SAND2016-4413PE

Exceptional service in the national interest

Sandia National Laboratories

Cyber Tracer Program

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. Sand2016-????

Cyber Tracer Program & RECOIL

Sandia National Laboratories

Combining Applied Research in Human Cognition and Cyber Security to Improve Capabilities and Accelerate Learning of Operational Incident Response Teams

Cyber Tracer Program

Sandia National Laboratories

- Our mission is to conduct research and develop techniques to:
  - Create a community of cyber defenders sharing expertise, skills, and competencies that raises the standards of individuals and the overall community of defenders
  - Attract, inspire, and grow the next generation of expert cyber defenders for the US
  - Support educational institutions to create educational capabilities and infrastructure to foster the development of future cyber defenders

What if we…

- Could enhance the performance of human analysts engaged in cyber defense?
- Could improve the ability to identify candidates that will be successful cyber analysts?
- How? By exploiting Sandia's demonstrated experience in cyber security live exercises (Tracer FIRE and RECOIL ForCE) and the emerging technology of neuroscience along with cutting edge work in machine learning at Sandia…

Then, we might be able to build a national cadre of "Grand Masters" in Cyber and up our game against our adversaries.

DOE/NNSA MSI & Federal Research Funding

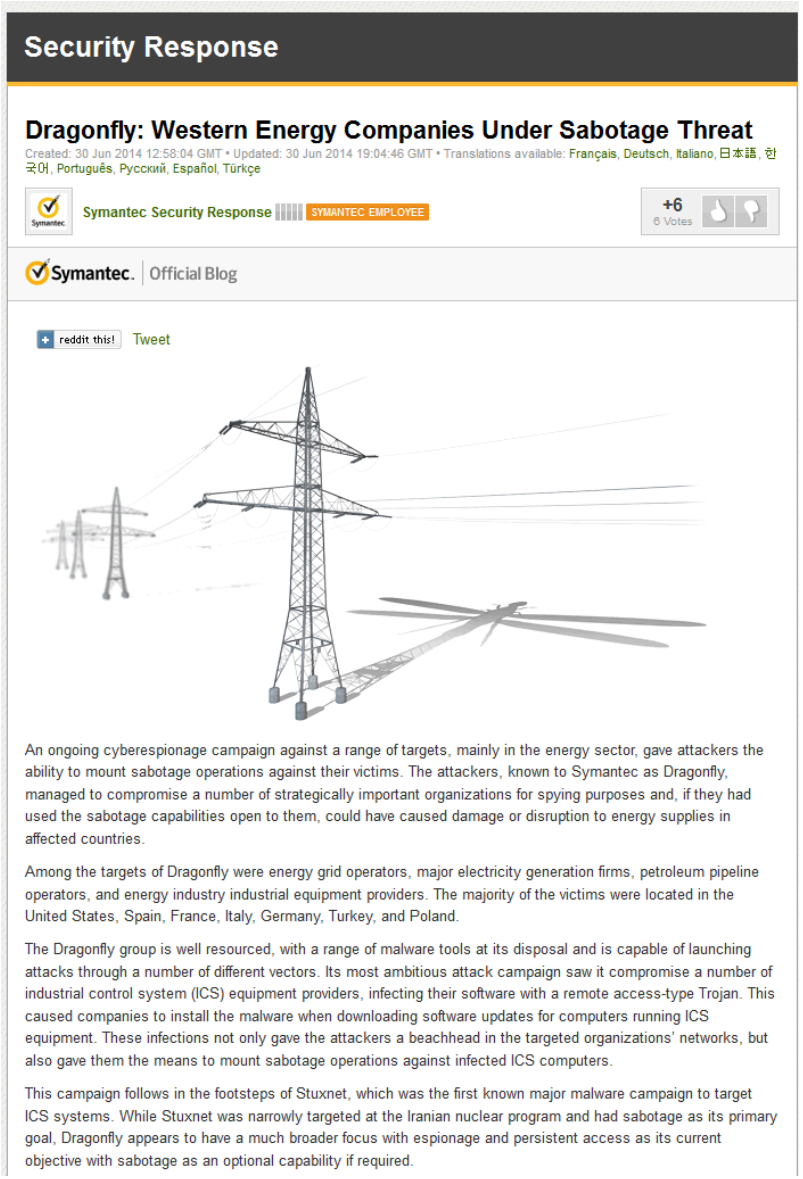
Sandia National Laboratories

- **$25M/5-year grant from DOE** to establish a Cyber Security Consortium amongst 14 MSI Universities (Norfolk State University is lead PI)
- **$500K AFRL grant** to study human effects of weapon induced failures from high power microwave
- LDRD has generated interest from other FFRDC's to collaborate or license Tracer FIRE technology for their research:
  - CMU CERT
  - Air Force Research Lab
  - Office of SecDef

