



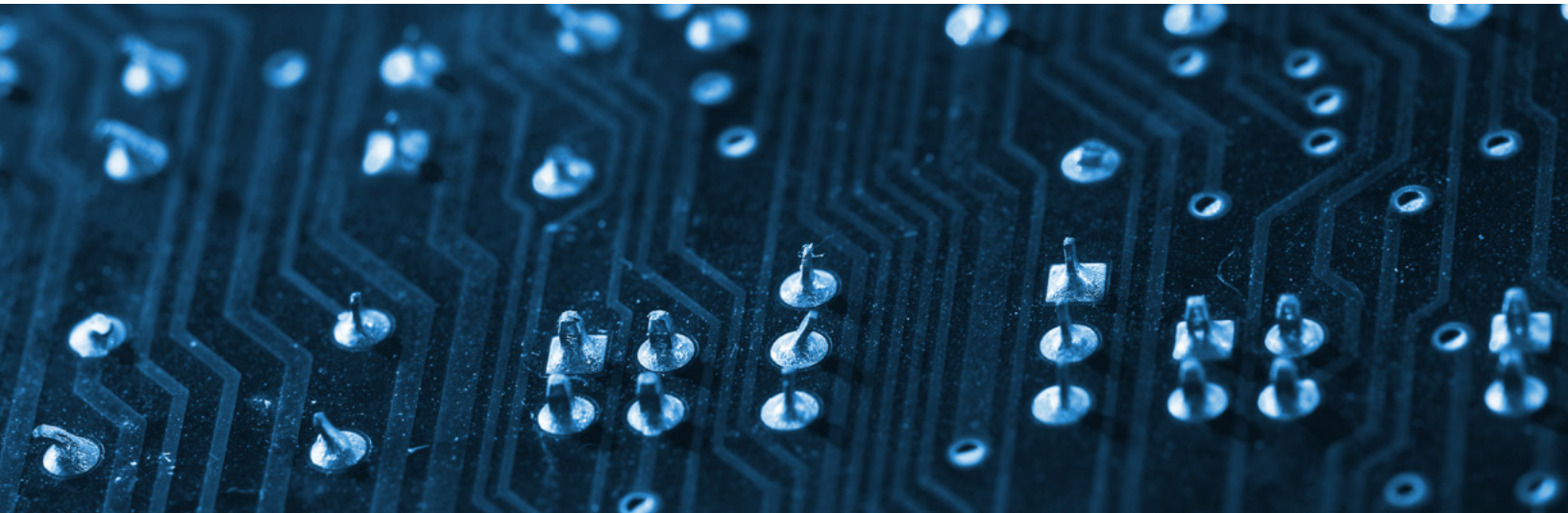
# CyberSci Symposium

## 2016 Proceedings

**CyberSci**  
symposium2016

## Table of Contents

Introduction.....	2
Symposium Goals.....	3
Cybersecurity Research and Development Recommendations for the 45th President of the United States.....	4
Expert Panel Recaps .....	9
Breakout Session Recaps.....	12
Keynote Presentation Summaries.....	25
Speaker List.....	30



## Introduction

This document conveys proceedings from the ICF Cybersecurity Research and Development Symposium 2016, the theme of which was "Cybersecurity Research and Development: Recommendations for the 45th President of the United States." The symposium brought together experts from industry, government, and academia to share the important developments in cybersecurity research and development (R&D). The event took place October 27 at ICF's headquarters in Fairfax, Virginia.

### The symposium comprised three panels:

- Cybersecurity and Privacy
- The Future of Cyber Operations and Technologies
- Beyond the Government: Mobilizing Industry and Academia

### Technical presentations were organized in three tracks:

- Cybersecurity in the Service of National Security
- Securing the Emerging National Smart Infrastructure
- Cybersecurity and the Social Network

Technical track presentations were selected through anonymous peer review. Presentations ranged from improving cybersecurity analysis and protecting cybersystems from electromagnetic pulse to developing cybersecurity R&D funding strategies.

Summaries of the keynote speeches are provided along with recaps of the panel discussions and breakout sessions. Following the symposium, ICF prepared summary recommendations to the 45th president of the United States concerning cybersecurity R&D. Those recommendations are presented here and represent the opinions of ICF, not necessarily those of individual CyberSci 2016 panelists and presenters. They reflect whole-of-nation cybersecurity R&D concerns rather than specific R&D efforts or cybersecurity technologies.

## Symposium Goals

Building on the success of its previous four predecessor events, CyberSci Symposium 2016 brought together industry, government, and academia for a unique gathering. Designed with size and scope to foster the sharing of ideas, the symposium allowed participants to interact and build on those shared ideas together, both in real time and upon return to their respective institutions.

Three keynote speakers addressed the shared cybersecurity context for all participants. Three expert panels and eight breakout sessions offered in-depth information about issues facing cybersecurity R&D and current R&D work.

In his opening remarks, Sudhakar Kesavan, ICF chairman and chief executive officer, gave an overview touching on key points that later presenters would revisit:

- Cybersecurity arises in every boardroom, reflecting a new level of anxiety and sense of inevitability about cyber attacks and exploits.
- We see how foreign players are using cyber to influence us and to diminish or destabilize our institutions.
- Gatherings like CyberSci are important and encouraging, gathering the industry's thought leaders to address work that matters so profoundly, solving problems of national importance, and sharing a mission orientation.

Event Chairman Samuel S. Visner, ICF senior vice president for cybersecurity and resilience and professor, Cybersecurity Policy, Operations, and Technology, Georgetown University, welcomed participants and shared his goals for the symposium's juxtaposition of cybersecurity concepts, policy, and technology:

- Use the opportunity to advance the cybersecurity R&D state of thinking and inform future action by speaking and listening, sharing and learning.
- Appreciate the advantage cybersecurity R&D can represent for the United States if we get it right.
- Understand the added complexity of working within our legal and regulatory framework.

# Cybersecurity Research and Development Recommendations for the 45th President of the United States

## General Observations

The cybersecurity R&D establishment of the United States covers a broad range of disciplines with deep and substantial resources invested in many areas vital to the nation's protection. Important work is underway to characterize the behavior of complex networks, including those that serve the nation's critical infrastructure, which is managed increasingly by IT. These "smart" infrastructures reflect the continuing interconnection of "traditional" enterprise IT systems and the IoT—the system of interrelated internet protocol-enabled devices from which we can extract important data and through which we manage these infrastructures. Impressive research also is under way to detect anomalous behavior in such complex networks as well as to detect, block, and mitigate advanced cyberthreats—including threats without known signatures. Researchers are probing the vulnerability of our cybersystems—including critical infrastructures—to electromagnetic pulse. Other researchers are examining the links between threats to cybersecurity and the use of social networking tools.

The range of organizations involved in cybersecurity research is impressive. Cybersecurity R&D is being conducted by the DoD—including the Army Research Laboratory, Navy Research Laboratory, Air Force Research Laboratory, Defense Advanced Research Projects Agency, and the Cybersecurity Information Analysis Center of the Defense Technical Information Center—the U.S. Department of Energy's National Laboratories, federally funded R&D centers (e.g., the Software Engineering Institute and MITRE), National Institute of Standards and Technology, various universities, and numerous private sector companies specializing in cybersecurity products and technology. Published in February 2016, the Federal Government Cybersecurity Research and Development Strategic Plan "establish[ed] the direction for the Federal R&D enterprise in cybersecurity science and technology (S&T) to preserve and expand the Internet's wide-ranging benefits..."<sup>1</sup> The plan challenges the federal government to lay out cybersecurity R&D priorities for the government's own resources.

At the same time, national cybersecurity R&D efforts remain unfocused. A national cybersecurity R&D community has yet to be defined. National cybersecurity challenges beyond those discussed at a high level in the aforementioned strategic plan should be identified. Also needing definition is a concept of operations to coordinate nationally the efforts of organizations engaged in cybersecurity R&D activity. At the highest level of

<sup>1</sup> National Science and Technology Council, Federal Cybersecurity Research and Development Strategic Plan, accessed October 20, 2016, at [https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016\\_Federal\\_Cybersecurity\\_Research\\_and\\_Development\\_Strategic\\_Plan.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf).

abstraction, cybersecurity R&D goals have not been coupled tangibly to expressions of the national interest or to the nation's security, defense, and homeland security strategies. This year's CyberSci symposium reflected cross-sector acceptance of cyberthreats as pervasive and permanent, making the establishment of foundational support from the White House more important than ever.

## **Recommendation 1:** Connect Cybersecurity Research and Development to National Technology Development.

---

Cybersecurity technology and practice are not keeping pace with advances in the IT infrastructures we must safeguard. Advances in IT are relentless, providing our nation with a global competitive advantage. Creating faster, more agile cybersecurity technology synchronized with advances in IT is vital.

---

The advance of technology in general throughout our nation's infrastructure is one of the hallmarks of national progress. IT is being called upon increasingly to manage transportation, energy, communication, manufacturing, and other infrastructures. Increased use and complexity are likely also to amplify vulnerabilities. However, the advance of technologies used throughout the nation has not been accompanied, necessarily, by commensurate advances in the cybersecurity technologies employed to protect our infrastructures. A tighter coupling of the technology development overall with the nation's approach to cybersecurity R&D would result in national infrastructures that are more secure and resilient.

The connection between such R&D efforts is possible. The Department of Energy's national laboratories are participating collectively in a grid modernization consortium. According to the department, "By coupling headquarters collaboration with the strengths of the labs—in areas including their tremendous computational abilities, *knowledge of cybersecurity systems* [emphasis added], integration of renewable and energy efficient technologies, and command of sensing and control technologies—the Consortium will tackle the challenges associated with achieving a modern grid that will make a clean energy future possible."<sup>2</sup> The consortium is serving as the vehicle to synchronize the development of the "smart grid" with the cybersecurity technologies necessary to protect it. This approach exemplifies what should be done nationally for every infrastructure sector and for every aspect of the national economy on which we depend for our national, homeland, and economic security.<sup>3</sup>

---

<sup>2</sup> U.S. Department of Energy, energy.gov, "Launch of the Grid Modernization Laboratory Consortium," accessed October 20, 2016, from <http://energy.gov/articles/launch-grid-modernization-laboratory-consortium>.

