09.28.17

CyberSci 2017 Symposium
Proceedings Report

#CyberSci2017

icf.com/cybersci

Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

ICF

icf.com/cybersci

#CyberSci2017

Contents

Introduction

The CyberSci Symposium 2017, for which the theme was : the Battle for Cyberspace," brought together participants from industry, government, and academia to share the important cybersecurity research and development (R&D) challenges. The Symposium took place September 28, 2017, at ICF's headquarters in Fairfax, VA.

The architecture of the Symposium included:

- Keynote speakers, addressing broad cybersecurity issues pertinent to cybersecurity R&D
- Policy and issue panels to discuss salient cybersecurity R&D challenges
- Technical representations, addressing specific cybersecurity R&D challenges.

Keynote speakers included:

- Samuel S. Visner, Senior Vice , Cybersecurity and Resilience, ICF (and adjunct professor, Cybersecurity Plicy, Operations, and Technology, Georgetown University)
- Mr. Larry Pfeiffer, Former Director,. White Hosue Situation Room
- Dr. Alexander Kott, Chief Scientist, Army Research Laboratory
- Mr. James Sidoran, Senior Project Manager, Air Force Research Laboratory
- The Honorable James Clapper, former Director of Natinoal Intelligence.

The Symposium's policy/issues panels included:

- The Battle for Cyberspace (Contested Cyberspace), chair by Samuel S. Visner and Aaron Gregg (Washington Post)
- Combating the Whole of Nation Cybersecurity, chaired by …
- Disruptive Technologies, Chaired by Dr. Misty Blowers, Vice , Cybersecurity Research, ICF

Technical presentations were organized in four tracks:

- Innovation for Information Sciences
- Computational Intelligence for Cyber Network Defense
- Cybersecurity, Vulnerability & Threat Assessment
- World of Cyber/Internet of Things

Technical track presentations were selected through anonymous peer review. Presentations ranged from designing intelligent assistants and using supervised learning to prioritize IDPS alerts to adaptive command and control in the age of hybrid warfare.

Summaries of the keynote speeches are provided along with recaps of the panel discussions and breakout sessions. Information presented here represents the opinions of ICF, not necessarily those of individual CyberSci 2017 panelists and presenters.

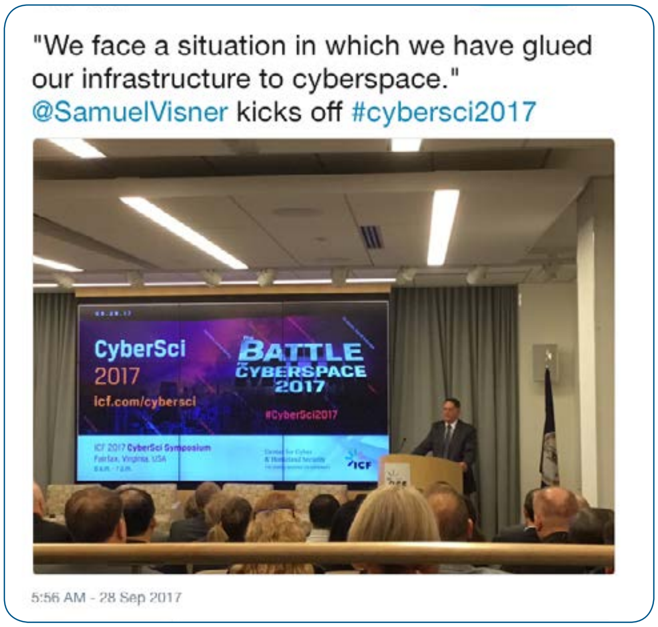
In addition, the CyberSci Symposium provided an opportunity to develop Cybersecurity Research and Development Recommendations for the Government of the United States and the broader cybersecurity R&D community in academia and the private sector. These Recommendations reflect the view of the Symposiuim's organizers, and are not necessarily the views of the Symposium's participants. The Recommendations, also available separately, are included in this Proceedings.

Executive Summary

The stakes have risen for cybersecurity that protects national interests effectively in the United States. Recent breaches reported in the electrical power grid and by credit monitoring services suggest a spectrum of motives ranging from large-scale financial theft to undermining the functionality of U.S. critical infrastructures. We see evidence that other countries are attempting to use cyberspace to diminish public confidence in national institutions, to alter electoral politics, to create disorder in our political processes, and to diminish public confidence in national institutions. These developments are troubling and may represent conceptions of cyberspace held by other countries that differ from the approach our own country has taken traditionally. The "Battle for Cyberspace," while not declared, has become a reality.

With an eye toward identifying and addressing the cybersecurity R&D challenges inherent in this battle, ICF recently hosted the CyberSci2017 Symposium, in cooperation with the George Washington University Center for Cyber and Homeland Security. The event—which featured leading experts on cybersecurity from a range of industries and organizations—addressed our need to confront and defeat efforts by others to seize and control the cyberspace on which our country's national security depends, and to which our critical infrastructures have become connected.

In his opening remarks, ICF Senior Vice President Samuel S. Visner introduced the concept of cyberspace as an environment in which other countries are contesting for influence, governance, sovereignty, and control. In contrast, the U.S. tends to view cyberspace as a "global commons," like oceanic waters, beyond the sovereign control of individual countries. America's government and military leaders don't think of cyberspace as sovereign territory; we don't claim it, and we certainly don't attempt to govern it. At most, we attempt to deter, detect, and defeat criminal and adversary activity. Authoritarian states, however, may believe that cyberspace is analogous to physical sovereign territory with the same opportunities, even obligations, for governmental control.



"We face a situation in which we have glued our infrastructure to cyberspace." @SamuelVisner kicks off #cybersci2017

5:56 AM - 28 Sep 2017

CyberSci 2017's speakers, panels, and technical track sessions considered the evolution and future of the Battle for Cyberspace from many perspectives:

- **Policy.** What are our interests in cyberspace?
- **Operational.** What do we do to prepare, manage, and recover?
- **Technology.** How do we build and sustain our edge to secure cyberspace for our interests, values, and institutions?

Cybersecurity Research and Development Recommendations Keynote Presentation Summaries

Cybersecurity and the White House Situation Room

Larry Pfeiffer, Senior Advisor at The Chertoff Group, former Senior Director of the Obama Administration White House Situation Room

A 32-year veteran of the intelligence community, Mr. Pfeiffer explained his roles and responsibilities in charge of the White House Situation Room, which include:

- Meeting space to host policy and national security meetings at the highest level of classification
- 24x7 watch operation (9 people) to monitor and raise alerts about breaking developments from around the world, utilizing a network of watch centers and awareness about areas of special interest (e.g. when head of Spain visits, focus on Spain)
- Support for information exchange between people/rooms at the highest levels of government and assure 24x7 information flow
- Switchboard for national security issues as the easiest place to find key players, maintain awareness, and ensure secure, high quality communications
- High-side secure communications (phones, teleconferencing, TS SCI computing) for national security council and executive branch staff including secure connectivity at workspaces, homes, and on travel (even aboard boats)
- Continuity of government's requirement for seamless support no matter what, so alternate locations are established and tested regularly along with tools that will ensure emergency decision-making is based on accurate, timely information

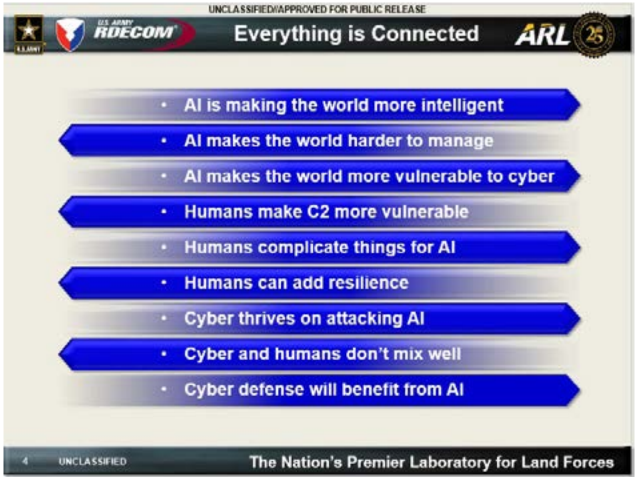
Initially, Mr. Pfeiffer found no plan for cybersecurity in Situation Room, so he made it a priority to sync up with cyber watch centers in DC and establish physical security. The hardest part of this challenge was determining what level of cyber incident required the President's attention. Staff needed training on what alerts even meant and eventually the stream of alerts was narrowed to only the most important. Awareness and education for Situation Room staff is a priority, with continual reminders about the importance of security and extreme care with phone storage (i.e not good enough to just switch it off and hold onto it).

Mr. Pfeiffer explored technology for its ability to improve Situation Room functioning and speed processes for analysts. State-of-the-art encryption meets the highest standards for security and even required that staff outfit encryption keys for that meet our communications security standards (using devices we own/manage) for counterparts in over 15 countries. Data analytics could help with filtering info (especially from Twitter) and improving the delivery of daily cybersecurity summaries (as produced now or as a new medium to be fed electronically all day, enhanced with graphics/images, etc.)

AI, Robotics and Cyber: How Much Will They Change Command and Control?

Dr. Alexander Kott, Chief Scientist, U.S. Army Research Laboratory

Dr. Kott presented his vision, reflecting a view of "intelligence" that unites the physical and cyber worlds. He explored the confluence of cyber and artificial intelligence (AI) in the context of military command and control and detailed the strengths and weaknesses of three groups that will increasingly work together for good or for bad: Bots (AI), Bits (cyber/IT), and Bodies (humans).



