Cybersecurity
Symposium 2016

Speakers and Authors
OCTOBER 27, 2016
ICF Conference Center | Fairfax, Virginia

CyberSci
symposium 2016

Giorgio Bertoli—Senior Scientific Technical Manager, U.S. Army Offensive Cyber Intelligence and Information Warfare Directorate, Communications-Electronics Research Development and Engineering Center, U.S. Army Research Development and Engineering Command

Collateral Effect Potential Metric for Computer Exploits

With 22 years of federal service, George Bertoli has extensive experience in cyber, electronic warfare, and military tactics both as a civilian and as a former active duty soldier. His primary research areas include the development of advanced electronic warfare, computer network operations, and cyber and quick reaction capability technologies. He is also a highly proficient programmer in several computer languages and a subject matter expert in genetic algorithms and software agent technology. With master's and bachelor's degrees in electrical engineering from the New Jersey Institute of Technology and a second master's degree in computer science from the University of Massachusetts at Amherst, Mr. Bertoli is also a certified information systems security professional. During his 6.5-year military career, he served as a combat engineer; was stationed in Germany, Ft. Bragg, and Korea; and was deployed as part of Operations Desert Shield and Desert Storm.

Dr. Misty Blowers—Vice President, Cybersecurity Research Programs, ICF

Beyond the Government: Mobilizing Industry and Academia Panel

Prior to serving as Vice President for Cyber Security Research at ICF, Dr. Misty Blowers led the cyber offensive research team at the United States (U.S.) Air Force Research Laboratory, Information Directorate, where she has managed over $95 million in government contracts. Dr. Blowers obtained her PhD from the SUNY College of Environmental Science and Forestry in applied science and engineering and a MS in computer science from Syracuse University. She gained extensive industrial experience as a chemical process engineer for a world leading manufacturing equipment supplier and blends this multifaceted background with knowledge of cyber operations to allow for substantial contributions to the security of cyber physical systems and the Internet of Things. Dr. Blowers combines hands-on practical knowledge with extensive research experience in the fields of machine learning, big data analytics, total systems engineering, modeling, and simulation. She has authored over 50 publications and provided plenary talks on behavior analysis of manufacturing processes and the future of cyber physical systems.

Timothy J. Cash—Senior Consultant, Timothy J. Cash and John W. Link
(John W. Link, Co-presenter)

Protecting the U.S. Infrastructure from Attacks via Electromagnetic Emissions from Devices

Timothy Cash has more than 30 years' experience as a senior systems engineer in military, government, and commercial business sectors, providing hands-on technical development of radio frequency, cellular, microwave, optical fiber, and satellite communications networks. He has been involved in nearly every aspect of technology development, including project management, test and evaluation, requirements analysis, development of concept of operations, creation of network architecture plans, test cases for communications networks, reverse engineering, and troubleshooting. In addition, he has worked in physical- and data-layer circuit testing; hardware design, development, and installation; and microwave path analysis and verification. In addition to his technical portfolio, Mr. Cash has a bachelor's degree in physics and mathematics from Indiana University, Bloomington; an associate of arts degree from United Electronics Institute; and project management certification.

Dr. Edward Colbert—Network Security Branch Cybersecurity Scientist, U.S. Army Research Lab (ARL)
(Daniel Sullivan, Co-presenter)

Cybersecurity Risks in the Industrial Internet of Things

Edward Colbert is a researcher at ARL in Adelphi, Maryland, where he conducts novel security research on methods for defending Army Supervisory Control and Data Acquisition (SCADA) and ICS systems. Before working for ARL, he was research fellow at ICF and has performed telecommunications research for the U.S. Department of Defense, Verizon, and Johns Hopkins University Applied Physics Laboratory. Dr. Colbert holds a research professorship at the Catholic University of America in Washington, DC, and has published in 50 refereed journals. He holds a PhD and an MS in astronomy from the University of Maryland and an MS in physics and BS in engineering physics from the University of Illinois.

Dr. Jennifer Cowley—Human Factors Psychologist, CERT/Software Engineering Institute/Carnegie Mellon University

Social Networking Tools May Accidentally Increase Insider Threat: The Unintended Psycho-social Effects on False Positive Indicators of Insider Threat

Dr. Jennifer Cowley is a principal investigator in the CERT Division at the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. Her research focuses on cybersecurity team selection, expertise development, indices of insider threat, and risk perception. Her research interests also include human error, warning system design, and development of tests/measures of psychological phenomena that impact human performance. She holds a PhD in human factors psychology from North Carolina State University, and during her graduate studies, she worked as a user interface designer at SAS Institute, Inc. and interned at MITRE Corporation.

