne** is the VP for Defense and Intelligence at Aveshka, Inc., with responsibility for overseeing high-end cybersecurity initiatives and plans in support of DoD and government organizations. He retired from federal civilian service in 2018 after more than 34 years with the U.S. Navy. He has been in various research and engineering positions while at the Naval Research Laboratory, Naval Undersea Warfare Center, and then as Program Officer for the Chief Scientist/Director of Research at the Office of Naval Research, where he provided leadership and oversight to a broad research portfolio for research centers within NAVSEA, NAVAIR, and SPAWAR. He was Chief Technology Officer for the Naval Surface Warfare Center Enterprise, and he provided leadership for establishing NAVSEA's first Cyber Red Team while Director of the Naval Engineering Education Consortium (NEEC).

## Panelist Biographies

**Karen Metzler** joined Northrop Grumman in 2009 and currently serves as the strategy director for the corporation's Artificial Intelligence Campaign. In her role she is responsible for execution of a corporate-wide initiative to accelerate the integration of Artificial Intelligence capabilities into our customers' systems, programs and advanced research. Ms. Metzler works with organizations across the company combining the mission and domain expertise with AI technologies to drive new solutions to our evolving customer needs. Ms. Metzler is also developing strategies to expand AI expertise across our workforce and AI talent recruitment and retention. She has 30 years of experience in both strategy and profit/loss roles across DoD and intelligence community programs. She has managed engineering, development and analytic contracts across multiple government agencies. She holds a MS Degree in Computer Science/AI from George Washington University and a BS in Computer Science from the University of Hartford.

### Workforce Development Panel

**Caroline S. Frampton** is the Vice President of the Engineering, Integration and Logistics Practice at Science Applications International Corporation (SAIC). She has more than 29 years of experience working in the Intelligence Community as a government employee and consultant. She has held various leadership, technical and engineering positions on programs where she and her team delivered some of our nation's most advanced technologies. In her current position, she leads SAIC's engineering and logistics solution development and workforce transformation strategies for defense, intelligence, and federal civilian customers. She has managed a technical, scientific and engineering workforce with as many as 1,500 employees and developed a workforce optimization strategy for her team to enable the company to realize its long-term business goals. Ms. Frampton was instrumental in planning and implementing two major corporate acquisitions, which involved the integration of 1,500 and 7,500 new employees while minimizing impact to ongoing program operations. She also assisted with planning and implementing two enterprise-wide reorganizations that streamlined operations and better positioned the company for profitable growth.

**Mike B.** is currently serving as the Deputy Associate Director of CIA for Talent where he oversees the Agency's employee training programs and professional development. He began this assignment in April 2018. Mr. B. has also served as the Director of the Office of Advanced Analytics in the Directorate of Analysis, Deputy Director of the Office of Resources and Support in the Directorate of Analysis, and as the Deputy Director of the Office of Collection Analysis, Strategies, and Advanced Analytics (CASAA). Prior to his CASAA assignment, Mr. Burns served as the Directorate of Intelligence's Chief of Staff (COS), from February 2012-July 2013, where he oversaw the day-to-day operations of the DI front office. Immediately following 9/11/2001 Mike was selected to serve as the Executive Officer in the DI's newly created Office of Terrorism Analysis (OTA). Before moving to OTA, Mr. Burns was the Executive Officer for the Directorate of Intelligence. Mike holds a B.A. from Virginia Tech with a double major in Political Science and Urban Planning. He did graduate work at the University of Virginia and American University, and has completed executive leadership programs at Harvard University's Kennedy School of Government and Northwestern University's Kellogg School of Management.

**Deborah Golden**, principal, Deloitte & Touche LLP, is the Government & Public Services (GPS) Cyber Risk Services leader, as well as the GPS Advisory Market Offering leader, GPS Empowered Well-being leader, and the lead principal for a major federal government health care provider. Golden has 25 years of information technology experience spanning numerous industries with an in-depth focus on government and public services, life sciences and health care, and financial services. She specializes in collaborating with clients on cybersecurity and technology transformation, and privacy & governance initiatives. Additionally, she serves on Virginia Tech's Accounting and Information Systems Board and the Masters in Information Technology Advisory Board. Golden is an active speaker and author on cybersecurity top-of-mind issues and women in cyber mentoring. Golden's insights have also been published in The Wall Street Journal and FCW on the topics of multifactor authentication and thinking like an adversary. She has appeared in numerous news outlets including Federal Times and Federal News Radio on issues ranging from biometrics to cyber simulations.



**Dr. Patricia “Patty” Finch** is the Director, Technical Development Center of Excellence for Northrop Grumman Mission Systems, Engineering & Sciences, and leading Technical Development activities for the sector to include: Rotational & Development Program, Applied Learning, and Academies. In this role, Dr. Finch is responsible for providing guidance and establishing processes for growing our technical workforce and enabling them to perform at the highest level. Over the course of her nearly 24 year career, she has participated in several workforce development activities across Industry and Academia. She received a BS from Washington College, an MS from Syracuse University and Webster University, and a PhD from Capella University.