UNCLASSIFIED//APPROVED FOR PUBLIC RELEASE

U.S. ARMY RDECOM | Everything is Connected | ARL

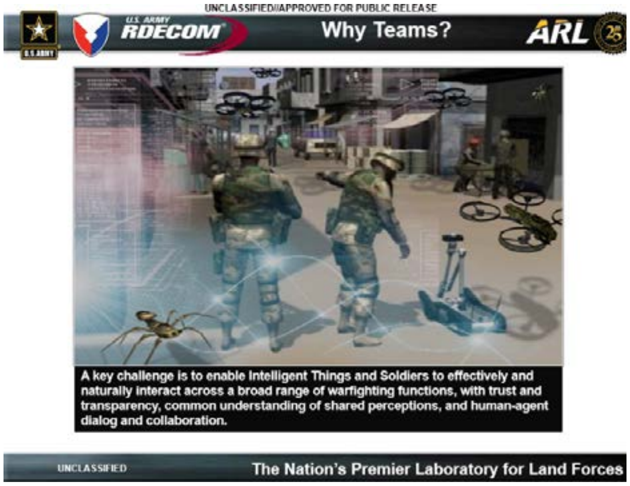
- AI is making the world more intelligent
- AI makes the world harder to manage
- AI makes the world more vulnerable to cyber
- Humans make C2 more vulnerable
- Humans complicate things for AI
- Humans can add resilience
- Cyber thrives on attacking AI
- Cyber and humans don't mix well
- Cyber defense will benefit from AI

4 UNCLASSIFIED The Nation's Premier Laboratory for Land Forces

In an extremely complex battlefield of human, AI, and IT devices—all interconnected and multi-directional—human cognition will emerge as the most severe constraint.

We seek information that is well-formed, reasonably-sized, essential, and highly relevant to our current situation and mission. We try to classify and aggregate information. And we are most susceptible to deception.

AI will be the solution to cyber attacks. Intelligent agents can defeat adversaries by redirecting to believable honeypots and honeynets, fighting back with anomaly detection, using continuous learning, and employing large-scale physical fingerprinting. But before we can populate the world with intelligent agents that rapidly learn, adapt, reason, and act in contested, austere, and congested environments, there are AI gaps to address (e.g. inability to handle small samples, dirty data, high clutter).



UNCLASSIFIED//APPROVED FOR PUBLIC RELEASE

U.S. ARMY RDECOM | Why Teams? | ARL

A key challenge is to enable Intelligent Things and Soldiers to effectively and naturally interact across a broad range of warfighting functions, with trust and transparency, common understanding of shared perceptions, and human-agent dialog and collaboration.

UNCLASSIFIED The Nation's Premier Laboratory for Land Forces

Success will depend on humans and AI teaming up to benefit from the strengths of each:

- Humans – understand implications, comfortable with lack of formality, understand each other, negotiate, adjust to ambiguity
- AI – needs defined goals, no personal agendas, no groupthink, not vague, detects inconsistencies

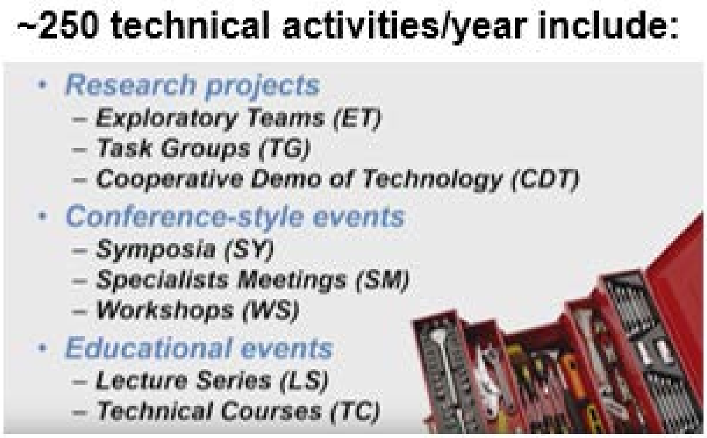
In 20 years, we'll see societal change to a mixed society, in which we're just one kind of intelligent being. Cyber science will focus on how to keep society running. This year's CyberSci set a record for the number of papers touching on AI, which reflects the trends we're discussing.

NATO's Role in Advancing Science & Technology and Multi-Domain Mission Modeling

James Sidoran, Senior Project Manager, U.S. Air Force Research Laboratory

Mr. Sidoran began his presentation with a review of NATO's purpose, membership, and structure. He shared quotes about NATO from different top-level perspectives, including from General James Mattis: "… Having served as NATO Supreme Allied Commander, … NATO is the most successful military alliance [probably] in modern history, maybe ever …"

Looking specifically at NATO Science and Technology, it's an organization, called Science and Technology Organization (STO) and a process that coordinates a distributed network of international experts, representing approximately 250 technical activities/year and roughly 5,000 experts.



~250 technical activities/year include:

- *Research projects*
  - *Exploratory Teams (ET)*
  - *Task Groups (TG)*
  - *Cooperative Demo of Technology (CDT)*
- *Conference-style events*
  - *Symposia (SY)*
  - *Specialists Meetings (SM)*
  - *Workshops (WS)*
- *Educational events*
  - *Lecture Series (LS)*
  - *Technical Courses (TC)*

Long-term goals are to:

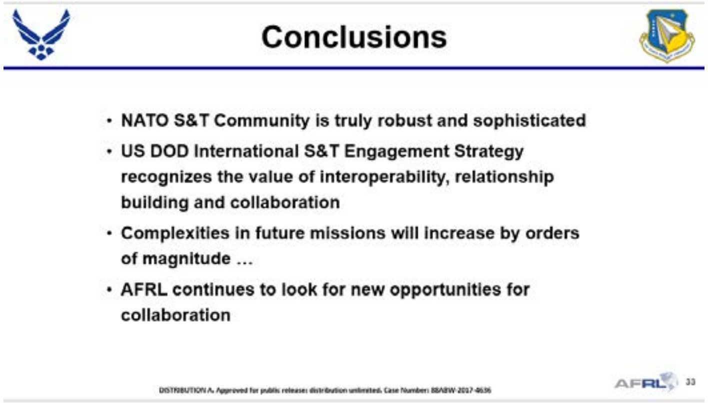
- Enhance interoperability, relationship building, and collaboration (ensure compatibility and lines of communication)
- Advance S&T

STO comprises the Office of the Chief Scientist, the Science & Technology Board, the Center for Maritime Research and Experimentation (CMRE), and the Collaborative Support Office (CSO).

As an example of an Exploratory Team research project, Mr. Sidoran shared a closer look at NATO's southern flank, the Mediterranean and activities including:

- Multi-domain Mission Modeling
- Unmanned and Autonomous Vehicles
- Mission Assurance
- Risk Assessment

He shared another applicable quote from General Mattis: "… security is always best when provided by a team … reinforcing deterrence and defense, and more directly addressing terrorist threats along NATO's southern flank, from the Mediterranean to Turkeys' border … new threats such as terrorism, cyber threats, and hybrid war …"



Conclusions

- NATO S&T Community is truly robust and sophisticated
- US DOD International S&T Engagement Strategy recognizes the value of interoperability, relationship building and collaboration
- Complexities in future missions will increase by orders of magnitude …
- AFRL continues to look for new opportunities for collaboration

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number: 88ABW-2017-4636

AFRL 33

The Battle for Cybersecurity

James Clapper, former Director of National Intelligence

Mr. Clapper began his remarks by admiring CyberSci's "assembly of big brains" and framed his intent to add a political science perspective to the technology, policy, and operational views expressed throughout the day.

Cyber is a tool used for propaganda, especially in social media, and exemplified by Russia's interference in the 2016 election. Posing a threat to our basic systems, Putin's goals were threefold:

1. Sow discord/discontent within US electorate
2. Make sure Hilary Clinton lost (out of paranoia about revolution she was fomenting)
3. Promote (the more desirable) Donald Trump

Russia is by far our biggest, most sophisticated threat. In 2016, their tactics were very aggressive and multi-faceted, including trolls, fake news, and use of RT to monitor and control information.

If we consider two groups of adversaries, nations vs non-nation players, nations are actually more vulnerable. They have much more to lose. And in some cases, information operations can compensate for other weaknesses.

Our next biggest threat after Russia is China, but in contrast to Russia, the Chinese economy is bound with ours. Even the threat of economic sanctions can be an effective deterrent. Next level threats are Iran and North Korea.

What can we do to protect ourselves?

1. Secure voting apparatus at the state level and the RNC/DNC, designate it as critical infrastructure.

2. Educate the public.

Mr. Clapper recounted Iran's 2012 Denial of Service attack on the U.S. financial services sector. With excellent attribution, the U.S. teed up a response, but Secretary of the Treasury Tim Geithner feared counter-retaliation, so we did not follow through with it. Lesson learned: It is pointless to attack if you are not confident in your defense against the worst-case scenario.

North Korea's attack on Sony also had excellent attribution and again the U.S considered retaliation options. In this case, we would have to use another country's infrastructure to help, and so again, the U.S. did not respond. Thus far, our only responses have been naming/shaming and economic sanctions.

Cyber R&D efforts are focused on auto cyber defense, situational awareness, mission support, critical infrastructure, endpoints/edges, IoT, and HW/SW assurance (meeting the supply chain challenge).

How do other countries and non-state actors view cyber?

Cyber is an enabler, a tool, not an end in itself, and the U.S. government is guilty with others of framing it as a standalone. Among other countries, there are two camps: Russia, China, Iran, and North Korea see cyber as divisive, the rest of United Nations countries seek to establish common norms.