<sup>3</sup> At CyberSci 2016, Congressman Ruben Gallego expressed his support for reaching across sectors as the new approach needed to address the cyberthreats that are growing rapidly in tandem with technological advances.

## **Recommendation 2:** Define a National Cybersecurity Research and Development Community.

The cybersecurity challenges facing the United States are vast and complex. Addressing them will require a whole-of-nation approach to the development and application of requisite cybersecurity capabilities. The next president should define carefully the national cybersecurity R&D community to ensure that all needed resources are applied and that efforts can be coordinated and effective.

Although an impressive range of enterprise is engaged in cybersecurity research, coordination of efforts awaits definition of the national cybersecurity R&D community. Defining a community that echoes the approach taken in post-World War II years to define R&D communities for nuclear energy and aerospace technology would improve collaboration, enable the synchronization of efforts to address specific cybersecurity R&D challenges, and illuminate progress against those challenges. Such a community would be well served by national-level leadership, possibly at the level of the White House and potentially informed by a national cybersecurity advisory committee to the president. The formal creation of a cybersecurity R&D community supported by such an advisory committee would elevate the importance of cybersecurity in general and could improve recruitment of some of the nation's best minds to the various cybersecurity R&D disciplines.<sup>4</sup>

## **Recommendation 3:** Define National Cybersecurity Research and Development Challenges.

Choosing cybersecurity R&D challenges that deserve priority attention by the national cybersecurity R&D community is more important than ever, given the challenges that exist to our critical infrastructure, intellectual property, and personal information. The effective allocation and coordination of vital R&D resources will depend on astute choices by the next president.

Creation of a national cybersecurity R&D community can be followed swiftly by definition of national cybersecurity R&D challenges for the community to address. Initial challenges can be derived from the *Federal Government Cybersecurity*

<sup>4</sup> In the CyberSci panel discussion *Beyond Government: Mobilizing Industry and Academia*, Dr. Alexander Kott of the Army Research Laboratory pointed out that our nation's higher education and private industry help define what makes us truly great but that we do not take sufficient advantage of these resources. Dr. David Honey of the Office of the Director of National Intelligence noted that as the work of industry, government, and academia move to the cloud, we are gaining new opportunities for collaboration.

*Research and Development Strategic Plan*<sup>5</sup> but should go beyond the plan to identify challenges associated with smart infrastructures—the IT-mediated management of infrastructures (e.g., energy and transportation)—and the needs of cybersecurity operators within DoD and the intelligence community. National-level cybersecurity challenges also should include securing our financial system, because crypto-currencies and global trading are increasingly important realities. Other challenges should be defined and prioritized, including those necessary to secure medical devices and medical information, protect vital intellectual property, and defend our critical infrastructure from the well-orchestrated computer network attacks of nation-state adversaries.<sup>6</sup>

## **Recommendation 4:** Enable Cybersecurity Research and Development Information Sharing.

Development of an effective national cybersecurity R&D community will pose the significant challenge of sharing important information quickly and securely. Although an existing Presidential Executive Order calls for stronger information sharing, efforts to build a national cybersecurity R&D information-sharing architecture should be formalized and accelerated.

The development of a national cybersecurity R&D community and the definition of national cybersecurity R&D goals should be enabled with strong information-sharing mechanisms.<sup>7</sup> The Presidential Executive Order of February 12, 2015, calls for improved private sector information sharing.<sup>8</sup> The order defines information-sharing and advisory organizations (ISAOs) at a high level. Such ISAOs can promote swift, efficient, and transparent information sharing for specific cybersecurity challenges (e.g., industrial control systems and smart infrastructures). ISAOs can complement existing, industry-specific information sharing and analysis centers and can be the vehicle to improve nationwide information sharing and collaboration for cybersecurity R&D. An effort is under way at the Intelligence and National Security Alliance's Cyber Research

<sup>5</sup> National Science and Technology Council, op. cit.

<sup>6</sup> A theme that echoed throughout CyberSci was the importance of understanding our adversaries' values and behavioral norms as a R&D priority, alongside more traditional technology-oriented priorities.

<sup>7</sup> Congressman Gallego noted that "cyber" is not owned by anyone, though it is used by everyone. Although discussions continue about where cyber "belongs," technology speeds along without the benefit of the best information available by those in our country who need it. Dr. Kott noted that we should not miss opportunities to share with and learn from our country's allies and partners.

<sup>8</sup> The White House, "FACT SHEET: Executive Order Promoting Private Sector Cybersecurity Information Sharing," February 12, 2015, accessed October 20, 2016, from <https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform>.



and Development Sub-Council to define such a cybersecurity R&D ISA0.<sup>9</sup> The subcouncil's work should enjoy the support of the White House in general, and of the Office of Science and Technology Policy in particular.

## **Recommendation 5:** Understand and Address Through Research and Development the Cybersecurity Technology Challenges Posed by Privacy.

---

Our Constitution's Fourth Amendment represents a cornerstone of our freedoms. R&D for the creation of new cybersecurity technologies should serve to enhance our protections rather than treat national cybersecurity and privacy as conflicting imperatives.

---

National concerns endure about the privacy of information used to safeguard the nation. The United States, with approximately 5% of the world's population, will continue to host and provide transit for a disproportionate amount of all internet and telephony traffic. Our intelligence community will need to conduct intelligence operations—including computer network exploitation—in an environment where foreign target communications transit the nation, targets of interest may communicate with U.S. persons, and national security and law enforcement concerns will overlap. Cybersecurity R&D activities should reflect cognition of these challenges, looking for ways to adhere to the protections afforded by the Fourth Amendment to the U.S. Constitution and ensuring that the search for vital intelligence does not become fixed surveillance of U.S. persons so protected. This challenge remains difficult. A January 2015 report from the National Academies notes that "no software-based technique can fully replace the bulk collection of signals intelligence, but methods can be developed to more effectively conduct targeted collection and to control the usage of collected data."<sup>10</sup> The development of these methods must respect the protections afforded by the Fourth Amendment and should be regarded as a cybersecurity R&D requirement of special importance.<sup>11</sup>

---

<sup>9</sup> Intelligence and National Security Alliance's Cyber Research and Development Sub-Council, accessed October 20, 2016, from <http://www.insaonline.org/i/c/cyber/c/index.aspx>.

<sup>10</sup> National Academies of Sciences, Engineering, and Medicine, National Research Council, "New Report Says No Technological Replacement Exists for Bulk Data Collection; Software Can Enhance Targeted Collection and Automate Control of Data Usage to Protect Privacy," accessed January 15, 2015 from <http://www8.nationalacademies.org/onpinews/newsitem.aspx?recordid=19414>.

<sup>11</sup> CyberSci's *Cybersecurity and Privacy* panel of experts analyzed this multifaceted issue, which is complicated by the amount of data becoming available and the value of those data for governmental and commercial decision making. The panel stressed our country's growing cybersecurity exposure resulting from the proliferation of unsecure software through IoT and discussed encryption, consumer education, and segmentation as possible components of an approach to improving cybersecurity while preserving privacy.

## Expert Panel Recaps

### Cybersecurity and Privacy

#### Panelists:

##### **Mark Weatherford**

*former Department of Homeland Security deputy undersecretary for cybersecurity*

##### **The Honorable Patricia Hoffman**

*assistant secretary of energy, Office of Electricity Delivery & Energy Reliability*

##### **Dr. Peter Eckersley**

*chief computer scientist, Electronic Frontier Foundation*

#### Moderator:

##### **Samuel Visner**

*ICF senior vice president/general manager for cybersecurity and resilience*

This panel highlighted the R&D challenges associated with enhancing and sustaining cybersecurity in support of national policy objectives while respecting privacy and civil liberty concerns. Panelists discussed civil liberties protection and the Fourth Amendment of the U.S. Constitution, encryption as it relates to civil liberties and national security, and the evolution of U.S. policy regarding the cybersecurity and privacy of the global information commons.



#### Highlights shared on Twitter during the event:

Common thread in recent #DDoS attacks were unsecured cameras. Old connected devices create a huge legacy problem—Weatherford.

Eighty percent of the data created have been created in the last three years. Managing those data is critical for #cybersecurity—Weatherford.

I think we'll technology our way out of the #cybersecurity analysis problem—Weatherford.

Human controls and redundancies necessary to improve #cybersecurity analysis—Hoffman.

Protection of comms pathways and endpoints are critical. Consumer ed. on use/updates key to #cybersecurity—Hoffman.

There's lack of understanding that #cybersecurity is public good. My insecure network affects your security—Eckersley.

Stronger passwords aren't always the solution for #cybersecurity, especially with shared networks—Eckersley.



## The Future of Cyber Operations and Technology

### Panelists:

**Lieutenant Colonel Paul Rozumski**, *U.S. Air Force*

**Christian Thomasson**, *U.S. Air Force*

**First Lieutenant Francis V Adkins**, *U.S. Air Force*

**First Lieutenant Val Red**, *U.S. Air Force*

### Moderator:

**Captain Daniel Stambovsky**, *U.S. Air Force*

Based on the recently released book, *Evolution of Cyber Technologies and Operations to 2035*, this panel explored the future of cybertechnologies and cyber operations and their influences on advances in social media, cybersecurity, cyberphysical systems, ethics, law, media, economics, infrastructure, military operations, and other elements of societal interaction. Discussion included the challenges of dealing with the speed of technological advances and of balancing risks against convenience when the risks are not necessarily known until after the fact. In the cyber-battlespace, there are few constraints. We must have situational understanding built block-by-block as well as cultural understanding of values.