Dr. Peter Eckersley—Chief Computer Scientist, Electronic Frontier Foundation

Cybersecurity and Privacy Panel

As Chief Computer Scientist for the Electronic Frontier Foundation, Dr. Peter Eckersley leads a team of technologists who watch for technologies that, by accident or design, pose a risk to computer users' freedoms—and then look for ways to fix them. Dr. Eckersley's work at EFF has included privacy and security projects such as Let's Encrypt and Certbot, Panopticlick, HTTPS Everywhere, and the SSL Observatory; helping to launch a movement for open wireless networks; fighting to keep modern computing platforms open; helping to start the campaign against the SOPA/PIPA Internet blacklist legislation; and running the first controlled tests to confirm that Comcast was using forged reset packets to interfere with P2P protocols. Dr. Eckersley holds a PhD in computer science and law from the University of Melbourne; his research focused on the practicality and desirability of using alternative compensation systems to legalize P2P file sharing and similar distribution tools while still paying authors and artists for their work.

Jason Ellis—Analyst, ICF
(Steve Hutchinson, Co-presenter)

Value-of-Information (VoI) Sensitive Cyber Sensor

Jason Ellis is a software developer with ICF, contracted to the U.S. Army Research Laboratory. His interests currently center around the development of novel network traffic collection and representation formats that enhance the intrusion detection process. He obtained a master's degree in computer science with a concentration in cybersecurity from Johns Hopkins University and a bachelor's degree in mathematics and computer science from Gettysburg College.

General Michael Hayden—Former Director, Central Intelligence Agency; U.S. Air Force, Retired

Cybersecurity and Privacy Panel

General Michael Hayden is a retired four-star general who served as director of the Central Intelligence Agency and the National Security Agency when the course of world events was changing at a rapid rate. As head of the country's premier intelligence agencies, he was on the frontline of global change, the war on terrorism and the growing cyber challenge. He understands the dangers, risks, and potential rewards of the political, economic, and security situations facing us. In addition to leading CIA and NSA, General Hayden was the country's first principal deputy director of national intelligence and the highest-ranking military intelligence officer in the country. In all of these jobs, he worked to put a human face on American intelligence, explaining to the American people the role of espionage in protecting both American security and American liberty. General Hayden also served as commander of the Air Intelligence Agency and Director of the Joint Command and Control Warfare Center and served in senior staff positions at the Pentagon, at U.S. European Command, at the National Security Council, and the U.S. Embassy in Bulgaria. He was also the deputy chief of staff for the United Nations Command and U.S. Forces in South Korea. General Hayden is currently a principal at the Chertoff Group and a distinguished visiting professor at the George Mason University School of Policy, Government and International Affairs. He is on the board of directors of Motorola Solutions in and serves on a variety of other boards and consultancies.

Dr. David Honey—Director, Science and Technology, Assistant Deputy Director of National Intelligence for Science and Technology

Beyond the Government: Mobilizing Industry and Academia Panel

As the Director, Science and Technology, and as the Assistant Deputy Director of National Intelligence for Science and Technology, Dr. David A. Honey is responsible for the development of effective strategies, policies, and programs that lead to the successful integration of science and technology capabilities into operational systems. Prior to this assignment, Dr. Honey served as the Deputy Assistant Secretary of Defense, Research, in the Office of the Assistant Secretary of Defense (Research and Engineering) where he was responsible for policy and oversight of DoD Science and Technology programs from Basic Research through Advanced Technology Development. He was also responsible for oversight of DoD laboratories, ensuring the long-term strategic direction of the Department's S&T programs, and for developing those technologies needed for continued technological superiority of US forces. Dr. Honey was the Director of the Defense Advanced Research Projects Agency (DARPA) Strategic Technology Office (STO), Director of the Advanced Technology Office (ATO), and Deputy Director and Program Manager of the Microsystems Technology Office (MTO).