Technical Track Presentations | Track 1: Innovation for Information Sciences

Session A

A Game Theoretic Model of Computer Network Exploitation Campaigns

By: Robert Mitchell – Member of Technical Staff, Sandia National Laboratories

Increasingly, cyberspace is the battlefield of choice for twenty first century criminal activity and foreign conflict. The Ukraine power grid attack of December 2015, the April 2016 United States Democratic National Committee (DNC) hack, the Banner Health spill of June 2016, the October 2016 Dyn Domain Name System (DNS) Distributed Denial of Service (DDoS) attack, the San Francisco Municipal Transportation Agency (MTA) ransom of November 2016 and the May 2017 WannaCry pandemic exemplify this trend's high impact. Management and incident handlers require decision support tools to forecast impacts of their investment decisions and technical responses, respectively.

Mathematical (e.g., closed form equations) and stochastic (e.g., Petri nets) models provide rigorous insight based on first principles. However, these models fall short when it comes to the human element of cyber warfare. Simulations and emulations suffer from the same flaw. Furthermore, simulations and emulations are not viable at Internet of Things (IoT) scale. Despite these shortcomings, leadership and incident responders still require situational awareness.

Game theoretic models consider the collaborative and competitive interaction between rational players striving to achieve their own best possible outcomes. This technique has yielded great results in the field of economics where eleven game theorists have won the Nobel Prize. We propose a game theoretic model based on a six phase model of computer network exploitation (CNE) campaigns comprising reconnaissance, tooling, implant, lateral movement, exfiltration and cleanup stages. In each round of the game, the attacker chooses whether or not to continue the attack, nature decides whether the defender is cognizant of the campaign's progression, and the defender chooses to respond in an active or passive fashion, if applicable. Decision makers can use this game theoretic model to implement defensive measures, and information security practitioners can develop tactics, techniques and procedures (TTPs) that render attacks inviable.

First, we proposed an extensive form game: This game is noncooperative, asymmetric, non zero sum and sequential; the current iteration of the game uses only discrete strategies and assumes perfect information. Next, we converted the extensive form game into normal form to facilitate analysis. Third, we identified the payoff functions for the attacker and the defender for every pure strategy set in the game. Attacker related parameters include cost of executing each attack phase and the value of the target data. Defender related parameters include cost of responding to each attack phase, the cost of spilling the target data and the value of the threat intelligence harvested from each stage of the attack. Nature related parameters include the probability of detecting each attack phase. Finally, we implemented an algorithm to find the pure strategy Nash equilibria given any parameterization of the game.

Session B

COUF, a Better Big-Data Analysis Method

By: Dr. Zhiping Wang – Founder, W Analytics

In the age of internet more and more people are using internet. As the results, tremendous data are generated every day and cyber security has become serious problems for government agencies, commercial companies and other organizations, as well as individuals. In order to ensure cyber security, big-data analysis is inevitable and critical. Currently Hadoop, Shark and others are widely-used big-data analysis methods. But each of them has its own problems, they cannot avoid redundancies, hence they are not efficient.

I will introduce a new big-data analysis method, COUF, or "Calculate Once, Use Forever". Unlike Hadoop and other big-data analysis methods, COUF eliminates both read and computation redundancies, hence it is much more efficient and effective. COUF is easy to implement, easy to use and easy to maintain. With COUF, cloud might not be needed in many cases. COUF will help every organization to increase cyber security. Furthermore, COUF will save millions of dollars for most of business.

Session C

Suggestions for Small Business Security Architecture in Response to Weapons Grade Exploits and Attack's in Critical Infrastructure

By: Adam Lipinski – President, Palm Solutions

Critical infrastructure and consumer systems are increasingly threatened by weapons-grade cyber exploits and attacks. Many of these networks are not built to withstand threats of this sort. Development of Enterprise Security Architectures is an appropriate response to weapons-grade cyber exploits and attacks in critical Infrastructure and consumer systems.

This paper will examine forces in play that will drive development of enterprise IT security architectures based on the federal government to be the norm for commercial and medium sized non-government organizations rather than only an endeavor for large-scale government contractors. Factors such as the gravitational pull of the federal government's Risk Management Framework, strong incentives in the administrations Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," market shifts to cloud computing, and legal liabilities will drive the cost benefit analysis for investment in enterprise security. Fortunately, there are several processes already developed to lessen the burden. This paper will briefly review the elements of a successful enterprise architecture, review of application of processes of the National Institute Standards and Technology (NIST), the Federal Risk and Authorization Management Program (FedRamp), and conclude with a brief mention of other standards which US entities may have to consider such as those of the European Union.

Session D

Adaptive Command and Control in the Age of Hybrid Warfare

By: Dr. Jim Greer – Vice President, for Strategic Leadership & Design, Abrams Learning and Information Systems

John Link – Director of Operations, VOLVOX, Inc.

Hybrid Warfare was actually coined in a 2005 article by current Secretary of Defense James Mattis. Hybrid Warfare is "the true combination and blending of various means of conflict, both regular and unconventional dominating the physical and psychological battlefield with information and media control…with the goal of breaking the opponent's will and eliminating the population support for its legal authorities."[1]

Hybrid Warfare exists in and involves a complex interplay of multiple domains: Diplomatic, Political, Economic, Cyber/Information, Media, Social Media, Psychology, Electromagnetic Warfare, and multiple degrees of Military Engagement. Further, within each of these Domains are multiple subdomains and interactions between domains – e.g. a hack becomes a Twitter, that ignites a political movement, which in turn becomes cover for Special Forces to merge with local irregular forces to change facts on the ground. National Security Leadership must manage an expanded battlespace from Networks, to TV, to Markets to Frontlines, and must identify rapidly moving elements in the hybrid attacks and formulate counter measures.

The Russians have developed the most complete Hybrid Warfare Doctrine — while Iran, North Korea, China and Non-State ISIS have all begun to utilize such a doctrine to varying degrees.

One of the keys to Russian Hybrid Warfare Doctrine is "Reflexive Control," shaping the enemy's perceptions to shape their actions to fit desired outcomes.

The challenges for our evolving Counter Hybrid Warfare Doctrine are amplified in US/NATO Command and Control that is siloed into various Areas of Operations (AO) and Domains, Nations, Combatant Commands, DNI, Agencies, and the National Security Council; structures designed to monitor and respond to conventional Military, Diplomatic and Intelligence activities of State Actors. Hybrid Warfare relies on these silos for Reflexive Control and favors the offense, combining multi-domain actions, stealth, and paralyzing deniability. Hybrid Warfare is also non-linear and adaptable to changing facts.

Responding to Hybrid Warfare requires creating adversary-specific fusion centers that can identify the disparate and seeming unrelated and unacknowledged activities of a Hybrid Warfare aggressor and coordinate responses.

This presentation will focus on the:

- Our Current Understanding of Hybrid Warfare and Reflexive Control
- The Centrality of Cyber, Social Media and Media to Hybrid Warfare
- Use of Collaborative Command which allows these command siloes to create emergent strategic and tactical response, including cyber.
- How to create Adversary-Specific Fusion Centers to monitor the Hybrid Warfare adversary and support Collaborative Command response across AOs.

[1] Guillaume Lasconjaris & Jeffery A. Larson, Introduction: A New Way of Warfare, NATO's Response to Hybrid Threats Journal, NATO Defense College 2015.Track 2: Computational Intelligence for Cyber Network Defense

Track 2: Computational Intelligence for Cyber Network Defense

Session A

Intrusion Detection and Prevention System (IDPS) Alert Prioritization through Supervised Learning

By: Gregory Shearer – Developer, ICF

Real-world implementations of intrusion detection and prevention systems (IDPS) by a computer network defense provider often produce a huge volume of alerts, of which only some fraction are actionable, while many others are false positives. Given the ever-increasing scale of monitoring needs and the frequent lack of qualified personnel, alert volume often exceeds the ability of analysts to view, classify, and report on such alerts in real time. The traditional answer to this problem is to implement controls, such as filters, blacklists, whitelists, and user-defined priority values to reduce analyst workload. However, these methods tend to examine only part of an alert, rather than the whole. In our study, using online supervised learning algorithms that dynamically incorporate past knowledge into a holistic prioritization process for new incoming IDPS alerts, we show which IDPS alerts are most significant and require highest priority for rapid response and immediate reporting. We reveal that these models can enhance IDPS accuracy in addition to improving its ease of use.

Session B

Creating an Adaptive Security Architecture Framework to Combat Advanced Threats

By: Matthew Joseff – Security Specialist, Splunk

Security architectures typically have involved many layers of tools and products as part of a defense-in-depth strategy. Unfortunately, they have not been designed to work together, leaving gaps in how security teams bridge multiple domains. In today's nefarious threat landscape these gaps are magnified and in many cases, pose a hurdle for optimal use of these investments and response capabilities. What is needed is a consistent framework that can provide a common interface for end-to-end visibility, automated retrieval and collaboration in a heterogeneous multi-vendor environment enabling security teams to quickly adapt to attackers' tactics using a range of actions including automated response. Such an approach would enable participants to extract new insights from existing security architectures and monitor, analyze and detect threats across the kill chain.

This presentation will focus how machine data from across the entire security and IT ecosystem can accelerate an Adaptive Response Initiative to create a robust and agile defense against today's advanced and increasing complex threats. We will also address how this approach can build confidence in security teams to automate response while optimizing your investments in defense-in-depth tools.

