Dupont Summit 2014

:::::::::: *Science, Technology, and Environmental Policy Issues*

December 5, 2014 ❖ Historic Whittemore House, Washington, DC

The Policy Studies Organization

Panel
"Exploring Cyberspace: Phishing, Security and Threats"

"The Human Element: The Biggest CyberSecurity Vulnerability in the 21st Century Workplace"
Elliott Lynn – *American Public University*

Information security and protecting critical infrastructure is essential to any organization operating today. Organizations invest millions of dollars on securing enterprise data assets and get a false sense of security when there is little to no protection over the unpredictable "human element" that creates the biggest vulnerabilities and potential losses that can destroy organizations. CCTV, security guards, checkpoints, complex passwords, biometric technology, and more all are vulnerable to the "human element". Background checks with full polygraph for the most secure jobs cannot detect or anticipate erratic human behavior. There are many thoughts and ideas on how to combat the "human element" but avoidable security breaches continue to plague organizations. The Human Element: The Biggest Cyber Security Vulnerability in the 21st Century Workplace will highlight vulnerabilities that continue to be overlooked by organizations and arm participants with an increased knowledge on how to minimize exposure to avoidable attacks consistent with the human element that plagues every organization.

Panel
"Exploring Cyberspace: Phishing, Security and Threats"

Biography
Elliott Lynn – *American Public University*

Elliott Lynn has over 20 years of professional experience in the Information Security and Technology field, with more than 16 of those years leading and supervising various types of information technology related projects and staff. He served over 10 years as the Director of Information Technology for a multinational aeronautical manufacturing firm, before transitioning as the Team lead of the Biometrics Data Team for the Department of Defense, and an Assistant Division Director for the New Jersey Office of Information Technology before settling in to my current position as Full Time Faculty for American Public University for ISSC graduate level programs. In all three of those executive positions, his management of information technology was critical and effective to the success of the organizations in which he served. He has the unique characteristic of having Information Management experience in Private Industry, Federal, and State Government organizations. He also possess a Level III Defense Acquisition Certification in Information Technology Management, which is the highest attainable certification (and requirement for all Senior Executive Service staff) awarded by the US ARMY.

His educational background includes a Ph.D. in Organization and Management with a specialization in Information Technology as well as a Master of Business Administration with a specialization in Information Technology Management. This allows him to relate to the diverse fields of study while possessing the technical competence needed to make the alignment of business and information security and technology that the workplace demands.

Publications include *Digital Divide or Digital Disinterest* 2014, *The Quality Online Learning Experience (Q.O.L.E)* 2011, and The Importance of IT Project Measurement and Metrics in State Government 2011