DOE/NNSA MSI & Federal Research Funding (cont.)

Sandia National Laboratories

- Beta-tested **new scenario called Dragonfly and Tracer environmen**t at LLNL in July 2014 (this prototype is being used for research data collection and to train staff and students used at events for DOE/JC-3 and Universities
- All of the software and hardware was **created by summer students** in the MSI and/or CCD program
- Will serve as a test case to integrate into University curriculum (targets: **Norfolk State, Bowie State, UNM, TTU, and University of Arizona**)



Security Response

Dragonfly: Western Energy Companies Under Sabotage Threat

Created: 30 Jun 2014 12:58:04 GMT • Updated: 30 Jun 2014 19:04:46 GMT • Translations available: Français, Deutsch, Italiano, 日本語, 한국어, Português, Русский, Español, Türkçe

Symantec Security Response SYMANTEC EMPLOYEE

+6 6 Votes

Symantec. | Official Blog

reddit this! Tweet

An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries.

Among the targets of Dragonfly were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

The Dragonfly group is well resourced, with a range of malware tools at its disposal and is capable of launching attacks through a number of different vectors. Its most ambitious attack campaign saw it compromise a number of industrial control system (ICS) equipment providers, infecting their software with a remote access-type Trojan. This caused companies to install the malware when downloading software updates for computers running ICS equipment. These infections not only gave the attackers a beachhead in the targeted organizations' networks, but also gave them the means to mount sabotage operations against infected ICS computers.

This campaign follows in the footsteps of Stuxnet, which was the first known major malware campaign to target ICS systems. While Stuxnet was narrowly targeted at the Iranian nuclear program and had sabotage as its primary goal, Dragonfly appears to have a much broader focus with espionage and persistent access as its current objective with sabotage as an optional capability if required.

RECOIL

Sandia National Laboratories

Research capability and facility that fosters the integration of cyber security and cognitive science

Created to collaborate with academia, industry, and government to facilitate experiments that apply a multidisciplinary approach in cyber using:

1) case study analysis of adversary techniques and exploit methods;
2) big data analytics and machine learning; and
3) cognitive psychology and cognitive neuroscience.

This multidisciplinary approach of **cyber security practitioners, psychologists, sociologists, and computer science researchers** working together offers a powerful combination of skills and experience that can be applied in a unique research facility.

"Achieving cybersecurity is far more than a technical problem: it is fundamentally a people problem, and since cybersecurity is a people problem, there must be a people solution."