Session C

Interrogator the Next Generation

By: Sidney Smith – Computer Scientist/Team Leader, Product Integration & Test Team, U.S. Army Research Laboratory

The US Army Research Laboratory has been using the Interrogator Network Intrusion Detection Architecture since 2004. Over the years the system has been update and modified several times. Recently a major modification to the graphical user interface (GUI) was planned to better integrate Interrogator into the Defense Information Systems Agency's Big Data Platform (BDP). In preparation for this effort, a baseline usability survey was conducted. This study produced 17 finding or which 9 were critical and 2 were duplicates. The focus of this presentation is the following 7 critical finds. **1)** The results of queries were slow to load and there was a general sluggishness in the performance of the GUI. **2)** Sometimes queries would return the wrong data or relevant data would be missing from the results. **3)** Interrogator allows the analyst to replay the network traffic that contained the alert, but it would often take an unacceptable amount of time for the system to gather and display the relevant traffic. **4)** The systems needs to collect relevant data, index this data, and display the data to the analyst. There were instances where a break down is one of these processes prevented the analyst from seeing the data necessary to fully understand the alert. **5)** Preparing an incident report is a time consuming process. There were instances where a timeout would be reached in the middle of preparing a report and all of the data entered would be lost. **6)** There were occasions where an analyst would open a form and it would be populated with residual data. **7)** Over the years many analysts have written scripts to automate repetitive tasks. These scripts have matured into a suite of command line tools. Many analysts expressed a desire for the speed and functionality of these command line tools. This presentation enumerates these 7 critical finding, describes how they were addressed when the Interrogator GUI was rewritten to be more compatible with the BDP, and the testing procedures which verified that they were corrected. This presentation enumerates the 7 critical findings. It discusses the root causes. It reviews typical solutions found in the literature. It describes the technologies and techniques used to address them when the Interrogator GUI was rewritten. It presents the testing procedures and results which verified that they were corrected.

Session D

Online Data Analytics and Adaptive Malware Defense for Cyber Resilience

By: Hasan Cam – Computer Scientist, U.S. Army Research Lab

A cyber resilient system needs to adaptively resist against attacks, minimize the adverse impact of vulnerability exploitations, and recover any compromised asset of the system. Such a resilient system requires not only detection and assessment of its vulnerabilities, attacks, and exploitations in real-time, but also determining those actions needed to keep the system resilient, controllable and observable, no matter whatever uncertainty or incomplete information is available. This paper proposes to employ a combination of online data analytics of all observations, real-time risk assessment, adaptive malware defense and maneuvers, with the help of machine learning and control-theoretic approaches. This approach requires not only detection of adversary activities, malware indicators, intrusions, and vulnerabilities, but also analysis of their interactions, causality, temporal and spatial orderings in real time. In order to provide an effective control of malware infection and spread, this paper presents a temporal causality and reward-based approach to analyzing and modeling the interactions of cyber events, assets, and sensor measurements and, then, taking actions to limit malware spread, recover infected assets, and patch vulnerabilities. The execution of such online and adaptive actions, especially in an automated manner, significantly enhances cyber resiliency of systems.

Track 3: Cybersecurity, Vulnerability & Threat Assessment

Session A

Human Factors Contributing to Cyber Vulnerabilities

By: Dr. Susan Conrad – Assistant Professor of Information Technology and Cyber Security, Marymount University

Daniel Broder – Graduate Student, Marymount University

Advancements in technology, Artificial Intelligence and Predictive Modeling are all on the forefront of combatting cyber-attacks, yet still it is the human vulnerability that continues to challenge organizations from becoming a victim. With the growth of social media, online presence and increased internet activity, unknowingly individuals become the reason systems become compromised. To better understand this phenomenon, a study about phishing and cyber awareness was conducted to learn how vulnerable individuals were for failing prey to social engineering attacks. The results may surprise you.

Session B

Increasing Efficiency in Packet Content Analysis for String-Literal Matches

By: Jason Ellis – Researcher, ICF

One of the dominant methodologies of intrusion detection involves examining packet content for string-literal matches of known malicious URLs or patterns. This allows a cyber security operation to label traffic sessions for further analysis and dissection to determine the potential of harm to friendly assets. One well-known tool that provides such pattern matching capabilities is Snort. This tool allows security analysts to create/use a set of rules that generates alerts upon observing packets with content matching the criteria defined within the rules. Currently, most intrusion detection processes rely heavily on the ability to efficiently relay these alerts back to the analysts, so that they may more deeply inspect the traffic sessions in question. In this talk, we compare the performance cost and benefits between using Snort versus a Perl Compatible Regular Expression (PCRE) sub-process for observing patterns contained within packets. We, first, review a novel network traffic collection tool, the Feature Extraction and Analysis Tool for Sessions (FEAT-S) – a collection and session representation hybrid. We implement both approaches within FEAT-S. We show, using a variety of Snort rules and their PCRE equivalents, that a PCRE sub-process within a FEAT-S sensor will allow for faster labeling of sessions, and thus, a faster intrusion detection process, than a sensor-side Snort instantiation.

Session C

A Performance Monitor Unit Based Approach for Malware Detection

By: Chen Liu – Assistant Professor, Clarkson University

Nowadays malicious software targeted towards computer systems continues to proliferate. There exist many classes of malware, e.g., Rootkits, Viruses, Trojans, Worms, Spywares, and Exploits, each having its own set of goals and behavior. Their complexity varies from simple toy programs to incredibly sophisticated attacks that span across several system's layers. To address the malware problem, researchers have devised various prevention and detection schemes, covering every stage of the malware life-cycle, from creation, distribution, to execution. Despite the valiant efforts, prevention techniques are not perfect as evidenced by the continued presence of vulnerabilities and the existence of third party marketplaces. Detection techniques are hence used as an extra line of defense when prevention fails. Performance Monitoring Unit, or the PMU, is found in all high-end processors these days. The PMU is basically hardware built inside a processor to measure its performance characteristics. We can measure hardware level events like instruction cycles, cache hits, cache misses, branch misses and many others. And as the measurement is done by the hardware there is very limited overhead. In this work, we propose a data-driven, machine-learning aided anomaly detection approach that utilizes information collected from the PMU at hardware level to detect malware attacks in user space libraries and applications. In our proposed approach, we will monitor different hardware events and employ advanced machine learning algorithms to help us classify between regular and abnormal behavior for the vulnerable applications. Our goal is to construct a run-time defending mechanism that use information obtained from low-level hardware events to detect malware attacks.

Session D

The Use of Packet Header Anomaly Detection in Lossy Network Traffic Compression for Network Intrusion Detection Applications

By: Sidney Smith – Computer Scientist/Team Leader Product Integration & Test Team, 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 if this is an actual intrusion or a failed attempt. The Interrogator Network Intrusion Detection Framework 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 of the 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. In previous research Smith and Hammell proposed that it should be possible to create a lossy compression tool using anomaly detection techniques. This strategy relies of the fact that most anomaly detection algorithms generate a score which may be used to measure how unusual a packet or session may be. The compression tool compares this score against a threshold to eliminate the most normal traffic from the data stream. The Snort network intrusion detection tool is run against a data set to establish a baseline of alerts. It is then run against the compressed data set to discover how many alerts were lost or the alert loss rate. This threshold is adjusted to find the best compression with the least alert loss. This research considers the Packet Header Anomaly Detection tool by Matthew Mahoney and Philip Chan as the anomaly engine for a network traffic compression tool. It describes efforts to modify the tool to work in this application. Specifically, the program was updated to use Libpcap and account of byte order, several key constants in the anomaly computation algorithm were made easy to adjust, and the training mechanism was adjusted to remove the requirement for clean training data. The results of using this new compression tool to compress the cyber defense exercise 2009 usama020 data set are presented graphing the compression and the alert loss rate for various anomaly thresholds.

Track 4: World of Cyber/Internet of Things

Session A

Designing an Intelligent Assistant to Augment Security Workers

By: Robert Flair – Data Scientist, Endgame

The security industry faces a workforce shortage, with an estimated deficit of 1-2 million workers in the coming years. In security operations centers, this shortage is compounded by non-intuitive interfaces and complex query languages that further impede the capabilities of the current security workforce. Researchers tackling this problem have focused more on augmenting analysts through standardized analytic processes, such as collaboration and information sharing, and less on providing user-friendly capabilities to help augment inexperienced and experienced analysts alike. Assistive technologies, such as conversational interfaces (e.g. chatbots), could fundamentally shift the way defenders interact with and wrangle the increasingly complex and growing data challenges.

Conversational interfaces and other assistive technologies, have increasingly been employed in other use cases that have both big data problems as well as users who lack the time, resources, or skills to analyze the data. These intelligent assistants can provide "best practices" guidance and recommended paths to desired actions within an intuitive, natural language interface. Could intelligent assistants similarly help security professionals defend their networks? To answer this question, we conducted user-experience research across diverse roles, behaviors, and workflows employed during day-to-day operations. We documented many of the key pain points of experienced and inexperienced analysts, including alert fatigue, data overload and complex user interfaces. In response to this research, we created a conversational interface to address these challenges while augmenting detection and response capabilities.

We will present our research and development process, including our user-centric research and personas that scoped the problem, the findings from our study, and the design requirements we generated. The result will be a case study dissection of Artemis, our conversational interface to reduce alert fatigue through natural language search, workflow recommendations, and guided triage. Throughout this use case, we will highlight the challenges we encountered and how we decided upon our solution. This will include limitations of open source bots for the security domain, as well as a solution that marries natural language processing and domain expertise within a user-friendly interface. Finally, we will stress the importance of the feedback loop and user testing that helped us hone a conversational interface that fits within but also augments the current workflow, expediting detection and discovery for security professionals.

Session B

ACAP's Quantum Leap to Interagency Agility

By: Jo Lee Loveland – President, VOLVOX, Inc. , John Link – Director of Operations, VOLVOX, Inc.

Based on DOD estimates, over the past 3 years, intrusions into critical U.S. infrastructure have increased 17 Xs. This portends even more urgency to develop more effective interagency strategies to combat them.