Dupont Summit 2014

:::::::::: Science, Technology, and Environmental Policy Issues

December 5, 2014 ❖ Historic Whittemore House, Washington, DC
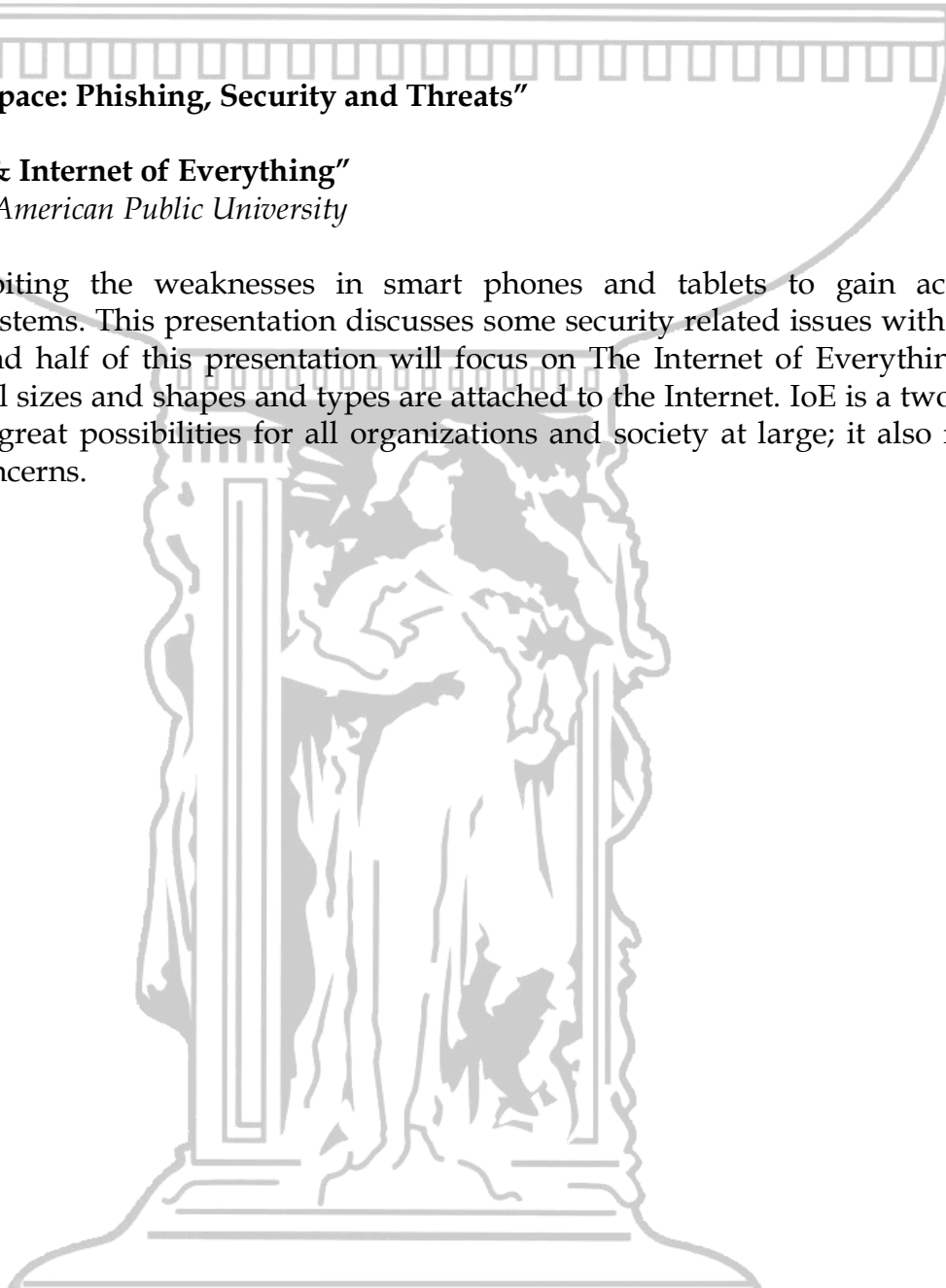
The Policy Studies Organization

Panel
"Exploring Cyberspace: Phishing, Security and Threats"

"Mobile Security & Internet of Everything"
Daniel Benjamin – *American Public University*

Hackers are exploiting the weaknesses in smart phones and tablets to gain access to information and systems. This presentation discusses some security related issues with mobile systems. The second half of this presentation will focus on The Internet of Everything (IoE) where sensors of all sizes and shapes and types are attached to the Internet. IoE is a two-edged sword; it presents great possibilities for all organizations and society at large; it also raises a myriad security concerns.

Panel
"Exploring Cyberspace: Phishing, Security and Threats"

Biography
Daniel Benjamin – *American Public University*

Mr. Benjamin is a graduate of the prestigious Indian Institute of Technology (IIT). He has over twenty years of experience providing Information Technology and Management education and consulting solutions in the public and private sectors. His clients include the White House, the U.S. Senate, the Department of Defense (DoD), the Department of Treasury (DoT), the Federal Aviation Administration (FAA), and the Department of Education DoEd).

Dan is an IT industry influencer; he served on the Executive board of the Federal Information Systems Security Educators Association (FISSEA). He also served on the Executive Committee of the Association of Computing Machinery (ACM) SIG on IT Education (SIGITE). He has also published/presented papers related to Learning Management Systems at the International Association for Computer Information Systems (IACIS) and the Information Systems Educators Conference (ISECON).

As Dean of the School of Science, Technology, Engineering and Math (STEM), Mr. Benjamin directs the administrative, curricular, and teaching aspects of 14 degrees, 30 certificate programs, and over 250 courses in Cybersecurity, Electrical Engineering, Environmental Science, Information Technology, Mathematics, Science, and Space Studies programs. He engages 7 Program Directors, 2 Faculty Directors, and over 400 part-time & full-time faculty to administer and teach over 25,000 student registrations in over 250 courses. He maintains a high level of quality in the curriculum and the classrooms in his school and uses educational technologies to maximize the learn experience. The Higher Learning Commission approved his proposals for undergraduate Information Technology, undergraduate Information Systems Security, and graduate Information Technology degree programs. The concentrations in the graduate program are IT Project Management, Information Assurance and Security, and Digital Forensics.