Lt Colonel Kern, Pell Center

SNL RECOIL Research

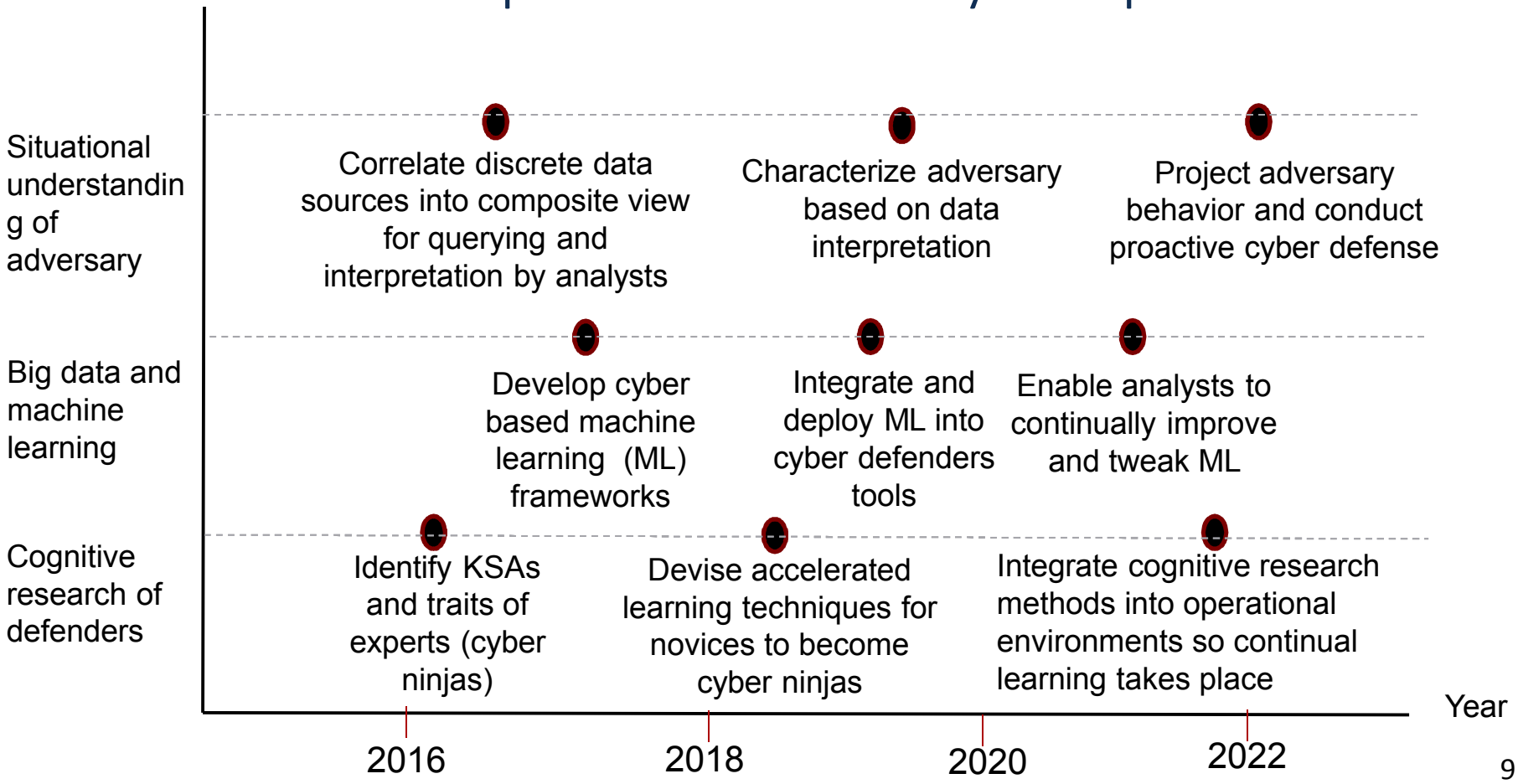
Sandia National Laboratories

- Research Question:
  - How do we train and develop high-performing Cyber Security Incident Response Teams (CSIRTs) in the US that can solve today's complex cyber challenges.
- Approach:
  - Narrative-Based and Scenario/Problem-Based Learning Competitions
  - Neuroscience based Cognitive Research and Competency/Performance Modeling for Cyber Defenders
  - Identify methods of assessing and recruiting qualified candidates to work in cyber security
  - Determine the influence of creativity and cognitive flexibility in expert cyber defenders
  - Identify methods to reduce cognitive workload

RECOIL Roadmap

Sandia National Laboratories

Integrating Human Performance Research and Big Data Science to Develop National Cadre of Cyber Experts



Tracer FIRE (Forensic Incident Response Exercise)

Sandia National Laboratories

- Focus is on Incident Response Training
- Real World Exercise Requires Student to Put the Pieces of the Incident Together or What is Referred to as the Cyber Kill Chain
  - Who is the adversary?
  - How did they get in?
  - What did they want and did they acquire it?
  - How to prevent recurring incidents?
- Students Investigate an APT (Advanced Persistent Threat) Style Adversary Throughout the Event
- Tracer FIRE Team Provides the Expertise, Infrastructure, & Network for the Exercise

Goal of Tracer FIRE

Allow students to achieve this state of “Flow” in Cyber Incident Response

Flow

“ is the mental state of operation in which a person in an activity is fully immersed in a feeling of energized focus, full involvement, and success in the process of the activity.”