Notable points made by panelists:

- Traditional warfare values are no longer limited to the field as enhanced cybercapabilities extend operational reach.
- To meet the increased tempo of engagement, especially use and manipulation through social media, the key is owning/operating platform up front.
- The action/reaction cycle in cyber is dynamic and ever changing, difficult to necessarily articulate or fund.
- We must accept that there will be breaches and perform cost/benefit analyses to allocate resources.
- We don't yet know how to define safety in the cyber engagement zone. Consider the morality of self-driving cars: Who are they designed to protect?
- Autonomous cyberresponse must consider attack response and collateral damage.
- Automated attack/defense challenges include autodetection of vulnerabilities, identification and resolution of threat, and self-healing/patching.
- Our future view will have to address the legal ramifications of an attack.
- These are disruptive times.
- Convergence may flip to divergence as traditional computers become operationally outnumbered by an unprecedented diversity of embedded systems.

## Beyond the Government: Mobilizing Industry and Academia

### Panelists:

#### Dr. David Honey

*director, science and technology, assistant deputy director of National Intelligence for Science and Technology*

#### Dr. Misty Blowers

*ICF vice president, cybersecurity research programs*

#### Dr. Alexander Kott

*network science division chief, U.S. Army Research Laboratory*

#### Dr. Douglas Maughan

*division director of the cybersecurity division in the Homeland Security Advanced Research Projects Agency within the Science and Technology Directorate of the Department of Homeland Security*

### Moderator:

#### John Paczkowski

*ICF senior vice president*

This panel examined ways to build a national cybersecurity R&D community, establish cybersecurity R&D priorities, and mobilize resources throughout the private sector and academia in support of national cybersecurity needs and policy requirements. Discussion included workforce recruitment and availability.



### Highlights shared on Twitter during the event:

Wargaming and public/private partnerships have been invaluable in assisting #cybersecurity R&D—Blowers

Making coding + #cybersecurity fun via things like Alice tutorials can help bring young people into #STEM careers—Blowers

Transaction transparency through blockchain is an attractive R&D option—Blowers.

Comm. and govt both moving toward cloud. Great opportunity in #cybersecurity collab. on that ground—Honey.

#IoT makers do not have #cybersecurity on their minds; professional community will have to pick up slack—Honey

The real struggle for growing #cybersecurity workforce is getting children to want to be scientists—Honey

Top issue for #cyber deterrence is attribution. More R&D needs to focus on that—Honey.

Are we making the most of our higher ed and military resources to create top-level #cybersecurity? Dr. Kott says possibly not.

Estonian #cyber pros (among best in world) can volunteer for defense efforts, similar to @RepRubenGallego's idea—Kott.

Lack of U.S. #cybersecurity PhDs mean that higher ed often cannot play a part in nat'l R&D due to clearance—Kott.

#cybersecurity is all about ppl. Too many comp. scientists, not enough psychologists working on fixing cyberspace—Maughan.

## Breakout Session Recaps

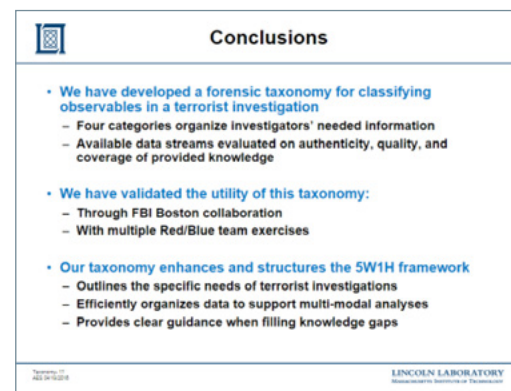
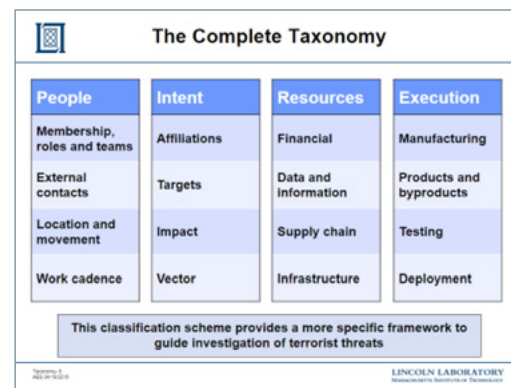
### A Data-Stream Classification System for the Investigation of Terrorist Threats

#### Era Vuksani

*assistant staff, Cyber Systems and Operations Group, Massachusetts Institute of Technology Lincoln Laboratory*

The role of cyberforensics in criminal investigations has greatly increased in recent years due to the wealth of data that are collected and available to investigators. Physical forensics has also experienced a data volume and fidelity revolution due to advances in methods for DNA and trace-evidence analysis. Key to extracting insight is the ability to correlate across multimodal data, which depends critically on identifying a touchpoint connecting the separate data streams. Separate data sources may be connected because they refer to the same individual, entity, or event. Ms. Vuksani presented a data source classification system tailored to facilitate the investigation of potential terrorist activity, the analysis of which was collaboratively conducted by a team of researchers at Lincoln Laboratory including Ms. Vuksani, Joshua Dettman, Jeffrey Gottschalk, Michael Kotson, Alexia Schulz, and Tamara Yu. This taxonomy is structured to illuminate the defining characteristics of a particular terrorist effort and designed to guide reporting to decision makers that is complete, concise, and evidence based. The classification system has been validated and empirically utilized in the forensic analysis of a simulated terrorist activity. Next-generation analysts can use this schema to label and correlate across existing data streams, assess which critical information may be missing from the data, and identify options for collecting additional data streams to fill information gaps.

Alexia Schulz, Joshua Dettman, Jeffrey Gottschalk, Michael Kotson, Era Vuksani, and Tamara Yu, "A Data-Stream Classification System for Investigating Terrorist Threats," Proc. SPIE 9851, Next-Generation Analyst IV, 98510L (May 12, 2016); doi:10.1117/12.2224104; <http://dx.doi.org/10.1117/12.2224104>.



## Recent Developments in Linkography-Based Cybersecurity

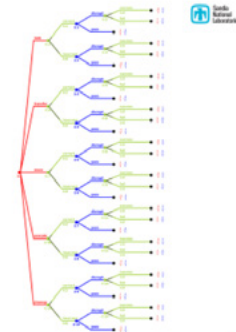
**Robert Mitchell**

*scientist, Sandia National Laboratories*

Since his presentation at last year's symposium, cyber attacks on our emerging national smart infrastructure have not decreased in frequency or complexity. Aggressors choose the time and place of these engagements; as protectors, we must identify, research, and develop defensive techniques that provide us an asymmetric advantage. A static, data-driven, preventative, automated defense is a losing strategy; an effective defense must be dynamic, behavioral, responsive, and capitalize on a human in the loop. Dr. Mitchell's presentation proposed human- and machine-performed linkography to detect, correlate, attribute, and predict attacker behavior and present a moving, deceptive target. Recently, his team generated a technology transfer strategy for linkography-based cybersecurity, proposed algorithms to extract and refine linkograph ontologies and subsessionize our input stream, and completed their previous related machine learning work. Linkography has been in the literature for decades, and their investigation indicates that it is an open, fertile topic for basic and applied cybersecurity research in the service of national security.

### Game Theory

- Key Components
  - Players
  - Information
  - Actions
  - Payoffs
- Variant
  - Noncooperative
  - Asymmetric
  - Imperfect Information
  - Zero Sum



20

### Conclusions

- Lessons Learned
  - Interdisciplinary Research Challenges
  - Current Cyber Attack Models are Macroscale
  - Humans In The Loop
- Future Work
  - Subsequence-Based Subsessionization
  - Alert Correlation
  - Additional Data Sources
  - Abstraction Refinement
  - Human Subject Research
  - Training Pivot

22



# Cyber and Intelligence Research and Development Funding Strategy

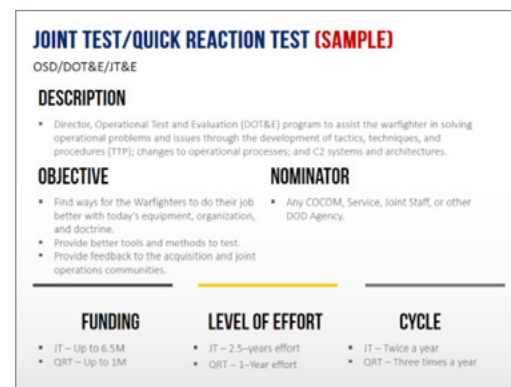
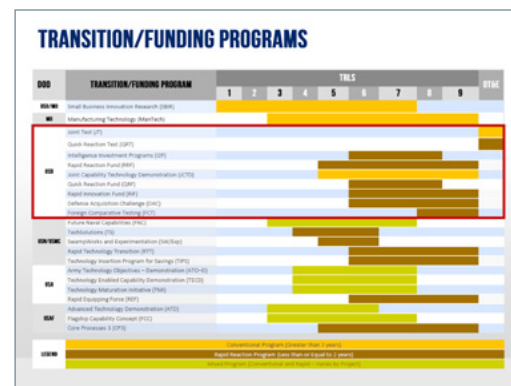
## Edmund Mitchell

chief business development officer, CSIOS Corporation

The purpose of the Department of Defense (DoD) Cyber Strategy 2015 is to guide the development of DoD's cyberforces and strengthen its cyberdefense and cyberdeterrence posture. The strategy focuses on building cybercapabilities and organizations for DoD's three cyber missions: defend DoD networks, systems, and information; defend the United States and its interests against cyber attacks of significant consequence; and provide integrated cybercapabilities to support military operations and contingency plans. The strategy is supported by five strategic goals and establishes specific objectives for DoD to achieve over the next five years and beyond. One of these goals is to build and maintain ready forces and capabilities to conduct cyberspace operations.

In support of this goal, Dr. Mitchell discussed how technology innovation sometimes moves too slowly from the lab to the field and outlined an R&D approach that seeks to leverage programs already established by DoD to fast track and mature R&D initiatives.

Within DoD, there are close to 20 different technology transition programs—managed by the Office of the Secretary of Defense and the military departments—that provide structured mechanisms and funding to facilitate the department's R&D needs and the transition of these products to our DoD warfighters. While these programs vary in mission, objectives, approach, funding, technology maturity, size, and expectations, they are complementing of each other and could be used to help accelerate the technology readiness levels and provide DoD with a significant advantage in developing leap-ahead technologies to defend U.S. interests in cyberspace. Dr. Mitchell illustrated his points through a sample business case that outlined how these programs have been used to assist and accelerate the DoD cyber and intelligence R&D mission.