The Honorable Patricia Hoffman—Assistant Secretary, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy

Cybersecurity and Privacy Panel

Patricia Hoffman was named Assistant Secretary for the Office of Electricity Delivery and Energy Reliability (OE) at the United States Department of Energy (DOE) in June 2010 after serving as Principal Deputy Assistant Secretary for OE since November 2007. Assistant Secretary Hoffman provides leadership on a national level on electric grid modernization, enhancing the security and reliability of the energy infrastructure and facilitating recovery from disruptions to the energy supply. This is critical to meeting the nation's growing demand for reliable electricity by overcoming the challenges of our nation's aging electricity transmission and distribution system and addressing the vulnerabilities in our energy supply chain. Ms. Hoffman holds a Bachelor of Science and a Master of Science in ceramic science and engineering from Pennsylvania State University.

Steve Hutchinson—Technical Specialist, ICF

(Jason Ellis, Co-presenter)

Value-of-Information (VoI) Sensitive Cyber Sensor

Steve Hutchinson is a researcher-analyst with ICF, contracted to the U.S. Army Research Lab. As an engineer in the chemical/pharmaceutical industry, he has led projects in manufacturing control, laboratory data acquisition, web-based applications, and knowledge-based systems development. His current research interests concern representation of network traffic and session behavior features to support quality decision making in hybrid, human-machine processes. He earned an MS in mathematics education from Drexel University, graduate studies in computer science at Rochester Institute of Technology, and a BS in electrical engineering from the State University of New York at Buffalo.

John W. Link—Senior Consultant, The Lever Group

(Timothy J. Cash, Co-presenter)

Protecting the U.S. Infrastructure from Attacks via Electromagnetic Emissions from Devices

John Link is a senior consultant with The Lever Group, providing IT capital planning investment control and organizational strategy for FEMA. He has 30 years' experience providing expert guidance in "human stuff" (organizational dynamics, strategy, technical integration and collaboration, and strategic communications) for a wide range of IT organizations, including corporate, government, and nonprofit clients. Mr. Link worked for the Army Chief of Staff for Installation Management CIO on IT strategy, policy, and knowledge management and was a charter senior member of the governance team for the DOD OSD CIO/NII Horizontal Portfolio Initiative, one of the first demonstrations of cloud-based information-sharing initiatives in DOD/IC. Mr. Link has an MS from George Mason University School for conflict analysis and resolution and a BA in English from the University of Virginia.

Dr. Edmund C. Mitchell—Chief Business Development Officer, CSIOS Corporation

Cyber and Intelligence Research and Development Funding Strategy

Edmund C. Mitchell is a distinguished executive officer and business strategist with more than 30 years' experience in various areas encompassing business development, capture strategies, and portfolio and program management. Dr. Mitchell has a career history identifying, qualifying, advocating, and tracking portfolios of qualified contract leads; creating business and research and development funding capture strategies for private and public organizations; and managing proposal lifecycles for clients in the defense, aerospace, and federal sectors. He is a retired veteran of the United States Marine Corps.

Dr. Robert Mitchell—Scientist, Sandia National Laboratories

Recent Developments in Linkography-based Cybersecurity

Before working for Sandia National Laboratories in the Cyber Security Technologies Department, Dr. Mitchell was a programmer at Boeing, BAE, Raytheon, and Alcatel-Lucent. His research interests include moving target defense, computer network defense, computer network exploitation, cyber physical systems, reverse engineering, game theory, machine learning, intrusion detection systems, modeling, and simulation. A former officer in the United States Air Force, he earned PhD, MS, and BS degrees in computer science from Virginia Tech.

Timothy Obenshain—Project Manager, ICF

Ransomware over the Past 5 years: Overview and Best Practices

Timothy Obenshain has been an ICF contractor for the U.S. Army Research Lab (ARL) and HPCMP CDSP since 2008. He started work as an entry-level network security analyst and is now a project manager in support of ARL CDSP's Information Security Continuous Monitoring Solution.

Dr. Dhananjay Phatak—Associate Professor, University of Maryland, Baltimore County (UMBC)

Securing Cyber Physical Systems

Dhananjay Phatak has been an associate professor of computer engineering in the Cyber Physical Systems Department at UMBC since 2000. His current research interests are in computer arithmetic algorithms and their h/w realizations and all aspects of cyber/information/data/computing/network/systems security. His research has been supported by NSF, NSA, and local companies (Aether Systems Inc., and Northrup Grumman), and he received the NSF Career Award in 1999. In the past, he has worked in many other areas, including development of the worldwide web; mobile and wireless Internet protocols; sensor networks; and most recently, security. Dr. Phatak received his PhD in computer systems engineering and MSEE in electrical engineering from University of Massachusetts at Amherst and B. Tech from IIT Bombay (Mumbai) in electrical engineering.