Mihaly Csikszentmihalyi

Scenario Driven Learning

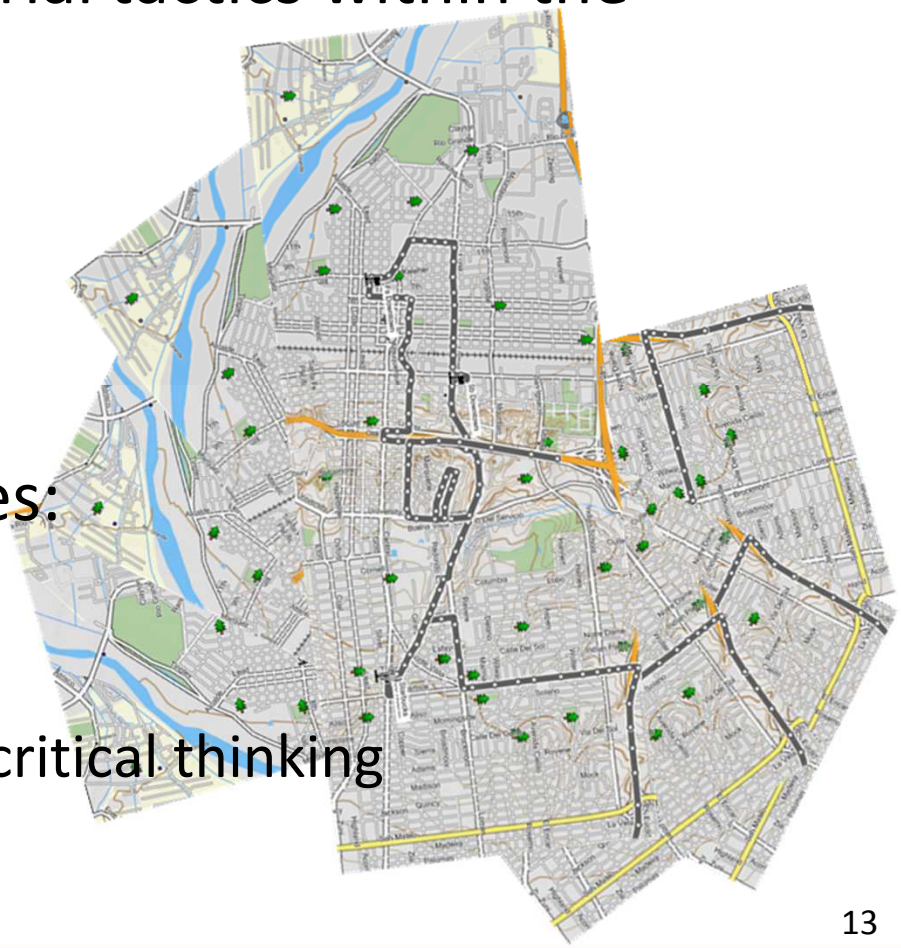
- TF5 Scenario was created with the concept of narrative based learning:
- Enables participants to enhance their understanding of cyber related problems and their solutions in contextually-meaningful ways
- Similar to medical education where students spend time in residency before qualification as a doctor.

ShmuxBux Coffee Company Under Attack

Incident Responders Learning

Sandia National Laboratories

- How to recognize adversarial tactics within the context of the kill chain:
  - Reconnaissance
  - Attack vector
  - Exploitation
  - Exfiltration
- Implicit Learning objectives:
  - Look beyond the clues
  - Infer adversarial intention!
  - Overall goal is to promote critical thinking



Tracer FIRE

Sandia National Laboratories

Self Select Teams

Team 1

Team 2

Team 3

Day 1

Concept & Tool Training

Incident Response Exercise

Day 2

Concept & Tool Training

Incident Response Exercise

• • •

Last Day

Incident Response Exercise

Debriefing

Tracer FIRE Options

- Tracer FIRE event can be 2 days, 3 days, or a full week
- Previously Developed Events are Available
- Concept and Tool Training Can be Customized for Customer Needs
- Incident Response Exercise Can be Customized to Customer Needs by Creating Scenarios that Match your systems and networks i.e., power plant scenario for power plant operators