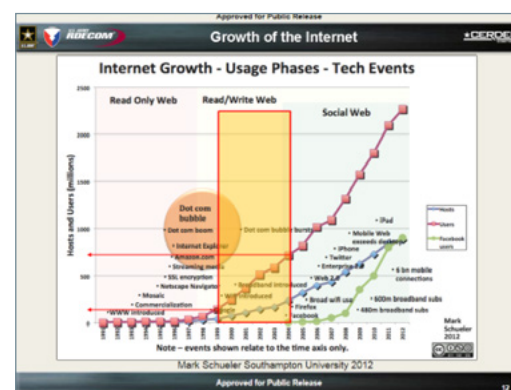
## Collateral Effect Potential Metric for Computer Exploits

**Giorgio Bertoli**

*senior scientific technical manager for Offensive Cyber Intelligence & Information Warfare Directorate, Aberdeen Proving Ground, Maryland*

As reliance on networked computing devices continues to expand, software vulnerabilities and corresponding malicious software will remain a widespread concern. While methods exist to categorize software vulnerabilities by severity, none exists to classify the exploits themselves. Mr. Bertoli proposed a framework that leverages concepts from epidemiology to define exploit attributes, which are then quantified and combined to yield an overall collateral damage potential metric. Collateral damage results primarily from the uncontrolled execution of a cyber effect. An exploit that is launched against a specific target system may also unintentionally or indiscriminately impact other systems. This behavior can be quantified. Much like a biological agent is categorized based on its potential to affect a large portion of the global population, the proposed framework focuses on the categorization of malicious software based on its propensity to indiscriminately affect a broad range of cyberspace systems.

The proposed Exploit Collateral Effect Potential (ECEP) metric is based on six attributes—damage, controllability, detectability, remediation, exclusivity, and propagation—which yield an overall metric that provides a relative measure of how "controlled" an exploit is in its design and concept of employment. An ECEP score can be used to assist in the prioritization of exploit signature creation and vulnerability patch deployments. In addition, this framework can support military commanders in the planning and execution of offensive cyber operations by quantifying the collateral damage potential associated with the employment of specific cybercapabilities.





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

**Jennifer Cowley**

*human factors psychologist, CERT/Software Engineering Institute/  
Carnegie Mellon University*

Dr. Cowley presented aspects of her years of research at the 2016 CyberSci Symposium as an individual. Her statements and assertions do not reflect the views and ideas of the Software Engineering Institute, CERT or Carnegie Mellon University.

Enterprise-level social networking software, intended to ameliorate employee collaboration and productivity problems, can actually engender additional, more serious workforce problems like insider threats. Dr. Cowley crafts this premise from an array of scientific evidence from multiple disciplines in the hopes of beginning a cross-discipline dialogue on the unintended effects of software engineering.

Software engineering (coding, architecture, etc.) often occurs with minimal consideration about how software products negatively impact users socially and psychologically. With recent media coverage discussing the unintended consequences (distraction, addiction, poor academic performance, work disengagement, loneliness, etc.) of different aspects of computing (social networking, information surfing, gaming, etc.), she began questioning how computing impacts employees in the workplace. Negative consequences of computing first arose in clinical psychology settings as early as the 1970s, when adolescents were becoming addicted to video gaming. Since then, this class of gaming addictions broadened into digital and internet addictions and eventually led to a formal psychopathological disorder listed in the DSM-V (Diagnosis and Statistical Manual of Mental Disorders, 5th Edition), a manual used by practicing clinical psychologists for diagnosing psychopathologies. However, it is hard to disentangle what aspect of computing—the software, the mobile devices, the internet, etc.—is giving rise to addictions. We know that software design has borrowed highly attractive and engaging features researched in the game design community to make their nongaming software, like social media, hard to not use. From a marketing perspective, the more addictive the software is, the more people use it and, thus, sales balloon.

How does social media usage impact work environments? Some people argue that modern work environments in the digital age have overemphasized electronic communications at the expense of doing technical work. Professionals who thrive on executing deeply technical work are particularly vulnerable to negative emotive states when encumbered from doing the work they are intrinsically motivated to execute. These negative moods are compounded with negative management practices being reported in modern computing work environments. To survive those environments, employees often unconsciously augment the negative mood in benign and familiar mechanisms like internet surfing, gaming, shopping, social media, etc. Recent research suggests that mood can be altered with social media viewing when

people are using it to avoid or escape negative realities or heavy workloads. However, other research indicates that the more frequently social media is used, the more isolated and lonely the person feels, which potentially begets more social media use. Enterprise-level social networking tools originally intended to improve work collaboration, coordination, and productivity may be doing the opposite. Enterprise-level social media is not used like private social media. Several recent publications report reduced digital social engagement, increased social isolation, and reduced job satisfaction, all of which can negatively impact productivity.

How do social media-engendered distractions exacerbate negative mood in the work environment? First, organizations have allowed digital distractions, like private and enterprise-level social media apps, into the work environment, which interrupt employees with some periodicity. This learned periodicity creates patterns of self-interruption, usually for mood augmentation. Furthermore, a corpus of research results indicates that in many circumstances, distractions lead to cognitive failures that directly and indirectly impact job performance. Reports indicate that when work is interrupted, it takes an adult between a few milliseconds to several minutes to re-engage with the work being executed prior to the interruption. If distractions have been reported on average to occur every 3 minutes, and it takes a person 1 minute to re-engage with the prior work tasking, that person has lost 160 minutes in an 8-hour period (~2.6 hours) that the employee is burdened with. Work productivity may seem impossible. Furthermore, the organization furnishes social media types of tools (e.g., collaboration wikis, SharePoint repositories, ticketing systems, etc.) that encourage distraction that impedes the employee's ability to focus on the deep technical work required for positive job-performance evaluation.

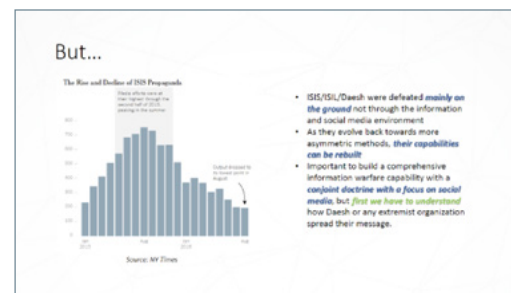
The reader may be curious about the tie between social media and insider threat. Organizations surveil employees' digital activities for work performance evaluation and for insider threat potential. One large corpus of research from the 1960s to the early 2000s robustly indicated that employees who were not satisfied with their jobs, who lacked management support, who felt the organization was unjust, and so on, were more likely to commit organization crime (theft, sabotage, etc.). Furthermore, recent findings suggest that surveillance causes people to distrust management, and employees are more inclined to withdraw from electronic communications unnaturally (called the "chilling effect"). While productivity seems to increase when surveilled, employees censor communications and commit behaviors that align with perceived cultural norms rather than what is natural. Organizational norms are thus false and only document the level of group conformity. Behavioral deviations for erroneous norms may also trigger false positive insider threat indices. And yet, for job performance purposes, management sometimes reviews enterprise-level social media activities for "objective job performance" assessment and yet employees are refraining from posting information online. Dr. Cowley would like to encourage the R&D community to discuss the merit of these ideas as we continue to produce new enterprise-level software.

## Modeling, Simulation, and Analysis of a Social Media Propaganda Network: The Case of ISIS/ISIL/Daesh

**Joseph Shaheen**

*researcher, NATO STRATCOM COE and George Mason University*

Mr. Shaheen presented analysis—conducted for NATO STRATCOM and funded by the U.S. Department of State—aimed at assisting in understanding methods of propaganda dissemination used by ISIS/ISIL/Daesh on social media networks and conducted at the strategic, operational, and transactional levels. Methods for combating social media propaganda were proposed using network theory. Additionally, by using advanced agent-based modeling techniques, Mr. Shaheen showed how advanced behavioral analysis can be fruitful in the identification of network microstructures and thus in the development of tactics to win the next information war. His conclusions were highly generalizable with applications on any network, not only on social media platforms.



### Final Insights

1. DAESH behavior is best understood as an **evolutionary, self-repairing, self-reinforcing** network – it's difficult to forecast or predict through deductive analysis alone.
2. To truly understand Daesh propaganda, and any terror group on social media, there must be greater focus on the **method of dissemination and prediction** as well as content.
3. As a consequence of this modeling effort, which includes analysis and simulation, a potential framework for social media warfare is presented.

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

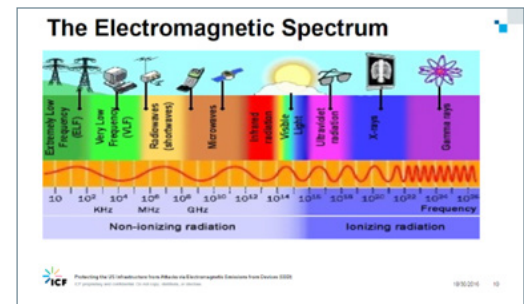
**Timothy J. Cash**

*senior consultant, The Lever Group*

**John W. Link**

*senior consultant, VOLVOX Inc.*

An emerging class of cyber attacks penetrates systems by way of the tiny electromagnetic fields given off by technology, referred to as electromagnetic emissions from devices (EED). Much of today's technology creates an unintended electromagnetic footprint that is unseen, yet readable, electromagnetic spillage at multiple frequencies. EED can be turned against us as a penetration vector or as a method of data extraction. This, in turn, creates multiple threat vectors for different types of intrusion technologies. EED, otherwise known as attacks across an "air gap," is currently the least used method of intrusion but represents an area of growing risk that must be managed to protect our cyber infrastructure, especially as a unique threat to the U.S. electrical grid. While messages and data on the network may be encrypted, the same data emanated from within the IT infrastructure produced by and between internal components and subsystems produces EED that is not encrypted. EED can be used to bypass passwords or biometrics, gain access to passwords, bypass firewalls and penetrate networks to extract data, and penetrate sensors on IoT networks. According to Link and Cash, the good news is that the EED threat vector is relatively easy to defeat through application of both technical and nontechnical means. The even better news is that we have an opportunity to get ahead of the hackers and nation-state actors, but only if we act now to include anti-EED intrusion protection technologies as part of our national cybersecurity strategy.