Originally proposed in 2015, the Agile Cybersecurity Action Plan (ACAP) is a Cybersecurity Strategy that uses an agile cycle of assessments of an organization's technology, people, processes, and polices against their constantly updating threat/risk matrix to identify needed upgrades to counter emerging threats and risks.

The success of ACAP relies on a whole systems approach to governance, self-assessment, information-sharing, and cybersecurity strategy development. Whole-systems thinking require eliminating information silos and hierarchal barriers to collaboration, yet retaining the legitimate equities of the various parts of the organization and its leadership.

Across the government our focus on insuring Cybersecurity "due diligence" is through standards/compliance via FISMA and Nation Federal Cybersecurity Framework which has the effect of creating compliance culture, while not adapting to changing threats. This is compounded by the tendency of agencies to not share their experiences (often failures), threat data, and ongoing risks that undermine their compliance narratives. While CDM has made some resources available it has tended to create "winners and losers" reducing the likelihood of innovative solutions succeeding in the Federal Market.

We are proposing an Agile Interagency ACAP-like Process to maximize threat and risk information sharing, development of innovative solutions and the creation of shared approaches to implementation.

This kind of agile interagency process creates fractal self-similarity and boundaries with the agencies without compromising their Jurisdictional Authorities. Moreover the government is notorious for great "problem identification", but allowing bureaucratic entropy to cripple implementation.

The critical component in ACAP the integrated Threat/Risk Matrix which requires fearless information sharing so technology, process, policy and people can be organically upgraded to meet emerging threats. ACAP, with its reliance on feedback loops and embrace of both linearity and non-linearity in understanding emerging ambient and targeted threats, can better enable our systems for ready response to strategic variations.

In brief, ACAP is a systems understanding that takes advantage of whole system creative thinking. Initially designed for a prototype CONOPS for a single system, ACAP has been expended in scope to embrace more broadly across systems. Now drawing in part on a breakthrough unified Fractal Model used in an intervention at Federal Aviation Administration to redefine three towers largely disconnected operationally, ACAP applies a nonlinear operational cross-design that allows efforts to harmonize process and policy beyond conventional modes of operation.

Session C

Using AWS IoT securely

By: James Robertson – Program Chair Software Development and Security, University of Maryland

Low cost sensors continue to become available and are connected to the Internet through the Internet of Things (IoT) revolution. With hundreds or even tens of thousands devices being connected to the cloud, large amounts of data are produced which could be ingested, parsed, processed, stored, analyzed and visualized.

Cloud technology from vendors such as AWS and Google have processes and technology in place for securely communicating with hundreds of thousands of sensors and performing big data analytics.

This paper and presentation provides detailed steps along with a demonstration of successfully and securely connecting low-cost IoT devices built on Raspberry Pi and Beagle Bone processor boards to leverage cloud technology using identity and access control management, log analysis and simple notification systems to alert system administrators of possible security issues and compromises.

AWS is used to communicate with and authenticate each sensor. Atypical patterns are identified and flagged for additional review and analysis. For example, analysis may reveal unusual access times or attempts to access sensors or sensor data that are considered unusual or atypical.

Session D

IoT Security at the Lowest Common Denominator– Power Analysis and AI

By: Steven Chen – CEO, PFP Cybersecurity

The emerging Internet of Things, with billions of new devices that have embedded network connectivity, is increasing both the urgency and the challenge of securing our information infrastructure. Internet of Things (IoT) cyber attacks include device impersonation, hacking, counterfeiting, snooping, and tampering are growing fast, causing disruption and damage.

Power analysis is a mature technology which has been used in side-channel attacks. Differential Power Analysis (DPA) can extract a secret key by measuring the power used while a device is executing an encryption algorithm. Power Fingerprinting turns the tables by using power analysis to detect tiny changes in power consumption caused by malicious changes in hardware, firmware, software, configuration, or data.

Cyber resilience greatly improves with immediate attack detection and remediation. It is broadly accepted that preventing all attacks is not realistic. Thus, the goal of PFP is to prevent or mitigate damage by detecting anomalies in power consumption caused by malicious execution and launching predetermined remediation measures within milliseconds.

PFP uses AC, DC or EMI data and can operate air-gapped from the IoT device using an external sensor. Also can be embedded inside IoT devices. To enable PFP, one must generate a baseline from a known good sample. Using machine learning, the analytics engine creates clusters with various feature sets which show the distribution of normal behavior of hardware and software.

In embedded PFP deployment, an IoT device digitizes the power consumption signals, extracts time and frequency features, compares with respect to the baseline to detect anomalies and remediates when dictated by a policy. Many ARM-based SoC already have the necessary modules for embedding PFP, such as an Analog to Digital Converter (ADC) on chip. PFP could be added as firmware. An external amplifier may be needed to boost the power signal. The PFP method could be applied to deliver millisecond detection and remediation. For low-power, less time-sensitive applications PFP monitoring can be scaled down to one scan a day or a week.

Compare with the typical cybersecurity solutions, the PFP solution is unique in the following ways: machine time response and remediation, could be air gapped or embedded, no need for threat intelligence, detect hardware and firmware attacks, detect counterfeits, detect malicious firmware, hackers could not know, could cost pennies.

The authors will discuss how this technique has been implemented in IoT devices to achieve cyber protection for resource-limited IoT devices. A variety of classification and anomaly detection approaches will be reviewed. Implementation factors and design in ARM-based FPGA (Field Programmable Gate Array) architecture will be illustrated. Additionally, PFP techniques will be described and results from our DARPA program focused on IoT and artificial intelligence will be highlighted.

09.28.17

CyberSci 2017 Symposium

Speakers' Bios

#CyberSci2017

icf.com/cybersci

Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

ICF

Sam Visner
8:45 a.m. - 9:00 a.m.

Samuel Sanders Visner is the Senior Vice President, Cybersecurity and Resilience, ICF. Sam also serves as member of the Cyber and Domestic Security Councils of the Intelligence and National Security Alliance and is an adjunct professor of Science and Technology in International Affairs at Georgetown University, where he teaches a course on cybersecurity policy, operations, and technology. Sam is also a member of the Council on Foreign Relations, an Intelligence Associate of the National Intelligence Council, and a member of the Intelligence Science and Technology Experts Group, sponsored by the National Academy of Science and serving the Office of the Director of National Intelligence.

Aaron Gregg (Moderator)
9:45 a.m. -10:45 a.m.

Aaron Gregg covers the Washington-area economy and defense contractors for Capital Business, the Post's local business section. He studied music (Jazz guitar) and political science at Emory University in Atlanta and has a graduate degree in public policy from Georgetown.

Larry Pfeiffer (Keynote)
9:00 a.m. - 9:45 a.m.

Larry Pfeiffer is a former Senior Director of the Obama Administration White House Situation Room and former Chief of Staff to then-CIA Director Michael Hayden. Currently a Senior Advisor at The Chertoff Group, Mr. Pfeiffer advises the firm's clientele on the current risk environment while helping them better understand the policy and program impacts arising from today's threat vectors. He is a highly respected and recognized expert in the areas of national and homeland security policy, crisis management, secure networked communications, intelligence strategy, analysis and collection, overt and covert operations, and budgetary matters. Mr. Pfeiffer is also a public speaker represented by Leading Authorities, Inc., most recently appearing as the lunch keynote speaker at the US Travel Association's Security Summit in New York this past spring.

Robert Knake (Panelist)
9:45 a.m. - 10:45 a.m.

Rob Knake is a Senior Advisor at Versive, a predictive analytics company. Rob advises Versive on the development of their security applications, which allow companies to detect Advanced Persistent Threats by analyzing the billions of interactions that occur on their networks each day.

Prior to joining Versive, Rob served from 2011 to 2015 as Director for Cybersecurity Policy at the National Security Council at the White House. In this role, he was responsible for the development of presidential policy on cybersecurity, and built and managed federal processes for cyber incident response and vulnerability management.

Before joining government, Rob was an International Affairs Fellow-in-Residence at the Council on Foreign Relations and a cybersecurity consultant. Rob is also an Adjunct Lecturer at Georgetown University's McCourt School of Public Policy and a Senior Fellow at the Council on Foreign Relations. He holds a Master's in Public Policy from Harvard's Kennedy School of Government and undergraduate degrees in history and government from Connecticut College.

Vinh Nguyen (Panelist)
9:45 a.m. - 10:45 a.m.

Mr. Nguyen leads the Intelligence Community mid- and long-term strategic analysis to support and advance the cyber mission. He serves as the subject matter expert and advises the Director of National Intelligence (DNI) on cyber issues in support of the DNI's role as the principal intelligence adviser to the President.

Recruited by NSA through the Stokes Program, Mr. Nguyen received the dual degrees in psychology and computer science from the University of Pennsylvania. He earned his MA in International Science and Technology Policy at the George Washington University's Elliott School of International Affairs, where he focused his work on defense innovation policies and processes. He was trained on positive executive leadership at the University of Michigan's Ross School of Business.

Hank Kenchington (Panelist) 9:45 a.m. - 10:45 a.m.

Hank Kenchington currently serves as Deputy Assistant Secretary (DAS) for Cybersecurity and Emerging Threats R&D in the Department of Energy's Office of Electricity Delivery and Energy Reliability (OE). Hank leads OE's efforts in the research and development of advanced technologies to reduce the risk of energy disruptions due to cyber and emerging threats to the nation's energy infrastructure. From 2009 to 2015, Hank directed the $3.4 billion Smart Grid Investment Grant program funded under the American Recovery and Reinvestment Act of 2009 to upgrade the nation's power grid with advanced digital technologies to improve system reliability, security, and efficiency. From 2009 to 2013, Hank also served as DAS for R&D with responsibility for development of advanced technologies in power electronics, energy storage, cyber security, smart grid, modeling and visualization, and synchrophasor technologies. Hank has a BS in mechanical and nuclear engineering from Virginia Polytechnic Institute and a master's degree in engineering administration from the George Washington University.