Tracer FIRE Outcomes

Sandia National Laboratories

- Promotes Critical Thinking & Problem Solving
- Provides Training on Tools & Capabilities to Perform Incident Response
- Provides Students with a Better Understanding of the Cyber Kill Chain & Why it is Important in Incident Response
- Allows Students to Interact with Live Malware Without Compromising Their Own Systems
- Promotes Collaboration Between Team Members
  - Co-workers
  - Colleagues from other institutions
- Strengthens Relationships Between Co-Workers
- RECOIL Capabilities Can Be Added to Tracer FIRE Platform
  - Identifying student level of expertise
  - Human factors research
  - Case study analysis of adversary techniques & exploit methods

Previous Scenario Showcase

Tracer FIRE 6 Scenario:
“Canuckistan”

- Students are incident responders for Canuckistan Power Company.

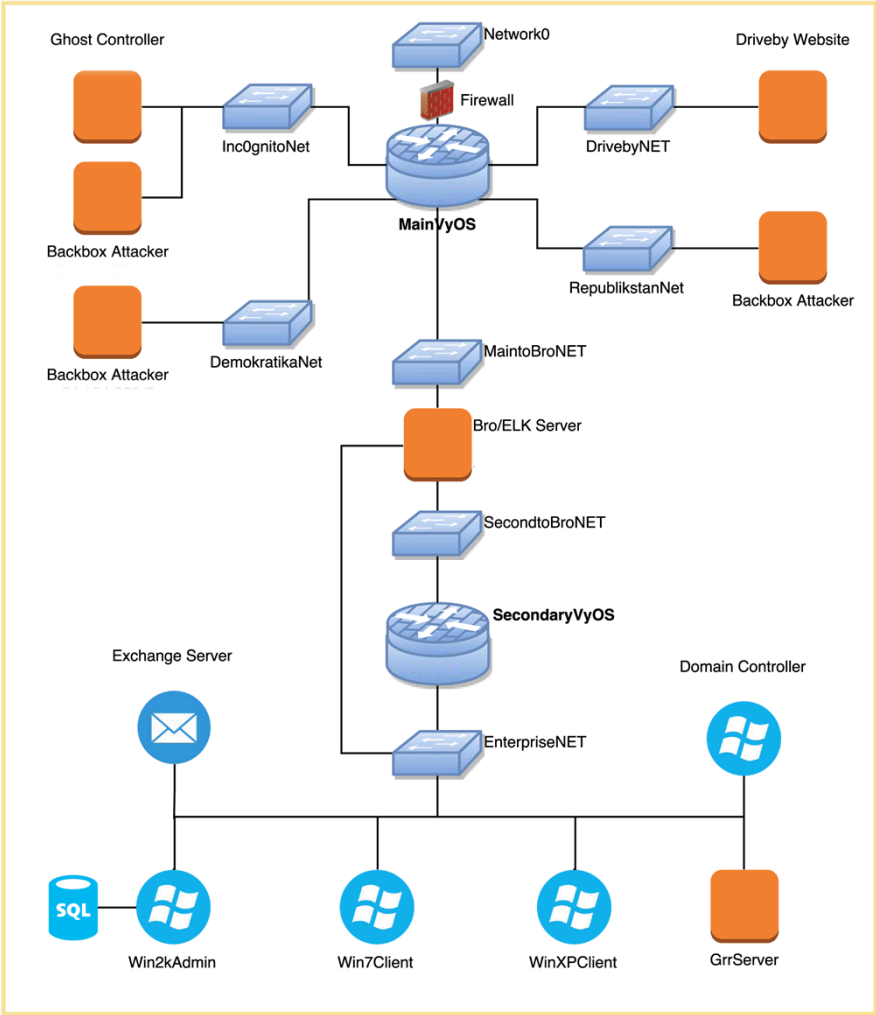
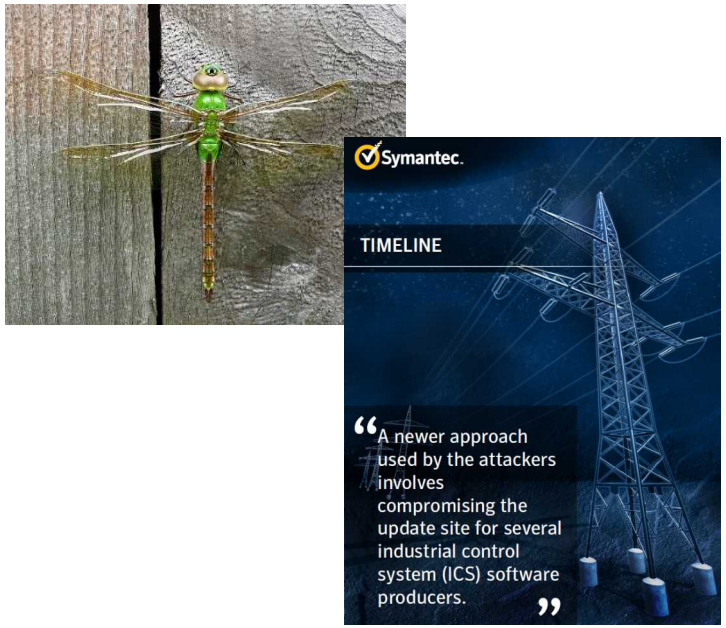