### Summary

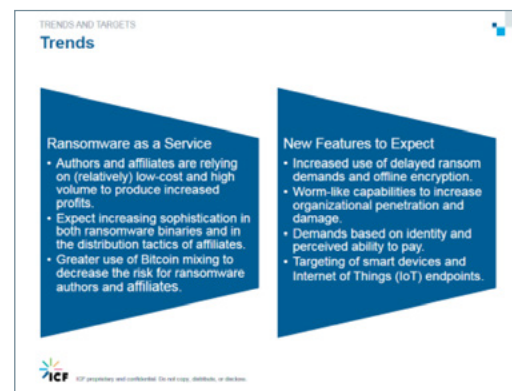
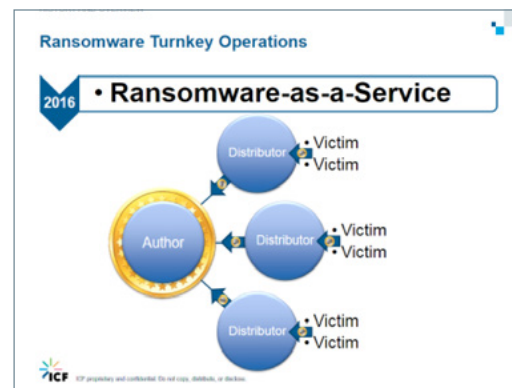
- EED has long been known about as threat but generally in the classified realm (TEMPEST)
- The EED vector represents a growing threat to Cybersecurity and to national infrastructure via:
  - Data Extraction
  - Malware Insertion
  - Controller or Cybersecurity Disruption
- As Cybersecurity controls and defenses improve, EED will become attractive to Non-State actors
- EED attacks can be countered by sensors, distance, shielding, and signal cloaking and disruption
- The EED area needs aggressive research and policy/standards development now

## Ransomware Over the Past Five Years: Overview and Best Practices

**Timothy Obenshain**

*project manager, ICF*

In the last five years, there has been a large rise in the number of computer security incidents characterized as ransomware. Mr. Obenshain's presentation examined the history of ransomware and provided a basic explanation for how it works, how it spreads, and how it is monetized. In doing so, he examined a selection of ransomware variants, discussing the characteristics of various pieces of malware and the differences in approaches. The discussion included a selection of best practices that can defend against ransomware attacks, addressing both prevention and remediation after infection. The security community has created a wide variety of solutions to help prevent the installation of ransomware on a properly protected system, to limit access if installed, and to notify administrators as quickly as possible if an infection is successful. In the case that a ransomware infection is successful, a strong and consistently applied backup solution is critical to avoid loss of data. Mr. Obenshain explored best practices for backup and recovery strategies, including new and emerging issues related to cloud backup solutions and how they are affected by ransomware. Certain older varieties of ransomware have known solutions that can allow for the decryption of files held for ransom.

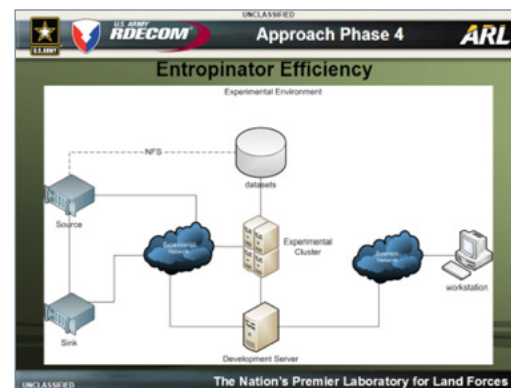


## The Use of Entropy in Lossy Network Traffic Compression for Network Intrusion Detection Applications

**Sidney "Chuck" Smith**

*computer scientist, U.S. Army Research Laboratory*

Most distributed network intrusion detection applications only send alerts to the central analysis servers. Often, alerts alone do not provide the forensic capability that analysts require to determine whether this is an actual intrusion or a failed attempt. The Interrogator Network Intrusion Detection Framework (Interrogator) solves this problem by transmitting some portion of the network traffic back to the central analysis servers for further analysis and forensic examination. This introduces another problem in that transmitting all data captured by the sensor would place an unacceptable demand on the bandwidth available to the site to conduct daily business. Lossless compression techniques alone are not able to compress the data sufficiently to relieve this demand. Interrogator currently employs a lossy compression technique that uses data mining to transmit the traffic most likely to be malicious. Much of today's network traffic is either encrypted or compressed. There is little value in transmitting either encrypted or compressed traffic for further analysis or forensic examination. Entropy has been used in other applications to identify encrypted and compressed data. Mr. Smith established a baseline through research for clear text using randomly selected books from Project Gutenberg, executables using binaries from Linux and Windows operating systems, compressed files by reducing the files used previously, and encrypted files using the same. His team studied network traffic to discover the distribution of entropy among popular protocols. They constructed a tool that would read network traffic in Tcpdump format and write out the packets with payload entropies less than the threshold provided on the command line. They examined these compressed files with Snort to observe the loss in alerts. Mr. Smith and his colleagues constructed a tool that would read network traffic from a network interface, compute the entropy, and save only those packets with payload entropies less than the threshold. They repeated the experiment, increasing the speed of the replay to assess the efficiency of the process. Applying these techniques to the data captured by gator020 in the 2009 Cyber Defense Exercise, they achieved a 72% compression ratio employing entropy alone and a 96% compression ratio when coupling this technique with GNU zip lossless compression. Using the Snort Community ruleset from August 2013 to examine the data before and after compression, the team found that they lost less than 1% of the Snort alerts in our compressed data.



### Conclusion

- Wide gap in the entropy values of clear text files and binary executable files vs. compressed and encrypted files.
- Many popular network protocols have a very wide range of entropy values.
- Entropic compression alone was able to reduce the size of the gator-usama020 data set from CDX 2009 to 27% of its original size losing only 0.6% of the alerts detected by Snort.
- Adding lossless compression using GNU Zip further reduced the data set to 4% of its original size with little impact to efficiency.
- Entropinator performs significantly better than Snort at higher speeds.
- Use of Entropy to compress network traffic that needs to be transmitted from the sensor to the CAS in network detection applications is feasible.

## Value-of-information Sensitive Cybersensor

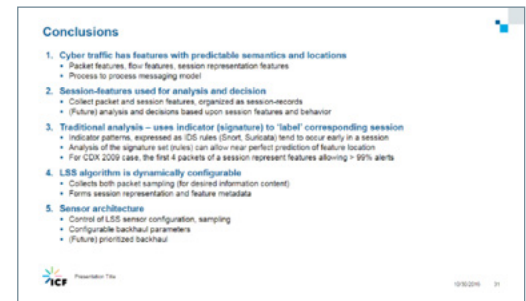
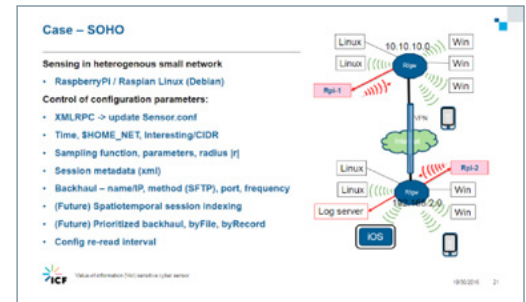
**Steve Hutchinson**

*technical specialist, ICF*

**Jason Ellis**

*analyst, ICF*

Hutchinson and Ellis described a novel (cyber) network traffic sensor method appropriate for use in applications with constrained computational and communication resources. Their collection method was sensitive to the information content of traffic sessions and thus able to preserve detailed evidence of data that would most strongly influence detection and decision. The sensor collection method was also controllable by external and downstream processes. During collection, the sensor accepted new specifications for information-content sensing, specifications for particular behaviors to represent, and the quantity of detailed traffic evidence to retain and represent. Collection specifications may also be controlled by a downstream detection and decision processes—allowing an enhanced collection interval, or particular protocols, or particular address ranges to be represented more completely. They shared results from deployment of the above sensing method on a Raspberry Pi version 2, deployed in a small heterogeneous (wired and Wi-Fi) network. Performance testing of the compressed representation was performed using Snort rules as the measure of information content. In numerous tests, this information content-sensitive representation preserved > 99.3% of evidence features for generation of corresponding Snort alerts.





## Cybersecurity Risks in the Industrial Internet of Things

**Dan Sullivan**

*Supervisory Control and Data Acquisition researcher, Raytheon*

**Ed Colbert**

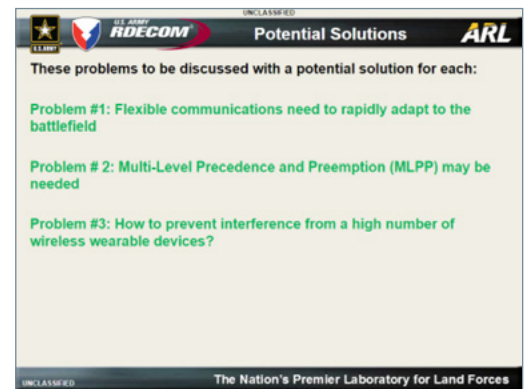
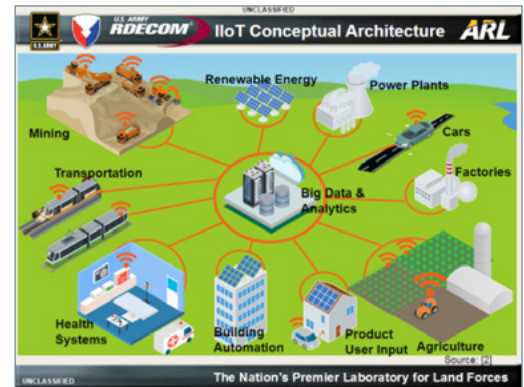
*researcher, U.S. Army Research Laboratory*

Represented by Mr. Dan Sullivan, this team effort defined the Industrial Internet of Things (IIoT) as the application of IoT implemented for industrial control systems (ICSs). The IIoT is based on the concept that multiple sensors reporting data about an automation process can be leveraged by analytics to optimize the process. The optimization is expected to reduce costs, improve quality, improve compliance with organizational policies, and predict when corrective action is needed to maintain automation goals. Many of these sensors are inexpensive wireless devices and the reported data may be stored in big data appliances where predictive analytics software can analyze the data and find the optimizations.