Dr. Alexander Kott 11:00 a.m. - 11:30 a.m.

Dr. Alexander Kott serves as the Chief, Network Science Division, Army Research Laboratory headquartered in Adelphi MD. 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 (DARPA) Program Manager responsible for a number of large-scale advanced technology research programs. His earlier positions included Director of R&D at Carnegie Group, Pittsburgh, PA; and IT Research Department Manager at AlliedSignal, Inc., Morristown, NJ. 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, Pittsburgh PA in 1989; published over 80 technical papers; and co-authored, and edited nine technical books.

Technical Presentation Speakers

Craig Roberts 12:30 p.m. - 1:00 p.m.

Craig Roberts serves as the Engineering Manager for the Cyber & Information Services Business Unit within Northrop Grumman's Technology Services sector. He and his team provide thought leadership to introduce innovations to current programs and demonstrate the depth and breadth of corporate capabilities to prospective customers. The scope extends beyond cybersecurity to include areas such as enterprise services, infrastructure support, system engineering, and modeling and simulation. The team is leveraged to support Business Development, Capture & Proposal efforts, Research & Development, and high-level engineering needs on programs across the organization. Prior roles include leadership positions on programs supporting the Department of Homeland Security, Department of State, and the US Army. With over 20 years at Northrop Grumman Mr. Roberts has held a variety of technical, management and Business Development positions delivering mission-critical services and solutions to Government customers.

Mr. Roberts earned a Bachelor's degree as well as a Master's in Technology Management from the University of Maryland.

Jennifer Fabius 12:30 p.m. - 1:00 p.m.

Jennifer Fabius is the IT Risk Director at Freddie Mac. In this role, Jenn is responsible for ensuring the consistent and logical application of the IT division's I&T Risk Framework. She is an accomplished senior risk management leader who has advised national security leaders in areas of policy, technology, and security strategy over the last 15 years. Prior to joining Freddie Mac, Jenn served as a senior risk adviser to intelligence and defense CIOs who spearheaded a U.S. government-wide security transformation initiative. The initiative resulted in a unified information security framework across the federal government. She also led the development and rollout of cyber risk management initiatives enabling the integration of IT and cyber considerations into broader organizational and enterprise risk management programs. Jenn is co-author of several NIST (National Institute of Standards and Technology) Special Publications, and she holds certifications in CISSP (Certified Information System Security Professional) and CRISC (Certified in Risk and Information Systems Control).

Jason Schaum 12:30 p.m. - 1:00 p.m.

Jason Schaum is a Cybersecurity Sr. Program Director with ICF, with over 15 years of experience in Cybersecurity, Information Technology, and Project Management for the private sector and U.S federal government. Mr. Schaum is currently responsible for managing ICFs contract with the Army Research Laboratory, which includes basic and applied cyber defense research, systems and network engineering, risk management, and a 24x7 Cybersecurity Service Operation. Mr. Schaum holds a Bachelors in Management Information Systems and maintains PMP, CCSP, CISSP, CISM, CEH, Security+, Network+ and A+ industry certifications.

Robert Mitchell 12:30 p.m. – 1:00 p.m.

Robert Mitchell is currently a member of technical staff at Sandia National Laboratories. He received the Ph.D, M.S. and B.S. from Virginia Tech. Robert served as a military officer for six years and has over 12 years of industry experience, having worked previously at Boeing, BAE Systems, Raytheon and Nokia. His research interests include game theory, linkography, moving target defense, computer network operations, network security, intrusion detection and cyber physical systems. Robert has published 20 peer reviewed articles.

Gregory Shearer 12:30 p.m. – 1:00 p.m.

Gregory Shearer has been a developer with ICF for 3 years, focusing on challenges in the cybersecurity domain, in particular the application of machine learning techniques to security analytics. Shearer holds a B.S. in Information Assurance Engineering, as well as CSSLP and Security+ certifications.

Dr. Susan Conrad 12:30 p.m. – 1:00 p.m.

Dr. Susan Conrad is an Assistant Professor of Cybersecurity and Information Technology at Marymount University. Prior to joining academia, she was employed at Siemens for 13 years as a senior manager for ERP consulting. She has worked as a fellow for an intelligence agency, a CIO for a hospital in South Carolina, a project manager with start-up healthcare data collection company on the west coast and a consultant for Accenture. She currently focuses her research on social engineering, teenage hacking and cyber awareness. She has a Ph.D. from George Mason; an MBA from Kansas State and a BA from the University of Wisconsin.

Daniel Broder 12:30 p.m. – 1:00 p.m.

Daniel Broder (Class of 2018) is currently enrolled in the M.S. Cyber Security program at Marymount University. He currently works for SE Solutions, Inc. where he supports the mission of the federal government in a variety of capacities.

Robert Filar 12:30 p.m. – 1:00 p.m.

Bobby Filar is a Senior Data Scientist working on intelligent assistants and malware classification at Endgame. Prior to joining Endgame, Bobby worked on various natural language understanding problems, including inference, entity extraction and topic modeling at a research nonprofit. Bobby has given talks at several security and machine learning conferences on topics ranging from adversarial networks to conversational interfaces.

Dr. Zhiping Wang 1:05 p.m. – 1:35 p.m.

Zhiping (Ping) Wang received his M.S. in operations research from Columbia University and Ph.D. in operations research and statistics from The Johns Hopkins University. Ping has worked in IT field for over 20 years in both commercial industry and government agencies, such as AT&T, MCI, EDS and U.S. Department of Education.

Zhiping Wang is a Principal at W Analytic, a consulting company helping other business in data analysis, especially in big-data analysis.

Matthew Joseff

1:05 p.m. – 1:35 p.m.

At an early age, Matthew had a passion for computers and game theory; he started out setting up computers at trade shows and managed an ISP while at university.

As the dependent of two government intelligence officers, Matthew was raised in several countries, including Japan and Italy, and later applied his real-world knowledge to his passion. With over three decades of substantial experience Matthew was a critical part of maturing several startups and integrating cutting edge technology with real world productivity.

Proficient in several languages, Matthew is also the youngest candidate to ever run for Governor of Louisiana, a former National Guardsman, and a former elected member of his town's Economic Development Commission.

Jason Ellis

1:05 p.m. – 1:35 p.m.

Jason Ellis is a research software developer with ICF contracted to the U.S. Army Research Laboratory (ARL). He obtained his Master's Degree in Computer Science with a concentration in Cybersecurity from Johns Hopkins University, and a B.A. in Mathematics and Computer Science from Gettysburg College. His interests are currently centered around the development of novel network traffic collection and representation formats that enhance the intrusion detection process.

Jo Lee Loveland and John Link

1:05 p.m. – 1:35 p.m.

John and Jo Lee are masters of the "human stuff," providing organizational management, communications and strategic consulting to corporate, government (DOD and IC) and non-profit clients. Jo Lee was for several years Visiting Scientist at Software Engineering Institute working with CMMI, Risk Management and Managing Technology Change at NRO, Warner-Robins AFB, and other agencies. John has worked for Army Chief of Staff for Installation Management CIO.

Both were Senior Members 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. They have worked with Johnson & Johnson, ARINC and George Mason University. They are co-designers/presenters for Chaos, Inc.™, an original experiential laboratory and seminar.

Adam Lipinski

1:40 p.m. – 2:10 p.m.

Adam Lipinski is the President of Palm Solutions. His background is in law and economics. He has over 20 years of experience advising federal clients on systems acquisitions, treaty compliance, and economic analysis. Recently, Adam has been involved in cybersecurity acquisitions for the Department of Homeland Security, the Department of Energy, and the Department of Commerce.

Sidney Smith

1:40 p.m. – 2:10 p.m.

Mr. Smith graduated from Towson State University with a Bachelor's Degree in Computer Science in January of 1990. In 2013 he earned his Master's in Computer Science at Towson University (TU). He is current working on his doctorate at TU. He began his career in Information Assurance in April of 1990 when he was hired by the U.S. Army as a Systems Administrator. Since that time he has served as an Information Systems Security Officer, Information Assurance Security Officer, an Information Assurance Network Manager, and an Information Assurance Program Manager. In addition he has served as an Agent of the Certification Authority, and Privacy Officer. In January 2010 he was hired as the Team Leader for the Army Research Laboratory Product Integration and Test Team. He has been a Certified Information System Security Professional since 2006, certified in the National Security Agency INFOSEC Assessment Methodology and INFOSEC Evaluation Methodology since 2006, Security+ Certified since 2008, a Certified Authorization Professional since 2008, and a Certified Information Systems Auditor since 2010.

Dr. Chen Liu 1:40 p.m. – 2:10 p.m.

Dr. Liu currently is an assistant professor in the Department of Electrical and Computer Engineering at Clarkson University, Potsdam, New York. He received his B. E. in Electronics and Information Engineering in 2000 from University of Science and Technology of China (USTC), M. S. in Electrical Engineering in 2002 from University of California, Riverside (UCR), and Ph. D. in Electrical and Computer Engineering in 2008 from University of California, Irvine (UCI), respectively. From 2008 to 2012, Dr. Liu was an assistant professor in the Department of Electrical and Computer Engineering at Florida International University (FIU). Dr. Liu is a member of IEEE, IEEE Computer Society, ACM, ACM SIGARCH, ACM SIGMICRO, and ASEE.