Diagram of Scenario Network Design

Canuckistan: Threat Actors

- Environmental Hacktivist Group called nC0Gnito
- Demands that Canuckistan Power shut down and convert to clean energy such as wind and solar or face a complete take over of their power generation facility



nC0Gnito video and threat narrative based on Dragonfly Campaign

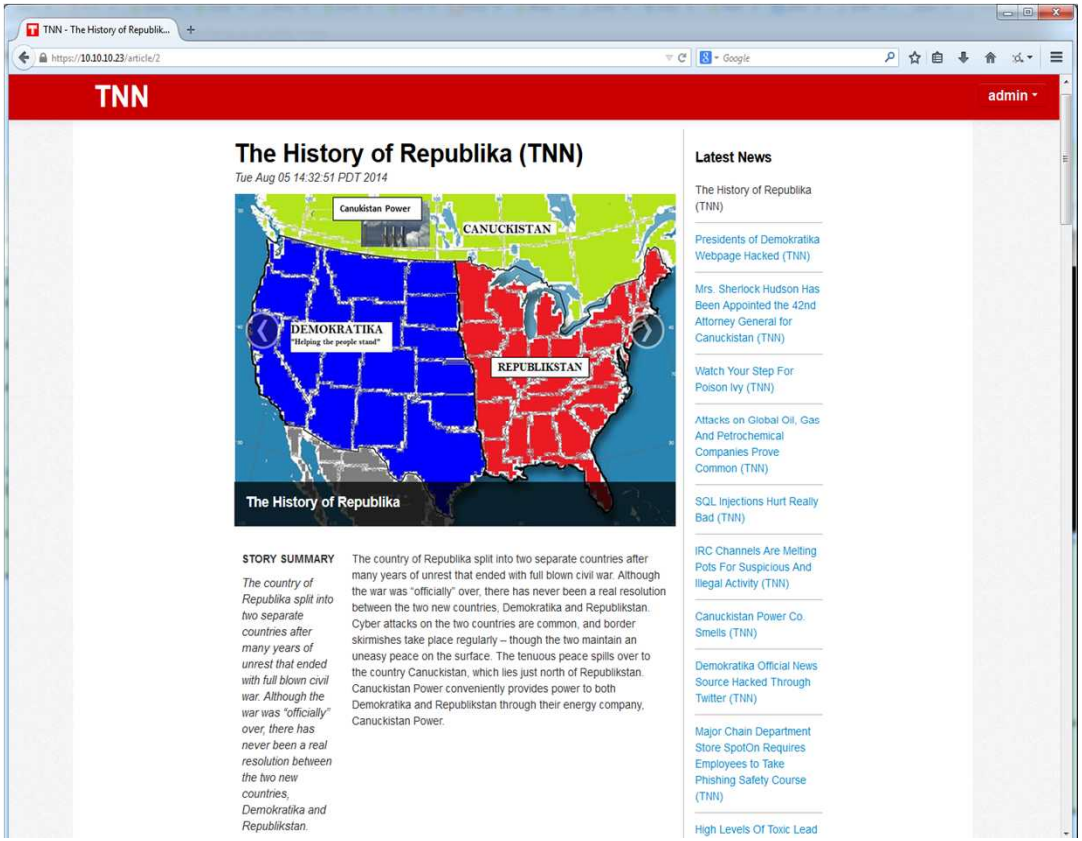
Created by Lauren Lockett (UNM), Kelly Cole, Susan Fowler (Purdue) and Rebecca Hart (Ohio State)