Mr. Sullivan described IIoT standards organizations; best practices; and example-use cases, such as wireless sensors in light bulbs to monitor light in a room and save energy, sensors in appliances to report energy usage so a consumer can turn off high-energy appliances, and sensors in hospitals to reduce patient infections.

He reviewed the security risk, such as recent malware attacks on ICSs and discussed industrial accidents, caused by faulty sensors or interconnections between the IT and ICS networks. He explained how these incidents may also occur with IIoT systems since threat actors may use similar techniques to compromise an IIoT to change logic, cause a denial of service attack to embedded wireless sensors, or manipulate sensor data. He made the case that authentication, but not necessarily encryption, is required in the embedded wireless sensors, and customers must demand that cybersecurity becomes part of the supply chain. In conclusion, he discussed why critical variables are important to protect and why defense in depth security must be designed into the architecture.

In addition to IIoT, Mr. Sullivan presented many of the challenges his team expects DoD will encounter to securely deploy and manage IoBT in the next 20 to 30 years. Dr. Alexander Kott spoke about IoBT in the morning keynote address. As IIoT depends on leveraging IoT technologies, IoBT will also utilize IoT in weapon systems and soldier-wearable devices. Any cybersecurity vulnerabilities in IoBT devices are much more significant because these devices could be exploited by enemies on the battlefield. Battles could be decided by an enemy hacking IoBT devices used by weapons. As part of their recommendations to the new presidential administration, Mr. Sullivan's team urges R&D in IoBT, because R&D is needed to ensure that our armed forces will maximize the expected benefits of a secure and interoperable IoBT.





## Securing Cyberphysical Systems

### Dhananjay Phatak

*associate professor, University of Maryland, Baltimore County*

Excess capacity in the form of Turing Equivalence is one of the main hurdles to the realization of provably secure computing systems. Dr. Phatak explained that despite this fact, almost all computing systems today (including the embedded ones) are realized using off-the-shelf hardware and software components in a manner that makes them Turing equivalent. As a result, determining whether a given program has malicious intent is extremely hard to decide completely and purely within the cyber domain. Fortunately, in cyberphysical systems; the cyber subsystem is tightly coupled to a physical subsystem, which it controls. He proposed methods to exploit this tight coupling to identify and mitigate malicious behavior by monitoring the signals at the interface/boundary between the cyber and the physical parts/domains of the system before the deviant inputs can propagate into the physical subsystem. The digital inputs sent to all the D/A converters turn out to be the critical boundary of interest. He also pointed out connections to fuzzy logic, and in particular, the fact that a fuzzy controller or a fuzzy control input verifier can be more easily and naturally specified and synthesized as a finite automaton. He concluded that the security properties of finite automata are decidable as well as provable via automated methods.

#### A good interim solution ??

- Devise tools (ex: compilers) that can express an application program as an execution sequences of finite automata (whenever feasible)
- Develop wrappers (s/w or h/w or both) that hide the full Turing Equivalent capacity of the embedded computing system. The wrapper should make the underlying computing system (processor, memory etc...) look like a finite automaton designed for the specific application scenario at hand

21

#### Connection to Fuzzy logic

- Fuzzy logic : avoids unnecessary precision by deliberately simplifying sharp/precise inputs into less sharp classes with fuzzy boundaries
- The fuzzy inference rules prescribe action based on what fuzzy state the system is in and what class the fuzzy inputs are in
- => fuzzy inference rules can be realized by a Finite Automaton whose state transition table comprises of the fuzzy-rules...
  - Also possible to implement with analog components that cannot be "hacked" in the same manner as s/w driven digital processors...

43

## Keynote Presentation Summaries

### The Internet of Battle Things

#### Dr. Alexander Kott

*director, Network Science Division chief, U.S. Army Research Laboratory*

Based in part on his work, "The Internet of Battle Things," upcoming in IEEE Computer, December 2016, with coauthors Ananthram Swami and Bruce J. West, Dr. Kott introduced the concept of the military Internet of Things (IoT), coined the "Internet of Battle Things" (IoBT). Observing that the same forces propelling the IoT—growth of machine intelligence and networked communications—apply in the military context, Dr. Kott shared his vision for the potential of an IoBT to improve the capabilities, servicing, and ultimately the survival of our armed forces:

- IoBT covers enterprise applications that resemble IoT (smart installations, energy management, logistics, industrial controls, etc.) and tactical applications at the front of engagement, including munitions, weapons, field sensors, robots, vehicles, and wearables. Among uses in the field are sense, communicate, collaborate, sustain, fix, defend, and attack.
- "Battle things" must be fluid, adaptable, and dynamic to override limited connectivity, technical opposition, and more. In a rapidly changing environment—with enemies always working to limit or disable functionality—this technology must be able to manage without reliance on humans for operations or support.
- Industrial control systems could be considered the "soft underbelly of the nation," due to their growing interconnectedness and resulting vulnerability. It is prohibitively expensive to retrofit to something less vulnerable, so protection requires continuous monitoring, predictive modeling, and compartmentalization. And despite all these efforts, human trust and data integrity will be the most important and complex factor in IoT defense applications. Once trust is lost, the system will not be used.
- Detectable, conventional radio frequency communications cannot survive. Diversity and alternative channels will be key, as will a network of collaborative parts rather than one central node.
- The enormity of the data with which we are confronted and the complexity of the networks we have built to process that data are almost more than our brains can comprehend. The sheer scale challenges management and adaptation. One million things per square km is well within the realm of possibility. In ways, the complexity may help with protection.



## Keynote Address: Congressman Ruben Gallego

### **Congressman Ruben Gallego**

*Arizona (D) House of Representatives, member of the House Armed Services Committee*

Congressman Gallego greeted the assembled cybersecurity R&D experts by joking that he represented a "technological backwater...Congress." Shifting tone, he noted that cybersecurity is high on the national agenda, but "our policy answers are not up to the challenge." We are "using old paradigms" and "preparing for old threats." The congressman sees the need for a new approach, one that includes greater cooperation with the private sector. Other key points from his talk included:

- Consideration of a structure or system of hackers—a cyberforce we can tap into for good. This could not have been anticipated in the 18th century concept of military strategy.
- Voting systems should be part of our critical infrastructure. Wikileaks hacks are brazen attempts by Russia to influence our election. If it had been a physical attack rather than cyber, the response would have been "worse than Watergate."
- Comparing to the post-World War II era of nuclear weapons development, we must speak about behavior norms and caps to pen in state actors. However, super weapons capabilities are not a deterrent in this case, because cyber warfare does not have a "mutually assured destruction" model curbing the arms race.
- It is time for rules of the road, and CyberSci participants are part of that effort. Each should consider what more can be done to encourage participation in the field as a moral and national security imperative.
- We cannot wait for Congress to establish policies—the threat is moving much too fast. It is better to bolster agencies in the executive branch and link up with private sector companies. The fundamental problem is that cyber does not "belong" anywhere.
- Regarding prosecution of cyber criminals, apply our current approach to terrorism—on foreign land, Central Intelligence Agency (CIA) and military involvement, on U.S. soil, domestic law enforcement, and due process. A change of weapons should not require a change of process designed to protect civil liberties.



## Russia, Putin, Hacks, Elections.... Where to Go from Here?

### General Michael Hayden

*retired four-star general, former director of the Central Intelligence Agency and National Security Agency*

General Hayden began sharing his uniquely informed perspective by framing the current geopolitical context and his firm belief that Russia is revanchist, not resurgent, and surviving on the residuals—the "flotsam and jetsam"—of the Soviet Union. Unable to match the United States physically, President Putin has moved to the "nimble, low-cost front" of the information space, where stories can be muddled and controlling spin is tradecraft.

Turning to the Democratic National Committee (DNC) hacks and Wikileaks, General Hayden's points included:

- Methods used to hack the DNC were similar to those used in Distributed Denial of Service (DDoS) attacks on Estonia in 2007 and Georgia in 2008. Putin turns to gangs in exchange for immunity.
- The DNC hack was conducted via spear phishing. One in four emails was clicked on.
- Putin is not trying to pick a winner. This is a case of a foreign state using cyber to degrade or discredit the election process. The goal is erosion of confidence in our institutions.
- Theft of emails is actually an "honorable international espionage," but weaponizing them through an influence campaign is dishonorable.
- Some ideas on how to respond:
  - Geopolitical tactics—arm the Ukraine (but risk escalation), pressure through international relations, frack Europe (wean off Russian gas).
  - Cyber tactics—target criminal platforms, name and blame perpetrators, push anonymizing software to remove attribution (attention).

In response to an audience question about considering the cyberfront a new cold war, General Hayden acknowledged that lessons about deterrence theory could apply, but he reiterated his belief about Russia's diminished capabilities relative to the Soviet Union: "It's not a cold war, because 'a cold war requires a peer or a near peer.'"





## The Cybersecurity Storm: Front Forces Shaping the Cybersecurity Landscape

**Samuel S. Visner**

*ICF senior vice president/general manager for cybersecurity and resilience*

Mr. Visner discussed the powerful underlying forces shaping a rapidly changing cybersecurity landscape and proposed a possible framework to generate hypotheses regarding global cybersecurity events. Echoing themes expressed throughout the day, he framed cybersecurity as intrinsic to information and enterprise, with increasing interconnectedness and technology enablement.

The strategic factors shaping the landscape include:


1. Importance of information and information intensity.
2. Information technology (IT) structures and migration to the cloud, including critical infrastructure in the near term.
3. Operational threats that are advanced, persistent, and patient.
4. Cyber as statecraft "up there with diplomacy and espionage," although Russian weaponization of American politics is not new (referencing the Zimmerman telegram of 1917).
5. Intertwined security/privacy concerns.
6. Computer network exploitation and addition of computer network "influence" to affect behavioral outcomes, as we saw with the Sony and Dyn hacks.