Dr. James Robertson 1:40 p.m. – 2:10 p.m.

Dr. Robertson has over twenty-five years of technical, engineering, and information systems experience with progressively increasing responsibilities in the areas of software security, data analysis, software and database design and development, and modeling and simulation. He has over fifteen years of experience managing, teaching and designing courses within the computer science and software development and security programs for the University of Maryland University College. Dr. Robertson also serves as a software and cybersecurity consultant for the Sensors and Electron Devices Directorate at the Army Research Laboratory.

Dr. Jim Greer 2:15 p.m. – 2:45 p.m.

Colonel (Ret) Jim Greer is the Abrams Learning and Information Systems (ALIS) Vice President for Strategic Leadership and Design. A former cavalry officer, he has commanded at all levels from platoon through Brigade. He has concept development experience, for Force XXI, Army After Next and Army Transformation and OSD-Net assessment 20XX Wargame Series. He is a former Director of the Army School of Advanced Military Studies (SAMS). Jim has supported strategic and operational planning, concept development (including the current Army Operating Concept). He has led research at Army Research Institute (ARI) on Integrated Planning Systems and Visualization of Complex Problems. Jim has designed, developed and delivered instruction in leadership, strategic foresight, and operational planning. Dr. Greer has a Doctorate in Education, Masters Degrees in Education, National Security and Strategic Planning from the School of Advanced Military Studies.

Hasan Cam 2:15 p.m. – 2:45 p.m.

Hasan Cam received the Ph.D. degree in electrical and computer engineering from Purdue University in 1992, and the M.S. degree in computer science from Polytechnic University, New York, in 1986. He is a Computer Scientist at US Army Research Laboratory. He currently works on the projects involved with assessment and management of cyber vulnerability, risk, resilience, agility, mission assurance, active malware defense over wired, mobile, and tactical networks. His research interests include cyber security, machine learning, data analytics, networks, algorithms, and parallel processing. He serves as the government lead for the Risk area in Cyber Collaborative Research Alliance. He has previously worked as a faculty member in the academia and a senior research scientist in the industry. He has served as an editorial member of two journals, a guest editor of two special issues of journals, an organizer of symposiums and workshops, and a Technical Program Committee Member in numerous conferences. He is a Senior Member of IEEE.

Steven Chen 2:15 p.m. – 2:45 p.m.

Steven Chen is a serial entrepreneur, investor, and mentor. He is the co-founder and CEO of PFP Cybersecurity (aka Power Fingerprinting, Inc.), an IoT security platform company with patented power analytics. Steven is the Chairman of the Cyber Security Investment Committee with Blu Ventures, with 14 cybersecurity portfolio companies. He serves as a Director of the Board of ThreatQuotient, a Threat Intelligence Platform (TIP) company, a star mentor of MACH37 and an advisor of AlphaTec. He chairs the IEEE Std 1451.5 Wireless Smart Sensor Networks Working Group.

Steven Chen is the Founder & Former CEO of 3eTI, a secure wireless company and an Intel Capital portfolio company, enhanced the security of Intel Centrino, received certificate #1 of Common Criteria for Wi-Fi. Mr. Chen oversaw the favorable exit of 3eTI to EF Johnson, a $200M public company. After the sale of 3eTI to EFJ, Mr. Chen served as CTO and VP of Corporate Development. He went on to found Totus Solutions and serve as their CEO and joined Blu Ventures as a partner. He received a BSEE from Tamkang University in Taiwan and MSEE from SUNY Buffalo.

Frank Cilluffo (GWU Panel Moderator) 3:00 p.m. – 3:45 p.m.

Frank J. Cilluffo is an Associate Vice President at The George Washington University where he leads a number of national security and cybersecurity policy and research initiatives. Cilluffo directs the Center for Cyber and Homeland Security and, along with the School of Business, launched the university's World Executive MBA in Cybersecurity program.

In addition to briefing Congressional committees and their staffs, he has publicly testified before Congress on numerous occasions, serving as a subject matter expert on policies related to counterterrorism, cyber threats, security and deterrence, weapons proliferation, organized crime, intelligence and threat assessments, emergency management, and border and transportation security. Similarly, he works with U.S. allies and organizations such as NATO and Europol. He has presented at a number of bi-lateral and multi-lateral summits on cybersecurity and countering Islamist terrorism, including the UN Security Council.

Prior to joining GW, Cilluffo served as Special Assistant to the President for Homeland Security. Immediately following the September 11, 2001 terrorist attacks, Cilluffo was appointed by President George W. Bush to the newly created Office of Homeland Security. During his tenure at The White House, he was involved in a wide range of counterterrorism and homeland security strategy and policy initiatives, served as a principal advisor to Governor Tom Ridge, and directed the President's Homeland Security Advisory Council.

Geoff Hancock (Panelist) 3:00 p.m. – 3:45 p.m.

Geoff Hancock is the CEO at the Advanced Cybersecurity Group. He leads the organization in the development of cybersecurity best practice for commercial and federal customers. Hancock has spent 25 years in cybersecurity. His experience includes active defense, intelligence, conducting red/blue team operations, managing investigations and developing threat modeling programs across Department of Defense, Intel Community, civilian agencies and corporations. He serves on several federal/commercial task forces advising on operations, active defense and cyber-deterrence. He currently serves as a Sr. Fellow at the George Washington Center for Cybersecurity, Chairman of the Federal CIO/CISO Alliance and is Co-Chair of the Cyber Intelligence Task Force at INSA.

Jeff Greene (Panelist) 3:00 p.m. – 3:45 p.m.

Jeff Greene is the Senior Director, Global Government Affairs & Policy at Symantec, where he leads a global team of policy professionals who focus on cybersecurity, data integrity and privacy issues. Prior to joining Symantec, Jeff was Senior Counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where he focused on cybersecurity and homeland defense issues. He also worked as a Subcommittee Staff Director with the House Committee on Homeland Security, Counsel to the Senate's Special Investigation into Hurricane Katrina, and as an attorney with a Washington, D.C. law firm. Jeff is a member of the National Institute of Standards and Technology's Internet Security and Privacy Advisory Board (ISPAB), and worked as a guest researcher supported the President's Commission on Enhancing National Cybersecurity. He recently served as the staff co-chair of the "Internet of Things" research subcommittee of the President's National Security Telecommunications Advisory Committee and is a Senior Fellow at The George Washington

University Center for Cyber and Homeland Security. He speaks often on cybersecurity, the "Internet of Things," data breach, and privacy issues. He has a B.A. in International Relations from Boston University and a J.D. with Honor from the University of Maryland, where he has taught classes in Homeland Security law and policy.

Jim Lutz (Panelist) 3:00 p.m. – 3:45 p.m.

Mr. Lutz brings over sixteen years of experience in system validation, cybersecurity vulnerability assessment, penetration testing, secure software development, Computer Network Defense (CND), Certification and Accreditation (C&A), Information Assurance (IA) and Information Technology (IT). Lutz leads RMC's Cyber Operations group which supports all aspects of validation and vulnerability assessments, secure software development, CND, C&A, cybersecurity, network operations, and Incident Response. Mr. Lutz has extensive experience with integrating Information Assurance practices into the Software Development Lifecycle for large-scale applications and systems and has managed 24x7 Security Operations Center's with intrusion detection and prevention, incident response, and perimeter defense capabilities. Lutz's experience includes implementation of DIACAP/Risk Management Framework processes, risk management and mitigation plans, policy development, and enforcement of Government and DoD Cybersecurity requirements.

RMC's Cyber Operations group has grown significantly under Mr. Lutz's leadership. Lutz and his team perform pre-DISA Command Cyber Readiness Inspections (CCRI) and USMC Cyber Security site assessments. The Cyber Operations team performs vulnerability assessments and system security engineering for new systems and applications prior to placing them on the Marine Corps Enterprise Network. His management of the cyber team includes assessment and review of Configuration Management plans, Quality Assurance plans, user manuals, and Information System Security Plans and COOP/disaster recovery plans. Lutz was awarded the designation of United States Marine Corps Approved Validator by HQMC C4 DAA.

Dr. Misty Blowers 3:45 p.m. - 4:45 p.m.

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

Dr. Douglas Maughan (Panelist) 3:45 p.m. - 4:45 p.m.

Dr. Douglas Maughan is the Division Director of the Cyber Security Division in the Homeland Security Advanced Research Projects Agency (HSARPA) within the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS). Dr. Maughan has been at DHS since October 2003 and is directing and managing the Cyber Security Research and Development activities and staff at DHS S&T. 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 over 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 (DARPA). Prior to his appointment at DARPA, Dr. Maughan worked for the National Security Agency (NSA) as a senior computer scientist and led several research teams performing network security research.

Mike Fanto (Panelist) 3:45 p.m. - 4:45 p.m.

Michael Fanto, Research Scientist at the Air Force Research Laboratory and Microsystems Engineering Ph.D. Student at Rochester Institute of Technology.

Mike received his B.S. degree in Physics from Utica College of Syracuse University in 2002. His current research areas are single/entangled photon generation and integrated photonics as applied to quantum information science.

Roger Guseman (Panelist) 3:45 p.m. - 4:45 p.m.

Mr. Guseman is a 1983 Graduate of the United States Naval Academy with a Bachelor of Science degree in Chemistry. He served 20 years in the Navy as a Nuclear Trained Submarine Officer.

Mr. Guseman finished his Navy career as a Division Chief in the Defensive Information Operations Directorate at the National Security Agency.

Following his career in the Navy, Mr. Guseman worked at Northrop Grumman Electronics Systems for 13 years as a Director/Senior Programs Manager in the Advanced Concepts and Technology Division. His innovation and entrepreneurial expertise lead his teams to achieve significant advances in technology growth for many classified programs.

