INFRASTRUCTURE: TED TALKS

WEDNESDAY: SESSION 4 TRACK 3

SESSION CHAIRS

- Cherrie Black, Idaho National Laboratory, cherrie.black@inl.gov
- John Hummel, Argonne National Laboratory, jhummel@anl.gov
- Frederic Petit, Argonne National Laboratory, fpetit@anl.gov

SESSION ABSTRACT

CYBER-CHAMP - A Model for Informing and Building a Cybersecurity Resilient Workforce

Shane D. Stailey, Jade Hott, Donaven Haderlie, and Ralph Ley, Idaho National Laboratory

Today's world of interconnected devices, networks, and business and technology systems make it very difficult for an organization to be able to securely design, implement, maintain, and support. For the most part securely provisioning Information Technology (IT) has been a business priority for many organizations over the last 10-20 years. However, what continues to allude proper c-level support and attention are the critical infrastructure systems that provide the backbone and longevity for critical lifeline support. Power, Water, Communications, IT, and Transportation are these critical infrastructure lifeline sectors.

In recent years there has been many highly visible cybersecurity breaches impacting the ability for a business, municipality, states, territory, and/or nation to keep critical infrastructure up and running. Who is responsible for these lifeline infrastructures? How can industry, government, academia, and the science and research communities work together to solve this ever-growing cybersecurity threat? How much is good enough, when it comes to cybersecurity, and how can an organization measure appreciable gains in cybersecurity and create continual plans for improvement? What training and/or competencies must the organizational workforce have to stay ahead of these global security threats? How can ICS Cybersecurity Workforce Development Competency be measured? How can an organization understand how to measure and improve ICS Cybersecurity Operational Readiness? Finally, what type of training and learning paths can an organization deploy to make sure that individual ICS cybersecurity job roles and responsibilities are known and carried out securely? These answers lie in the ICS (Industrial Control Systems) Cybersecurity Competency Health And Maturity Progression (CYBER-CHAMP©) model.

Developing an Explainable Deep Learning Model for Enhanced Critical Infrastructure Analysis

Shiloh Elliott and Ryan Hruska, Idaho National Laboratory

With recent advances in the fields of satellite imagery and machine learning we now have the ability to develop explainable deep learning models that enhance critical infrastructure analysis. Funded through Idaho National Laboratory's (INL) Laboratory Directed Research and Development (LDRD) office we are in the process of developing a deep learning model capable of identifying critical infrastructure facilities and embedded features within those facilities. Utilizing current limit of practice techniques in the machine learning areas of explainability and transfer learning our model, once complete, will have the capacity to be used on multiple different imagery data sets and produce results that not only classify critical infrastructure facilities, but also explain why a critical infrastructure facility was classified as a certain type

of facility. These advancements eliminate the 'black box' approach deep learning models have had in the past, where a user will have to trust the conclusion of a model without understanding what reasoning when into the model's classification process. They also expand a model's usefulness, traditionally a deep learning model will have to use the same data set it was originally trained on. Given the long training times of deep learning models this is impractical in a number of scenarios. By utilizing transfer learning advancements, we are eliminating the need to train our model on the same data set it is then run on to classify critical infrastructure facilities. We are also enabling the analysis and classification of data sets that are potentially too small to be divided into a training and testing data set. Once completed this model can provide a foundation to enhanced critical infrastructure analysis, dependency analysis, and potential disaster relief efforts.

ICS Dependence and Cyber Risk of National Critical Functions

Jackie N. First and Chloe J. Applegate, Lawrence Livermore National Laboratory

The Department of Homeland Security has defined National Critical Functions (NCFs) as "The functions of government and the private sector that are so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety." Many of these functions are heavily dependent on industrial control systems (ICS), which can lead to vulnerabilities and risk from cyber-attacks.

Our project involves prioritization of NCFs with respect to ICS cyber risk as well as identifying NCFs that would not be disrupted in an event of cyber-attack. We have developed a framework for NCF cyber dependence and vulnerability which accounts for both the vulnerability of the NCF to cyber-attack and the potential consequences of a set of cyber-attacks.