Canuckistan: Tracer News Network

Sandia National Laboratories

Content Management System

- Injects the relevant and irrelevant news and information into scenario and requires teams to comprehend narrative and research
- Provides researchers ability to measure situational understanding and awareness of teams while they participate in exercise
- Motivates teams to perform intelligence analysis as they progress through exercise

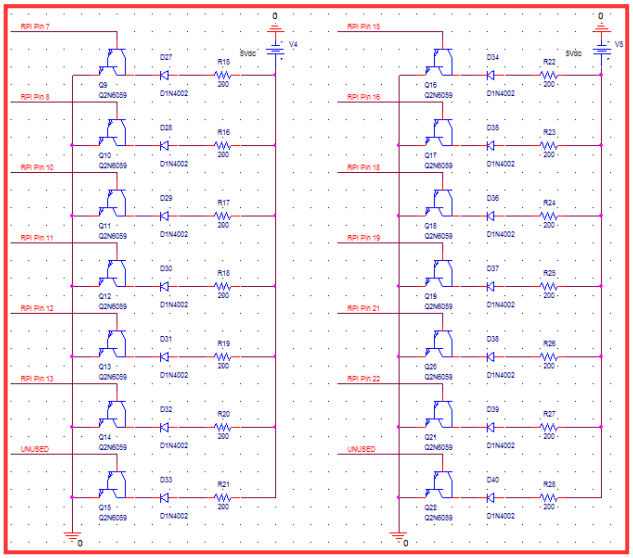


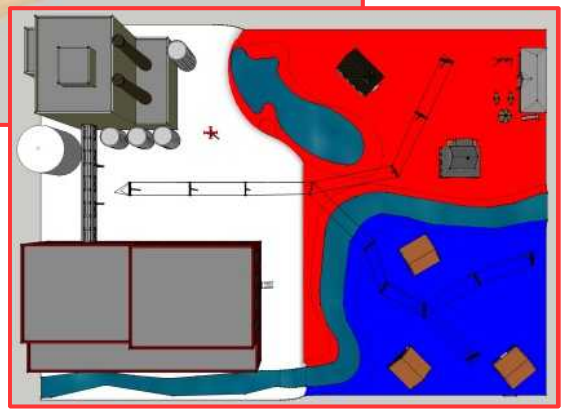
Canuckistan: SCADA Model

Sandia National Laboratories

Power Generation Simulation

- Design implemented Raspberry Pi's to simulate a SCADA system for power generation
- Portable system that can be taken to Tracer FIRE events on the road
- Realistic HMI display that emulates power plant SCADA systems and power grids to educate cybersecurity experts on how to respond to energy crisis scenarios like blackouts from cyber attacks





Jeremy Gin (University of Arizona), Matthew Letter (UNM) and Marcos Torres (UNM), and Rain Dartt (Rose-Hulman Institute)

THE UNIVERSITY OF ARIZONA.

UNM

ROSE-HULMAN INSTITUTE OF TECHNOLOGY

Event Debrief & Research Efforts

Sandia National Laboratories

Event Debrief

- Teams are asked to make sense of their analysis that they performed during the week and tell a complete story of what the **adversary did and their possible motives and intentions**
- Provides teams **opportunity to reflect** on what they did and observed during the week

Research Efforts

- Teams have agreed to be videotaped and research is underway to analyze team and individual performance aspects
- Sandia's cognitive team has designed agent software to monitor students **workflow and application usage**
- Sandia is exploring research methods that include measurement of participants **eye tracking and EEG**
- Objective is to gain a **fundamental understanding of cognitive skills** of individuals and teams while they perform under stress during a simulated cyber attack

Team DeadBeef Cafe Briefing at ENDEX

Questions

Sandia National Laboratories