**Kent Pride** is Director of University Partnerships for Raytheon Intelligence and Information Services (IIS). Raytheon Company, with 2018 sales of \$27 billion and 67,000 employees, is a technology and innovation leader specializing in defense, civil government and cybersecurity solutions. IIS is a global leader in intelligence, surveillance and reconnaissance; advanced cyber solutions; weather and environmental solutions and information-based solutions. Kent became the Director of University Partnerships for the IIS Engineering & Technology organization in March of 2015. In this role he is responsible for developing and implementing a strategy to develop strong partnerships with a number of universities where IIS can align the use of our research investments, education assistance dollars, recruiting resources, internships and other collaborative activities to maximize the ROI in technology research and insight into the best and brightest recruits. Kent brings more 40 years of engineering and program management experience to this position. His engineering management areas of expertise include development for large programs with specific emphasis on software, systems and hardware engineering, algorithm development, aeronautical engineering, quality and manufacturing. Kent holds a bachelor’s degree in physics from Mississippi College, and has obtained Raytheon certifications in Program Management. He currently serves on the industry advisory board (Chair) for the School of Engineering and the Darwin Deason Cyber Security Institute both at Southern Methodist University.

### Cyber Influence Operations Panel

**Chris S. Anderson** is the NSA Technical Leader of their Analytic Platforms Security Team. He enhances the security posture of critical national security information systems by leading efforts with the organization’s compliance to DoD’s Risk Management Framework, development of Big Data security technology and tools, and collaboration on Trusted Computing Group standards with virtualized platforms. He serves as the NSA Academic Liaison to several universities that are Centers of Academic Excellence in Cyber Defense including Virginia Tech where he also engages on their Cyber Operations focus. He graduated from Virginia Tech in 1986 with a Bachelor’s Degree and from UVA in 1989 with a Master’s Degree both in Mechanical Engineering. He is a licensed Professional Engineer in the State of Maryland, holds several industry certifications such as CISSP and MCSE, as well as holds one U.S. patent.

**Christopher C.** is a Supervisory Special Agent (SSA) in the Federal Bureau of Investigation’s Cyber Division. SSA C. began serving the FBI in 2009, where upon graduation from the Academy, he was assigned to the FBI’s-flagship New York Division. While in New York, Christopher was assigned to investigate cyber-criminal matters, specifically cases involving Anonymous/Lulzsec, Silk Road, ransomware, carding, and money mules as facilitated through the Zeus financial trojan. In 2015, SSA C. was promoted to Supervisory Special Agent at FBI Cyber Division Headquarters in Washington, DC, serving the Middle East Africa Unit (MEAU). MEAU’s mission is to support the FBI’s National Cyber Security Mission as it pertains to nation state-sponsored cyber threats against the US and its international partners. In 2019, Christopher was promoted to Field Supervisor in the Richmond Division, supervising both the Cyber Squad and Computer Analysis Response Team, where he currently serves today. Prior to the FBI, Christopher worked as an Oracle Systems Administrator for Ricoh North America and Agere Systems/Lucent Technologies. Christopher is a graduate of The Pennsylvania State University with a Bachelor’s Degree in Pre Law and Master’s Degree in Cyber Security and Information Assurance.

## Panelist Biographies

**Phil Harvey** is a Principal Engineering Fellow and is the Chief Security Engineer on a DHS national cyber protection program at Raytheon. He previously held the Technical Director position for the Cybersecurity and Special Missions business within Raytheon Intelligence, Information and Services. Harvey has over 25 years of experience in system design, integration and testing of cybersecurity, communications, and ISR (intelligence, surveillance and reconnaissance) systems. He has spent the past six years developing and leading a variety of strategic initiatives within Raytheon aimed at helping international, federal, civil, and government customers solve their toughest cyber challenges. Harvey has led cross-corporation internal research and development (IRAD) activities, including the development of cyber hardening and dynamic cyber defense tools and capabilities. With his technical leadership, Harvey directed cybersecurity strategies and investments that drove the growth Raytheon's cyber business. Harvey has a bachelor of science in electrical engineering and computer science from the University of California, San Diego. He is currently pursuing a Masters of Engineering in Cybersecurity Governance and Policy at George Washington University.

**Dr. Chad Levinson** is an assistant professor in SPIA's Government and International Affairs program based in the National Capital Region. His research focuses on U.S. national security politics, with a particular interest in propaganda, civil society, information warfare, and the presidency. He has been a research fellow in the International Security Program at the Harvard Kennedy School's Belfer Center and the Stanley Kaplan Postdoctoral Fellow at Williams College. He earned his doctorate in political science from the University of Chicago in 2017, where he served as a preceptor for the Committee on International Relations. His work includes experimental, quantitative, and historical research on propaganda and information warfare, and has appeared in *Presidential Studies Quarterly*. He worked in the technology industry for ten years as an information architect, database designer, and programmer before returning to university to pursue a Ph.D.

**Dr. David Raymond** is Director of the Virginia Cyber Range and Deputy Director of Virginia Tech's IT Security Lab. He is also adjunct faculty in the Bradley Department of Electrical and Computer Engineering where he teaches networking and cybersecurity courses. David is a retired Army officer and former faculty member in West Point's Department of Electrical Engineering and Computer Science. He has a BS in Computer Science from the United States Military Academy at West Point, an MS in Computer Science from Duke University, and a PhD in Computer Engineering from Virginia Tech. David is a Senior Member of the IEEE and is co-author of *On Cyber, Towards an Operational Art for Cyber Conflict*.



Distinguished Members

**CACI**

EVER VIGILANT



**SAIC**

Principal Members

**BAE SYSTEMS**

**Deloitte.**



**MITRE**

**NASIK**