Mr. Visner concluded by thanking event speakers and attendees for making CyberSci 2016 an extraordinary conversation about cybersecurity issues and solutions.



**The technology and structure of the IT infrastructures we seek to safeguard**

- IT/OT allows us to manage and mediate individual and converged infrastructure (electricity, roads, traffic enforcement, etc.)
- The cloud has arrived and it's consuming just about everything
- We're moving to multi-cloud (cloud orchestration) environments
- Will it consume OT? More to the point? Why would it not?



ICF The Cybersecurity Storm Force  
© Copyright 2016 ICF. All rights reserved. All devices.

10/10/2016 6

**As we move forward ...**

- We'll need to analyze our proposed actions against these factors
- The environment is changing rapidly – perhaps this model will help us change accordingly




ICF Presentation Title  
© Copyright 2016 ICF. All rights reserved. All devices.

10/10/2016 11

## Conclusion

The CyberSci 2016 Symposium made clear the need to mobilize academia and the private sector more strongly in support of cybersecurity R&D. It also brought into sharp focus the need to build cybersecurity technologies and capabilities that do not offend our national values or impinge on our legal protections. The creation of a national cybersecurity R&D community and the definition of appropriate national cybersecurity R&D challenges—coupled with an understanding of the role cybersecurity R&D should play in support of national technology development—would signify important steps toward addressing a national imperative. The next administration has the opportunity to play a pivotal role in the way our country addresses the serious challenges posed by cybersecurity. We hope these recommendations will well serve the 45th President of the United States in doing so.

## Speaker List

### First Lieutenant Francis V Adkins

*U.S. Air Force*

#### The Future of Cyber Operations and Technologies

First Lieutenant Frank Adkins is a U.S. Air Force officer, security enthusiast, and ardent futurologist. He also enjoys pen testing (certified OSCP), bug hunting, red teaming, and playing CTF. As a researcher, Lt. Adkins has worked with the U.S. Air Force Academy Center for Cyberspace Research, DARPA, the Intel Corporation Antimalware Laboratory, and MIT Lincoln Laboratory. He facilitates operational mission planning, C2, execution; and delivers USCYBERCOM's highest priority effects. Additionally, Lt. Adkins develops and delivers OCO training and prepares members to excel in DoD's toughest cybercourses. He usually specializes in formal program analysis and automated exploit generation but is also known to dabble in malware detection.

### Giorgio Bertoli

*senior scientific technical manager for Offensive Cyber Intelligence & Information Warfare Directorate, Aberdeen Proving Ground, Maryland*

#### Collateral Effect Potential Metric for Computer Exploits

With 22 years of federal service, Giorgio 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***ICF vice president, cybersecurity research programs***Beyond the Government: Mobilizing Industry and Academia**

Prior to serving as vice president for cybersecurity research at ICF, Dr. Misty Blowers led the cyber offensive research team at the U.S. Air Force Research Laboratory, Information Directorate, where she managed more than \$95 million in government contracts. Dr. Blowers obtained her Ph.D. from the SUNY College of Environmental Science and Forestry in applied science and engineering and an M.S. 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 cyberphysical systems and IoT. 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 more than 50 publications and has provided plenary talks on behavior analysis of manufacturing processes and the future of cyberphysical systems.

**Timothy J. Cash***senior consultant, The Lever Group***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.



**Ed Colbert***researcher, U.S. Army Research Laboratory***Cybersecurity Risks in the Industrial Internet of Things**

Dr. Edward Colbert is a researcher at the U.S. Army Research Laboratory in Adelphi, Maryland, where he conducts novel security research on methods for defending Army Supervisory Control and Data Acquisition and ICS systems. Before working for the U.S. Army Research Lab, he was research fellow at ICF and has performed telecommunications research for the DoD, 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 Ph.D. and an M.S. in astronomy from the University of Maryland and an M.S. in physics and B.S. in engineering physics from the University of Illinois.

**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 Ph.D. 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**

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 Electronic Frontier Foundation has included privacy and security projects such as Letter Encrypt and Certbot,

Panoptick, 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 Ph.D. 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*

### Value-of-information 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.

## Congressman Ruben Gallego

*Arizona (D) House of Representatives, member of the House Armed Services Committee*

### Keynote

Congressman Ruben Gallego was elected to the Arizona House of Representatives in 2010 and served until 2014. He represented District 27, which covers much of Phoenix. He rose quickly in the state legislature, serving as assistant minority leader. Congressman Gallego became known for his tough stand against extreme legislation pushed by Republicans in the state legislature. He led the opposition to the discriminatory SB 1062, which Governor Jan Brewer ultimately vetoed. As a state legislator, Congressman Gallego also led the push for Medicaid expansion and to secure in-state tuition for veterans. In his first year in Congress, Congressman Gallego introduced the VETS Act, which would reduce the burden of student loan debt on veterans and has supported legislation to increase the hiring of veterans and provide additional benefits to wounded or deceased veterans and their families.

Congressman Gallego helped lead the effort to strengthen and restore the Voting Rights Act to ensure that all Americans have access to the ballot box. He also authored legislation to encourage gun dealers to be stronger community partners

in the struggle against gun violence and to crack down on irresponsible gun dealers. Congressman Gallego serves as a senior whip for the Democratic Caucus, the whip of the Congressional Hispanic Caucus, vice chair of the Congressional Progressive Caucus, and vice chair of the Equality Caucus. He currently serves on the House Armed Services Committee and the Natural Resources Committee.

## General Michael Hayden

*former director, Central Intelligence Agency and National Security Agency; U.S. Air Force, Retired*

### **Russia, Putin, Hacks, Elections... Where to Go from Here?**

General Michael Hayden is a retired four-star general who served as director of the CIA and the National Security Agency (NSA) 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 the 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 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, 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 George Mason University School of Policy, Government, and International Affairs. He is on the board of directors of Motorola Solutions and serves on a variety of other boards and consultancies.

## The Honorable Patricia Hoffman

*assistant secretary of energy, Office of Electricity Delivery & Energy Reliability*

### Cybersecurity and Privacy

Patricia Hoffman was named assistant secretary for the Office of Electricity Delivery & Energy Reliability at the United States Department of Energy in June 2010 after serving as its principal deputy assistant secretary 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. She holds a B.S. and an M.S. in ceramic science and engineering from Pennsylvania State University.

## Dr. David Honey

*director, science and technology, assistant deputy director of National Intelligence for Science and Technology*

### Beyond the Government: Mobilizing Industry and Academia

As the director of science and technology and assistant deputy director of National Intelligence for Science and Technology, Dr. David 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 science and technology programs—and for developing technologies needed for continued technological superiority of U.S. forces. Dr. Honey was director of the Defense Advanced Research Projects Agency Strategic Technology Office, director of the Advanced Technology Office, and deputy director and program manager of the Microsystems Technology Office.

## Steve Hutchinson

*technical specialist, ICF*

### Value-of-information Sensitive Cyber Sensor

Steve Hutchinson is a researcher-analyst with ICF, contracted to the U.S. Army Research Laboratory. 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 M.S. in mathematics education from Drexel University, graduate studies in computer science at Rochester Institute of Technology, and a B.S. in electrical engineering from the State University of New York at Buffalo.

## Sudhakar Kesavan

*ICF chairman and chief executive officer*

### Opening Remarks

Sudhakar Kesavan serves as chairman and chief executive officer of ICF, a global management, technology, and policy consulting firm headquartered in Fairfax, Virginia. The firm has offices throughout the Americas, Europe, and Asia, and has more than 5,000 employees serving clients in the public and private sectors. Mr. Kesavan is a member of the board of directors of ABM Industries, Inc., one of the largest facilities management companies in the United States. He serves on the board of trustees of the Inova Health System in northern Virginia and as an emeritus board member of the Northern Virginia Technology Council and the Rainforest Alliance.

Mr. Kesavan received his M.S. degree from the Technology and Policy Program at the Massachusetts Institute of Technology (1984), his post-graduate diploma in management (equivalent to an M.B.A.) from the Indian Institute of Management, Ahmedabad (1978), and his B. Tech. degree (chemical engineering with distinction) from the Indian Institute of Technology, Kanpur (1976), which awarded Mr. Kesavan the Distinguished Alumnus Award in 2010.

**Dr. Alexander Kott**

*director, Network Science Division chief, U.S. Army Research Laboratory*

**The Internet of Battle Things****Beyond the Government: Mobilizing Industry and Academia**

Dr. Alexander Kott serves as the chief, Network Science Division, Army Research Laboratory headquartered in Adelphi, Maryland. In this position, he is responsible for fundamental research and applied development in network performance and security, intrusion detection, and network emulation. Between 2003 and 2008, Dr. Kott served as a Defense Advanced Research Programs Agency program manager responsible for several large-scale advanced technology research programs. His earlier positions included director of R&D at Carnegie Group, Pittsburgh, Pennsylvania, and IT Research Department manager at AlliedSignal, Inc., Morristown, New Jersey. Dr. Kott received the Secretary of Defense Exceptional Public Service Award and accompanying Exceptional Public Service Medal in October 2008. He earned his Ph.D. from the University of Pittsburgh in 1989 and has published more than 80 technical papers and coauthored or edited 9 technical books.

**John W. Link**

*senior consultant, VOLVOX Inc.*

**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 M.S. from George Mason University School for Conflict Analysis and Resolution and a B.A. in English from the University of Virginia.

