CSIA RFI Responses, January 15, 2019

Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan RFI Responses

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities. We bear no responsibility for the accuracy, legality or content of all external links included in this document.

January 14, 2019

The National Coordination Office
Networking and Information Technology Research and Development (NITRD)

Re: RFI Response: Federal Cybersecurity R&D Strategic Plan

Submitted by:
Dr. Eman El-Sheikh, Director, Center for Cybersecurity, UWF
Dr. Tirthankar Ghosh, Associate Director, Center for Cybersecurity, UWF
Mr. Guy Garrett, Assistant Director, Center for Cybersecurity, UWF
Dr. Guillermo Francia, Faculty Scholar, Center for Cybersecurity, UWF
Dr. Greg Hall, Research Scientist, Center for Cybersecurity, UWF

Introduction and context

The University of West Florida (UWF) Center for Cybersecurity is a nationally-recognized leader in cybersecurity education and workforce development. Designated as a Center for Academic Excellence (CAE) in Cyber Defense Education by the NSA and DHS, the Center also serves as the NSA/DHS Cybersecurity Center of Academic Excellence Regional Resource Center for the Southeast U.S. This is a prestigious recognition awarded to only nine higher education institutions nationwide. UWF provides leadership to advance cybersecurity education among colleges and universities in Alabama, Florida, Georgia, Mississippi, Puerto Rico and South Carolina. The Center works with external stakeholders and academic colleges and departments to expand and strengthen UWF's unique multidisciplinary approach to cybersecurity including undergraduate and graduate programs and certificates in cybersecurity, IT/cybersecurity and information security management. In addition, UWF offers the only CAE-designated stand-alone BS in Cybersecurity in the State of Florida. The UWF Center for Cybersecurity was the only higher education institution in Florida to receive NSA/NSF funding to host GenCyber K12 camps for 2017 and 2018.

Following are the Center's response to the NITRD NCO's request for input for the 2019 update of the Federal cybersecurity R&D strategic plan

Response:

What innovative, transformational technologies have the potential to greatly enhance the security, reliability, resiliency, and trustworthiness of the digital infrastructure, and to protect consumer privacy?

Advent of Internet of Things (IoT) has completely transformed our everyday lives as consumers. We have never seen such ubiquity and pervasiveness of computing and communication devices that have inherently integrated with our daily lives. With this ubiquity comes challenges - challenges to make them secure, challenges to make the communications private, and challenges to maintain their reliability and functionality in the face of adversarial actions. Few technologies that have the potential to transform our digital infrastructure, including IoT and Industrial Control Systems (ICS) are:

- Automated continuous security monitoring using Machine Learning technology
- Block chain enabled authentication mechanism
- Intelligent detection of product tampering in the supply chain
- Using Artificial Intelligence (AI) and Machine Learning (ML) to proactively hunt for and respond to threats in the critical infrastructure domain

What areas of research or topics of the 2016 Strategic Plan should continue to be a priority for federally funded research and require continued Federal R&D investments?

All areas of research topics and challenges that were highlighted in the 2016 strategic plan are worth pursuing. some of the topics are more relevant than others in today's context, some of them are highlighted below:

- In addition to Deter, Protect, Defend, and Adapt, a fifth element, namely Counter, should be added to strategize offensive cyber operations. Significant amount of research needs to be done using Machine Learning and Deep Learning to proactively study adversarial behavior, using predictive analytics to stop them from advancing through the Cyber Kill Chain, and taking counter actions to stop them from happening.
- Offensive cyber operations will entitle a multi-disciplinary research approach to solve social, economical, psychological, legal, ethical, and of course technical problems to devise and launch a strategic approach.
- Developing of automated tools for cyber threat forecasting in order to assess the limitations of protective measures was emphasized in 2016. It should be enhanced to developing of automated tools to assess the limitations of counter offensive as well.
- Greater emphasis should be placed on analysis of adversarial behavior using Deep Learning techniques. Psychology of adversaries should be studied in details in the context of various attack motivations in line with Antecedent-Behavior-Consequence model, and Social Trust models.
- Growing emphasis should be given on vehicular security and critical infrastructure security.

What changes to cybersecurity education and workforce development, at all levels of education, should be considered to prepare students, faculty, and the workforce in the next

decade for emerging cybersecurity challenges, such as the implications of artificial intelligence, quantum computing, and the Internet of Things on cybersecurity?

Traditionally, higher education in colleges and universities have been designed using a degree-centred approach. Certain number of courses are packaged together to create a degree program, and students are required to complete all courses to obtain a degree. This student-centred degree-oriented approach, while historically serving a certain body of traditional-age students, is increasingly being proven ineffective in a fast-changing and diverse workforce training scenario. Cybersecurity education, being one of the nation's top workforce development priorities, should follow a more learner-centred competency-oriented approach, where specific scalable learning modules need to be created and delivered to satisfy the increasing demand for skilled workforce.

Competency-oriented modular approach to curriculum design will also help educational institutions to create a seamless pathways for students from high school through 2-year colleges and universities to employment. Moreover, it will also help higher educational institutions to partner with private and public sector companies to offer apprenticeship programs that would cater to working professionals for on the job training, as well as help displaced workers get back to the workforce.

As job demand in Cybersecurity is growing almost every day and organizations are struggling to find skilled workforce, apprenticeship programs should be of significant priority for educational institutions. Historically, colleges and universities in USA have not considered apprenticeship as an option for higher education. Fortunately, they are beginning to understand the value of the training that's being conducted in the apprenticeship program. Over 300 colleges have partnered with employers in the Registered Apprenticeship-College Consortium, a national organization that translates apprenticeship work into college credentials, which can help workers earn associate's or bachelor's degrees. More colleges and universities should start offering college credits for these types of training, and a modular learner-centred curriculum design will help them in achieving this objective.

With the increasing trend with automation and applications of Artificial Intelligence (AI) and Machine Learning (ML), more and more cybersecurity jobs will require higher levels of skills and knowledge. Day-to-day cybersecurity jobs involving operational skills like firewall management and log analysis and parsing will be taken over by sophisticated ML algorithms, creating further demand for high skilled knowledge-based workforce with knowledge of AI/ML, Cloud Computing, and Deep Learning in a distributed cloud-based environment. Universities and colleges should prepare students with these skills and knowledges, and should design apprenticeship programs in conjunction with industry partners to train employees on these sophisticated skills. Traditional view of apprenticeship as a skill-based tradecraft needs to be changed to a more knowledge-based training to cope with the increasing demand of knowledge economy.

In case of any question, please contact:

Dr. Tirthankar Ghosh
Professor and Associate Director
Center for Cybersecurity
University of West Florida
Email: tghosh@uwf.edu