He authored books on Java and Oracle that were published by Element-K Press (formerly Ziff-Davis) and McGraw-Hill/ Oracle Press. He made many winning presentations that have resulted in multi-million dollar contract awards. He developed IT curriculum for three universities using multi-tiered Learning Outcomes Assessment (LOA) Architectures.

He established successful Information Technology, Business Process Reengineering, Technology, and Educational practices at various companies. Many of his practices were cited for excellence. His practices and contract awards realized over 25 Million dollars in revenues. His various roles included Vice-President, Chief Academic Officer (CAO), and Chief Technology Officer (CTO); he is currently Vice-President and Dean of the School of Science, Technology, Engineering and Math at APUS.

He facilitated various management and Joint Application Design (JAD) workshops. He is a certified F.A.S.T. Facilitator and a certified Project Management Professional (PMP). He is also an excellent instructor and uses humor effectively to communicate the principles of developing Information Technology and Management solutions.

Dupont Summit 2014

::::::::: *Science, Technology, and Environmental Policy Issues*

December 5, 2014 ❖ Historic Whittemore House, Washington, DC

The Policy Studies Organization

Panel
"Exploring Cyberspace: Phishing, Security and Threats"

"How Do Cyber Weapons Affect Strategic Stability?"
Clay Wilson – *American Public University*

I propose the research the following questions for my presentation at the DuPont Summit conference scheduled for December 2014. What are Characteristics of Cyber Weapons? How are cyber weapons related to Meta-Data and Intelligence gathering? Are we entering a time for a new, global Cyber-Arms race? How does the proliferation of cyber weapons affect Strategic Stability and the global balance of power?

Methods for international conflict have changed. Cyber weapons will be a part of all future international conflicts, both military and economic, and the identity and intent of cyber threat actors is usually not clear initially to the nation-state that is the target of a cyberattack. The essential components of cyber weapons are Zero-Day Exploits (ZDEs), and these are now bought, openly or secretly, in a global marketplace. However, these cyber weapons can also be sold or shared with extremist groups, which heightens the unpredictability of possible targeting if they are used as part of a cyber weapon.

The countries with the highest dependency on cyber technology are the most vulnerable to the threat due to proliferation of cyber weapons, and that list is most likely topped by the United States.

Several important policy questions emerge as cyber weapons become more widely available to threat actors. These will be discussed as part of the presentation.

Dupont Summit 2014

::::::::: Science, Technology, and Environmental Policy Issues

December 5, 2014 ❖ Historic Whittemore House, Washington, DC

PSO

The Policy Studies Organization

Panel
"Exploring Cyberspace: Phishing, Security and Threats"

Biography
Clay Wilson – *American Public University*

Dr. Clay Wilson is Program Director of Cybersecurity Studies at the American Public University System. The Cybersecurity program emphasizes a multi-disciplinary approach and examines the complexity of cybersecurity management for critical infrastructures. Dr. Wilson was past Program Director of Cybersecurity Policy at the University of Maryland University College. Prior to that, Dr. Wilson was a researcher at the Congressional Research Service where he analyzed cyber intelligence reports for the U.S. Congress and NATO committees on technology topics such as net-centric warfare, cybersecurity, nanotechnology, electromagnetic pulse, and the related vulnerabilities of high-technology military systems and national critical infrastructures.

Dr. Wilson is a member of the Landau Network Centro Volta, International Working Group, an organization that studies non-proliferation of CBRN and Cyber Weapons. He has moderated panels for the National Nuclear Security Administration on nonproliferation for Cyber Weapons in Como, Italy, and has presented at the China Arms Control and Disarmament Association in Beijing. He has also presented at the US Defense Cyber Investigations Training Academy, at the US National Defense University on the topic of cybercrime, and at the Cyber Conflict Studies Association on the cyber capabilities of terrorist groups. Other projects while living abroad in the United Arab Emirates involved research for the Abu Dhabi government on computer security and network technology for defense and crisis management. His PhD from George Mason University concentrated on Protection of Intellectual Property.