## Dr. Douglas Maughan

*director of the Cyber Security Division, Homeland Security Advanced Research Projects Agency, Department of Homeland Security*

### Beyond the Government: Mobilizing Industry and Academia

Dr. Douglas Maughan has been at the Department of Homeland Security (DHS) since October 2003 and is directing and managing the Cyber Security Research and Development activities and staff at DHS Science and Technology. His research interests and related programs are in the areas of networking and information assurance. Dr. Maughan has been responsible for helping bring to market more than 40 commercial and open-source information security products during the past 12+ years while at DHS and is the senior executive responsible for the DHS Silicon Valley Innovation Program. Prior to his appointment at DHS, Dr. Maughan was a program manager at the Defense Advanced Research Projects Agency, and prior to that, he worked for NSA as a senior computer scientist and led several research teams performing network security research. Dr. Maughan received bachelor's degrees in computer science and applied statistics from Utah State University, a master's degree in computer science from Johns Hopkins University, and a Ph.D. in computer science from the University of Maryland, Baltimore County.

## Edmund Mitchell

*chief business development officer, CSIOS Corporation*

### Cyber and Intelligence Research and Development Funding Strategy

Dr. Edmund 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 R&D 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.

**Robert Mitchell***scientist, Sandia National Laboratories***Recent Developments in Linkography-Based Cybersecurity**

Before working for Sandia National Laboratories in the Cybersecurity Technologies Department, Dr. Robert Mitchell was a programmer at Boeing, BAE Systems, Raytheon, and Alcatel-Lucent. His research interests include moving target defense, computer network defense, computer network exploitation, cyberphysical systems, reverse engineering, game theory, machine learning, intrusion detection systems, modeling, and simulation. A former officer in the U.S. Air Force, he earned Ph.D., M.S., and B.S. degrees in computer science from Virginia Tech.

**Timothy Obenshain***project manager, ICF***Ransomware Over the Past Five Years: Overview and Best Practices**

Timothy Obenshain has been a member of the ICF team supporting U.S. Army Research Lab and HPCMP CDSP since 2008. He started work as an entry-level network security analyst and is now a project manager in support of U.S. Army Research Lab CDSP's Information Security Continuous Monitoring Solution. He holds bachelors' degrees in Communication and Media Studies, Political Science and Government, and Information Assurance from the University of Maryland College Park.

**John Paczkowski***senior vice president, ICF***Beyond the Government: Mobilizing Industry and Academia**

John Paczkowski heads ICF's homeland security and national resilience practice serving both public and private sector clients. A former career executive at the Port Authority of New York and New Jersey, he was the lead architect of a five-year, \$1.0 billion risk-based security capital improvement program after the attacks on the Authority's World Trade Center after 9/11. He has a B.S. in industrial engineering and an M.S. in engineering management from the New Jersey Institute of Technology, an M.A. in organizational psychology from Columbia University, and an M.A. in security studies from the Naval Postgraduate School. He is a senior fellow of the George Washington University Center for Cyber and Homeland Security and a board director for The Infrastructure Security Partnership. He is also a past chairman of the Security Analysis and Risk Management Association.



## Dhananjay Phatak

*associate professor, University of Maryland, Baltimore County*

### Securing Cyber Physical Systems

Dr. Dhananjay Phatak has been an associate professor of computer engineering in the Cyber Physical Systems Department at University of Maryland Baltimore County since 2000. His current research interests are in computer arithmetic algorithms and their hardware realizations, and all aspects of cyber/information/data/computing/network/systems security. His research has been supported by the National Science Foundation, NSA, and local companies (Aether Systems Inc., and Northrup Grumman), and he received the National Science Foundation 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 Ph.D. in computer systems engineering and his M.S. in electrical engineering from University of Massachusetts at Amherst and his B. Tech. from IIT Bombay (Mumbai) in electrical engineering.

## First Lieutenant Val Red

*U.S. Air Force*

### The Future of Cyber Operations and Technologies

First Lieutenant Val Red manages a collaborative enclave of system administrators and secure application developers who investigate, test, and assess new technologies for their readiness to transition into operational production network environments. He earned his B.S. in electrical and computer engineering at Rutgers University and his M.S. in cybersecurity, with a concentration in cyber operations, at Utica College. During his junior and senior years in undergraduate engineering, he served as webmaster and system administrator, respectively, for the Rutgers' Mathematical Finance graduate program and Rutgers Engineering Computing Services. Among his most recent achievements, he ranked number 10 out of 483 InfoSec practitioners in the 2015 SANS ICS Cyber Security Challenge and earned the title of Associate of (ISC)2 after passing the CISSP exam in July 2016.

## Lieutenant Colonel Paul Rozumski

*U.S. Air Force*

### **The Future of Cyber Operations and Technologies**

Lieutenant Colonel Paul Rozumski is commander of the 32d Intelligence Squadron, 707th ISR Group, 70th Intelligence Wing, Fort Meade, Maryland. He is the former deputy chief, Analysis Integration Branch, Analysis Division, deputy chief of staff, Intelligence, Surveillance and Reconnaissance. As a founding member of the Analysis Division, he led 12 military members and contractors to transform and modernize intelligence analysis across the U.S. Air Force. He also served on the Air Staff as the deputy director of Air Force wargaming and as an air-sea battle analyst. In those capacities, he led efforts to advance Air Force warfighting concepts and doctrine and shape defense policy and enable the national defense strategic guidance rebalance to the Pacific. He has significant experience in analysis, collection management, and operations-intelligence integration.

## 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 nongovernmental 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 B.S. in physics, an M.B.A., and is currently pursuing his doctorate at George Mason University's Computational Social Science program. His work focuses on the intersection of agent-based modeling and simulation, network analysis, and policy making. Mr. Shaheen is also associated with the Mitre Corporation.

## Sidney "Chuck" Smith

*computer scientist, U.S. Army Research Laboratory*

### **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 U.S. Army Research Lab 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+, NSA INFOSEC assessment methodology and INFOSEC evaluation methodology. He holds master's and bachelor's degrees in computer science from Towson University, where he is currently working on his doctorate.

## Captain Daniel Stambovsky

*U.S. Air Force*

### The Future of Cyber Operations and Technologies

Captain Daniel Stambovsky is a deputy flight commander for the 32d Intelligence Squadron, Fort George G. Meade, Maryland. He is responsible for the management, development, experimentation, and testing of land, sea, and air short/long-range communications systems. Additionally, he designs new antenna arrays fundamental to transmission/reception of advanced communication protocols and techniques. He enlisted in August 2004 and graduated ground radar systems apprentice training at Keesler Air Force Base, Mississippi, in June 2005. Following this he was assigned to 54th Combat Communications Squadron, 5th Combat Communications Group, Robins Air Force Base, Georgia, where he quickly attained the rank of staff sergeant. Captain Stambovsky was selected for the Scholarships for Outstanding Airmen to ROTC program and was commissioned as a 61D physicist with a B.S. in physics from University of Connecticut in 2012. He singlehandedly spearheaded R&D efforts in the radio frequency sensing and communications domain, performing first-of-its-kind satellite communications tests in Antarctica and holding five antenna-related pending patent applications. Prior to his current position, he was a distributed radio frequency applications physicist at the Information Directorate, Air Force Research Laboratories, Rome, New York.

## Dan Sullivan

*Supervisory Control and Data Acquisition researcher,  
Raytheon*

### Cybersecurity Risks in the Industrial Internet of Things

Daniel Sullivan is a senior principal software engineer at the Raytheon Company and supports the U.S. Army Research Lab in Adelphi, Maryland, where he researches methods to defend the Supervisory Control and Data Acquisition and ICS systems. He received his M.S. in electrical engineering from the Naval Postgraduate School and his B.S. in electrical engineering from the University of Illinois.

## Christian Thomasson

*U.S. Air Force*

### The Future of Cyber Operations and Technologies

Christian Thomasson works to identify the next generation of threats to our tactical systems. Upon identification of threats, he works to ensure that U.S. Air Force senior leadership is made aware of—and understands—the technical requirements to secure them. Mr. Thomasson is also a special agent with the Air Force Office of Special Investigations (AFOSI) in the U.S. Air Force Reserves. He became an AFOSI agent in 2003 and specialized in computer crimes in 2004. As a field examiner, he conducted investigations ranging from child exploitation to homicide to espionage.

The unique insights from his past have provided Mr. Thomasson with valuable context on the cyber landscape. Prior to AFOSI, Mr. Thomasson worked on F-15E and A-10 weapons systems, giving him further insight into the nature of advanced avionics and tactical system architectures.

## Sam Visner

*senior vice president and general manager, Cybersecurity, ICF*

### Cybersecurity and Privacy

#### The Cybersecurity Storm Front—Forces Shaping the Cybersecurity Landscape

Samuel Visner joined ICF in 2014 and has more than 35 years of experience in national security and cybersecurity work for the private sector and for the U.S. federal government. He is general manager for ICF's cybersecurity business. Previously, Mr. Visner held executive leadership roles at CSC Global Cybersecurity, SAIC, and NSA, where he served as Chief of Signals Intelligence Programs. Mr. Visner is an associate of the National Intelligence Council and serves as an advisor to the U.S. national security community. He is also a member of the Council on Acquisition Reform of the Intelligence and National Security Alliance (INSA) and is co-chair for INSA's Cybersecurity R&D Sub-council. He is also an adjunct professor of cybersecurity policy, operations, and technology at Georgetown University. Mr. Visner holds a B.S. in International Politics from Georgetown University and an M.A. in Telecommunications from the George Washington University.

**Era Vuksani***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 Massachusetts Institute of Technology Lincoln Laboratory. She joined the laboratory in October 2012 and is currently working in data analytics and network reconnaissance. Previously, she 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 B.A. 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 the Lincoln Laboratory.

**Mr. Mark Weatherford***senior vice president and chief cybersecurity strategist,  
vArmour, former Department of Homeland Security deputy  
undersecretary for cybersecurity***Cybersecurity and Privacy**

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 to create strategic security programs. He remains a senior advisor in the firm. In 2011, Mr. Weatherford was appointed by President Obama as the DHS's first deputy undersecretary for cybersecurity, and before DHS, he was the vice president and chief security officer at North American Electric Reliability Corporation, where he directed the cybersecurity and critical infrastructure protection program and worked with electric utility companies across North America.

# CyberSci

symposium2016

icf.com



## About ICF

ICF (NASDAQ:ICFI) is a global consulting and technology services provider with more than 5,000 professionals focused on making big things possible for our clients. We are business analysts, policy specialists, 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](http://icf.com).