Dr. Venkateswara Desari (Panelist) 3:45 p.m. - 4:45 p.m.

Venkat R. Dasari, Ph.D., is a scientist at the Computational Science Division, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD. Previously, he worked both in the Government and private sectors in development of programmable network protocols and architectures. He has advanced degrees in Biology and Computer Sciences. His current interests are focused on programmable adaptive computing abstractions, algorithms, distributed computational Intelligence and quantum network applications.

James Sidoran (Keynote) 4:45 p.m. – 5:15 p.m.

James Sidoran is a Senior Scientist with US Air Force Research Lab, Information Directorate in Rome, NY. His technical interests include formal methods, analysis and specification techniques, and modeling complex system behavior. Over the years, he's earned an M.S. in Computer Science and an M.B.A. from Syracuse University, directed a number technical programs in AFRL's cyberspace portfolio, and served as technical consultant and program management support to DARPA, IARPA and DHS, totaling over $250M. James has spoken and published at numerous conferences, including technical reports, and has owned an independent technical consultant business providing software and system services to organizations in the health and insurance industries. In his role of senior strategist, and innovation and technology transition specialist, he serves as strategic advisor to Pacific Air Force (PACAF) and US Pacific Command (PACOM).

James has been active in the international S&T community for over 15 years including Singapore, European Office of Aerospace R&D, as well as with numerous NATO bodies and national cyber security experts. Most recently, James is chairing an international research team on modeling techniques for mission assurance and risk assessment that is addressing security challenges for multi-domain unmanned and autonomous systems.

James Clapper (Keynote) 5:15 p.m. – 5:45 p.m.

The Honorable James R. Clapper served as the fourth U.S. Director of National Intelligence (DNI) from August 9, 2010 to January 20, 2017. In this position, Mr. Clapper led the United States Intelligence Community and served as the principal intelligence advisor to President Barack Obama.

Mr. Clapper retired in 1995 after a distinguished career in the U.S. Armed Forces. His career began in 1961 when he enlisted in the U.S. Marine Corps Reserve and culminated as a lieutenant general in the U.S. Air Force and Director of the Defense Intelligence Agency. His intelligence-related positions over his 32 years in uniform included Assistant Chief of Staff for Intelligence at Headquarters, U.S. Air Force during Operations Desert Shield/Desert Storm, and Director of Intelligence for three combatant commands: U.S. Forces, Korea; Pacific Command; and Strategic Air Command. He served two combat tours during the Southeast Asia conflict, and flew 73 combat support missions in EC-47's over Laos and Cambodia.

Following his retirement, Mr. Clapper worked in industry for six years as an executive in three successive companies with the Intelligence Community as his business focus. He also served as a consultant and advisor to Congress and to the Departments of Defense and Energy, and as a member of a variety of government panels, boards, commissions, and advisory groups. He was a senior member of the Downing Assessment Task Force which investigated the Khobar Towers bombing in 1996, was vice chairman of a commission chaired by former Governor Jim Gilmore of Virginia on the subject of homeland security, and served on the NSA Advisory Board.

Mr. Clapper returned to the government two days after 9/11 as the first civilian director of the National Imagery and Mapping Agency (NIMA). He served in this capacity for almost five years, transforming it into the National Geospatial-Intelligence Agency (NGA) as it is known today. Prior to becoming the Director of National Intelligence, Mr. Clapper served for over three years in two Administrations as the Under Secretary of Defense for Intelligence, where he served as the principal staff assistant and advisor to the Secretary and Deputy Secretary on intelligence, counterintelligence, and security matters for the Department. In this capacity, he was also dual-hatted as the Director of Defense Intelligence for the DNI.

Poster presenters:

Lori Gordon

6:00 p.m. - 7:00 p.m.

Lori Gordon is Senior Strategist and Lead for Infrastructure Protection Security and Resilience at HWC. She brings more than 18 years of experience with federal, state, and local governments, including the U.S. Departments of Homeland Security and Energy, and non-profits. Ms. Gordon oversees consulting service delivery and performance in strategy development, program design, process improvement, human capital, transformation, and outreach initiatives, advising clients in homeland security, cyber and physical security, emergency management, and public health missions.

Ms. Gordon is also Director of the Women in Homeland Security (WHS) Science, Technology, Engineering, and Math (STEM) program, and is coordinator for Infragard National Capital Region's (NCR) CyberCamp programming. She serves on the Montgomery County Curriculum Advisory Board for Information Technology and Cybersecurity, and the Montgomery County Program Advisory Committee for Law, Government, and Public Safety. She is an advisor to the International Organization for Standardization (ISO) Technical Advisory Group on TC 268 Sustainable Development in Communities, the National Institute for Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Working Group on Cyber Workforce Management, and the NIST's NICE Working Group on K-12 Cyber Education. Ms. Gordon holds a Masters in Public Administration from the University of Massachusetts, Amherst.

George McAleese 6:00 p.m. - 7:00 p.m.

George McAleese is an Associate at HWC who focuses on homeland security and emergency management consulting. He provides strategy, risk assessment, research, and analytics consulting support for clients. He has provided research and communications support for political campaigns across the US and in 7 countries, as well as working for a city prosecutor's office. Mr. McAleese also serves as an advisor to the ISO Technical Advisory Group on Sustainable Development in Communities and is a member of the Board of Directors of the Washington, DC Chapter of the American Constitution Society. He earned his Juris Doctor at Hofstra University and a Masters degree in Political Management from George Washington University.

Dr. Okon Akpan 6:00 p.m. - 7:00 p.m.

Okon H. Akpan holds Ph.D. and Ms. degrees in Computer Science and MS. degree in Chemical Engineering. He had been a university professor for over seventeen years teaching mainly at the graduate level, conducting research and making a number of publications (including books) on diverse topics in both computer science and engineering. His expertise is High Performance Computing. Recently, Dr. Akpan has also been interested in application of modern data mining tools to harvest understanding from large network data as well as application or adaptation of machine learning techniques to support Kelly Compression research presently carried out at the Army Cyber-research Analytics Laboratory (ACAL).

Dr. Vojislav Stojkovic 6:00 p.m. - 7:00 p.m.

Vojislav Stojkovic earned Ph.D. (1981), MS (1977), and BS (1972) from University of Belgrade, Belgrade, Serbia. He served as an assistant/associate professor of computer science at University of Belgrade (1982-1988), University of Novi Sad (1981-1988), San Diego State University (1988-1989), Bowie State University (1992), University of Maryland University College (1996), and Morgan State University (1989 - present). He is currently the associate professor of computer science at the Morgan State University, Computer Science Department, Baltimore, Maryland. His research areas are programming languages, automata, formal languages, language processors, bio, parallel and distributed, DNA, and quantum computing, artificial intelligence, and cybersecurity. He published more than 85 scientific and professional papers.

Matthew Monte 6:00 p.m. - 7:00 p.m.

Matthew Monte is an executive leader with an extensive background in computer security and software engineering. Across leadership positions, he has set and implemented the strategic direction of core computer security business areas and helped build and expand several small companies.

Mr. Monte began his career at the Central Intelligence Agency as an engineer and a technical operations officer. His experience in operational environments around the world helped shape his views on mission focus, management, and the rapid development of solutions. Mr. Monte is author of the book Network Attacks and Exploitation: A Framework (Wiley 2015). The idea for the book began with a naval observation. It takes 7 years to build an aircraft carrier. It takes 20+ years to "build" a captain capable of commanding it and generations to develop and refine the doctrine required to train that captain. Doctrine matters and it is lacking. There are no guiding principles for targeted computer espionage and therefore little structured thought as to how they are countered. The book establishes and details the strategic and tactical principles for the field. He is currently working for Kudu Dynamics, a small software company, performing duties as required in a startup environment including business development, customer marketing and management, small team oversight, and software design and development.

Dick Astrom 6:00 p.m. - 7:00 p.m.

Dick Astrom, currently a Senior Telecommunications Analyst at ICF, is a lifelong computer scientist, with a BS in Math from the University of Michigan and an MS in Information Sciences from the University of Chicago. He developed software and system studies for telecommunication systems at Bell Laboratories and Motorola; and he developed signal processing and control software for military systems at Raytheon, Argon ST, and Sparta. He performed and supported research in cyber defense, specializing in network intrusion detection, at the Army Research Laboratory and in the Cyber Lab at ICF.

In his current work in telecommunications, Mr. Astrom analyzes telecommunication networks and systems for concentration points and potential vulnerabilities, as part of the Defense Critical Infrastructure Protection (DCIP) program for the US Navy. Included in this analysis is consideration of cyber security practices related to telecommunications infrastructure in various European countries, giving Mr. Astrom an overview of European cyber defenses and the organizations involved.

Paris Stone 6:00 p.m. - 7:00 p.m.

Paris Stone is currently a Senior Systems Engineer at vArmour Networks for the Federal, Mid-Atlantic and Canada territories. Paris is the Former Novell, Microsoft and Cisco Certified Trainer and is an Open Source Enthusiast and Technologist. Previous work includes over 25 years of Network Security Engineer & Architect experience and 10 years of experience on an Infrastructure Security Engineering Team Lead for a top 5 US Bank.

CyberSci 2017

icf.com/cybersci

#CyberSci2017

About ICF

ICF is a global consulting services company with over 5,000 specialized experts, but we are not your typical consultants. At ICF, business analysts and policy specialists work together with digital strategists, data scientists and creatives. We combine unmatched industry expertise with cutting-edge engagement capabilities to help organizations solve their most complex challenges. Since 1969, public and private sector clients have worked with ICF to navigate change and shape the future.