Python Simulator for Cyber Event Scenarios (PySCES)

Mike Nygaard, Lawrence Livermore National Laboratory

Cyber-attacks on critical infrastructure that cause physical impact and affect performance are no longer a remote possibility, but a reality. Since the first confirmed cyber-attack to cause a power outage, which occurred in Ukraine in December of 2015, the energy industry has been keenly aware of this reality. Subsequent attacks—such as 2016's CrashOverride event in Ukraine, 2017's TRITON attack in Saudi Arabia, and recent reports of ransomware causing a multi-day outage of an unnamed natural gas compression facility in the US—highlight the fact that the US energy infrastructure system is at constant risk of cyber-attacks.

Existing methodologies for assessing the impacts to energy infrastructure systems stemming from novel device vulnerabilities hinge upon qualitative assessments from subject matter experts, which is time consuming, burdensome, and potentially prone to errors. To fill this void, LLNL has developed the Python Simulator for Cyber Event Scenarios (PySCES). PySCES facilitates the co-simulation of two distinct modeling domains, and links energy system modeling tools such as Synergi Gas or PSLF with detailed multi-domain process modeling tools like Simulink and Simscape. This co-simulation allows analysts to trace the impacts of a cyber-attack as it affects a particular device, as that device causes mis-operation of an energy system facility, and as that facility affects the energy infrastructure system as a whole. Modeled ICS devices are detailed enough to assess specific device-level impacts from the attack, but are generalized to avoid the need to create unique models for every unique vendor and model.

Understanding the impact that a device vulnerability can have on the broader energy infrastructure system is key to determining how the mitigation of the vulnerability should be treated. PySCES allows for

rapid assessment of the system impact, and provides analysts with the system-level context needed to make an informed decision on mitigation.

Intelligence-Led Protection of the Infrastructure Environment

Frederick Ferrer, Idaho National Laboratory

This abstract outlines a proposal by which a longtime threat analysis methodology used by the military and law enforcement—Intelligence Preparation of the Battlefield/Operational Environment (IPoB/IPOE)—can be modified for use by Infrastructure Analysts to provide greater awareness of the threats to critical infrastructure and key resources in their areas of responsibility.

This modified Intelligence Preparation of the Infrastructure Environment (IPIE) would be used to help the analyst better model, analyze and provide information to decision makers that enables them to better understand the threats and vulnerabilities to critical infrastructure. The knowledge and decisions made from this enhanced viewpoint would, in turn, help in a myriad of ways—from enabling law enforcement and security to better protect and secure critical infrastructure and key resources to preparing others in support of decision-making that enhances resilient investment, planning and development of infrastructure.

The purpose of empowering infrastructure analysts and others with this modified IPIE assessment methodology is just not so they can develop an increased, more comprehensive range of knowledge about threats to infrastructure and assets within their areas of responsibility, but could enhance the cycle of information and intelligence that flows, horizontally and vertical across various sources. Stated another way, the application of IPIE will not just provide a more comprehensive picture of threats to the infrastructure environment, but a tool to relay to the eyes and ears of infrastructure protection—law enforcement, first responders and private security that work in and around a region's infrastructure—on the front lines of critical infrastructure protection.

This talk would be comprised of the following components:

- a brief overview of the current information/intelligence flow of critical infrastructure information and intelligence between Federal, State and local law enforcement and intelligence agencies;
- typical sources of information collected and used by analysts in order to develop the threat environment to infrastructure in their areas of responsibility;
- the additional contextual information brought to the threat landscape using the IPIE methodology; and
- how this more comprehensive information can help to leverage law enforcement, security personnel and others to better recognize and report threats and hazards to critical infrastructure and key resources.

To best evaluate the levels of protection needed to secure and safeguard a region's critical infrastructure and key resources, infrastructure protection analysts, decision-makers and security personnel must know more than the location of their most critical assets and the list of possible threats to these assets. Intelligence-focused Preparation of the Infrastructure Environment provides a methodology through which they can add non-traditional and contextual attributes of an environment to better understand and evaluate how to better protect the nation's critical infrastructure and key resources.