Joseph Shaheen—Researcher, NATO STRATCOM COE and George Mason University

Modeling, simulation, and analysis of a Social Media Propaganda Network: The Case of ISIS/ISIL/Daesh

Joseph Shaheen is a researcher and analyst working with various governmental and non-governmental agencies to build modeling and analysis tools methods. Previously, Mr. Shaheen worked with NATO STRATCOM to study and explain the methods by which ISIS/ISIL/DAESH disseminated propaganda on social media through the use of social network analysis methodology. Mr. Shaheen earned a bachelor's degree in physics, an MBA, and is currently pursuing his doctorate degree at George Mason University's Computational Social Science program. His work focuses on the intersection of agent-based modeling and simulation, network analysis, and policymaking. Mr. Shaheen is also associated with the Mitre Corporation.

Sidney "Chuck" Smith—Computer Scientist, U.S. Army Research Lab (ARL)

The Use of Entropy in Lossy Network Traffic Compression for Network Intrusion Detection Applications

Chuck Smith began his career in information assurance in the U.S. Army as a systems administrator. He has served as an information systems security officer, information assurance security officer, information assurance network manager, information assurance program manager, agent of the Certification Authority, and privacy officer. In January 2010, Mr. Smith was hired as team leader for the ARL product integration and test team. He is both a Certified Information System Security Professional and a Certified Information Systems Auditor. He is further certified in Security+, National Security Agency INFOSEC Assessment Methodology and INFOSEC Evaluation Methodology. He holds master's and bachelor's degrees in computer science from Towson University, where he is current working on his doctorate.

Daniel Sullivan—Senior principal software engineer, Raytheon Company and Supervisory Control and Data Acquisition (SCADA) Researcher, U.S. Army Research Lab (ARL)

(Dr. Edward Colbert, Co-presenter)

Cybersecurity Risks in the Industrial Internet of Things

Daniel Sullivan is a senior principal software engineer at the Raytheon Company and a member of the ICF team supporting ARL in Adelphi, Maryland. At ARL, he researches methods to defend the SCADA and ICS systems. He received his MS in electrical engineering from the Naval Postgraduate School and his BS in electrical engineering from the University of Illinois.

Era Vuksani—Assistant Staff, Cyber Systems and Operations Group, Massachusetts Institute of Technology Lincoln Laboratory

A Data-Stream Classification System for the Investigation of Terrorist Threats

Era Vuksani is an Assistant Staff member in the Cyber Systems and Operations Group at MIT Lincoln Laboratory. She joined the Laboratory in October 2012 and is currently working in data analytics and network reconnaissance. Previously, she has worked on a variety of topics, ranging from cyber modeling and simulations of attackers, defenders, and missions, to moving target analytics, to metrics about attacker and defender actions and strategies. Her interests include software engineering, big data analysis, attacker/defender strategies, password research, simulation work in different fields, and learning and teaching computer security via interactive media. Ms. Vuksani earned a BA degree with honors in computer science at Wellesley College in 2012. Her thesis dealt with teaching about attackers and defenders in computer networks and was done in conjunction with Lincoln Laboratory.

Mark Weatherford—Senior Vice President and Chief Cybersecurity Strategist, vArmour

Cybersecurity and Privacy Panel

Mark Weatherford has more than 20 years of security operations leadership and executive-level policy experience in some of the largest and most critical public and private sector organizations in the world. At vArmour, Mr. Weatherford focuses on helping customers understand the rapidly evolving cybersecurity needs of the cloud and 21st century data center technologies while expanding vArmour's global customer-base across government and commercial markets. Prior to joining vArmour, he was a Principal at The Chertoff Group where he worked with businesses and organizations around the world create strategic security programs and he remains a Senior Advisor in the firm. In 2011, Mr. Weatherford was appointed by President Obama as the Department of Homeland Security's first Deputy Under Secretary for Cybersecurity and before DHS, he was the Vice President and Chief Security Officer at the North American Electric Reliability Corporation (NERC) where he directed the cybersecurity and critical infrastructure protection program and worked with electric utility companies across North America.
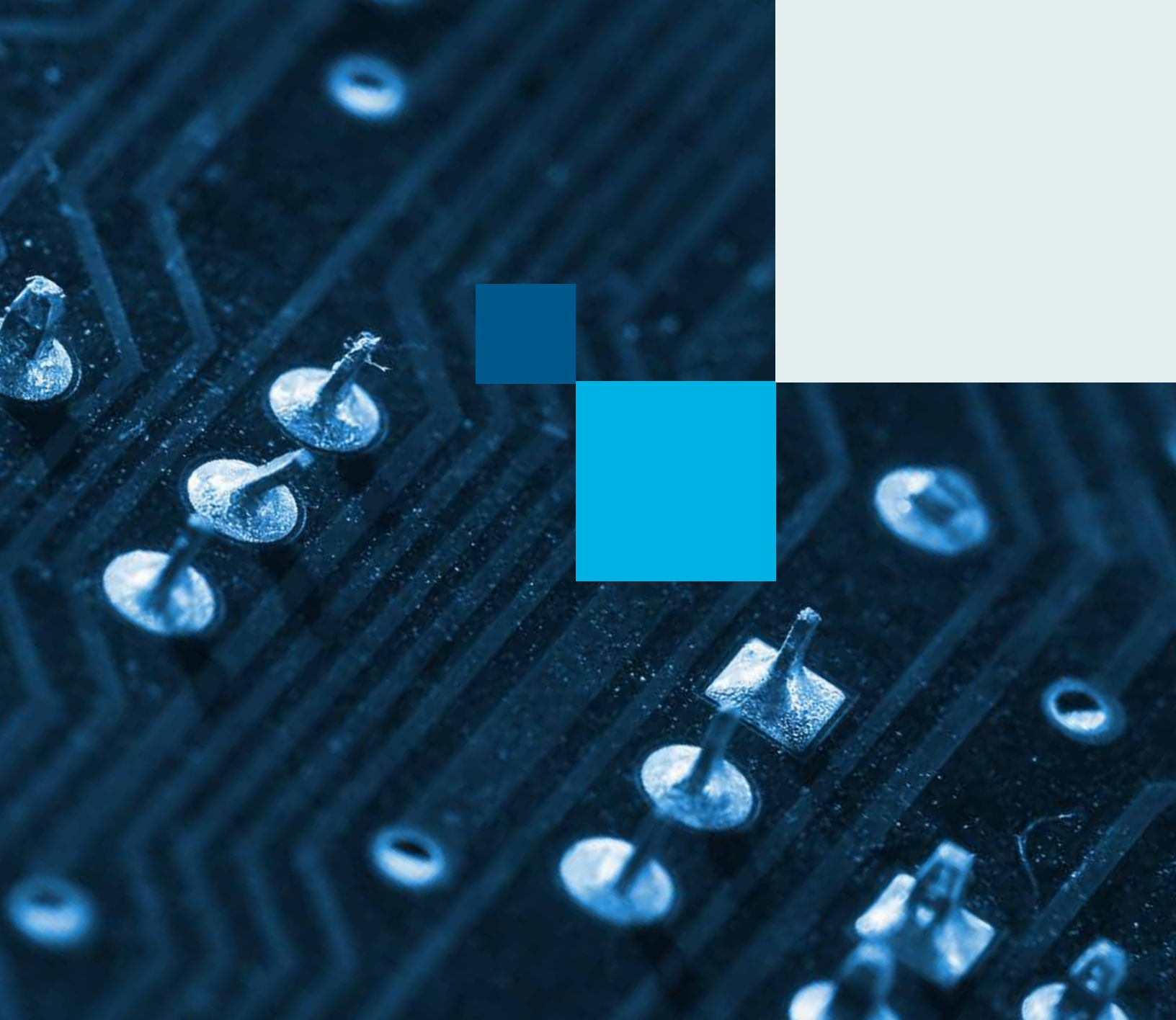
About ICF

ICF (NASDAQ:ICFI) is a global consulting and technology services provider with nearly 6,000 professionals focused on making big things possible for our clients. We are business analysts, public policy experts, technologists, researchers, digital strategists, social scientists, and creatives. Since 1969, government and commercial clients have worked with ICF to overcome their toughest challenges on issues that matter profoundly to their success. Come engage with us at **icf.com.**