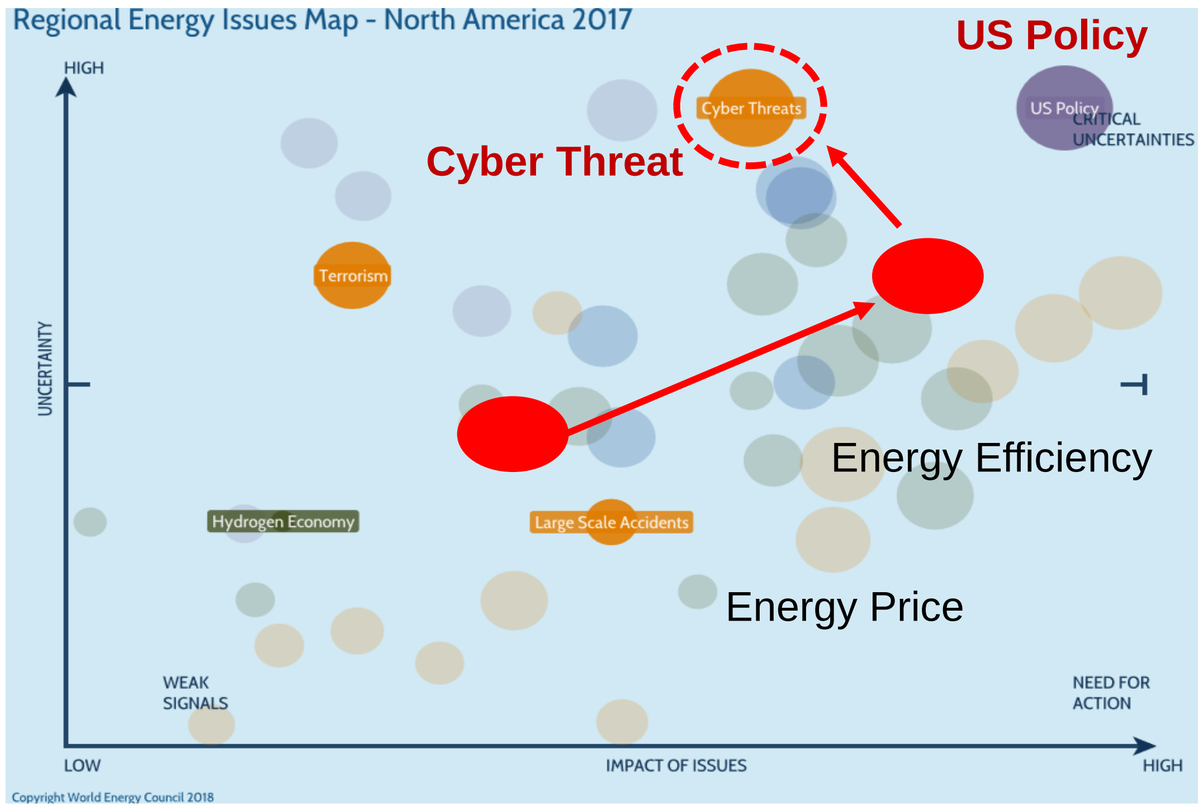
Real-time Cyber Analysis to Improve Operational Response to a Cyber Attack

Stuart Madnick, Michael Siegel, Keman Huang, Mohammad S Jalali, Keri Pearlson, Isabelle Chong

CYBER THREATS KEEP LEADERS AWAKE AT NIGHT

"Cyber threats are among top issues keeping energy leaders awake at night in Europe and North America."



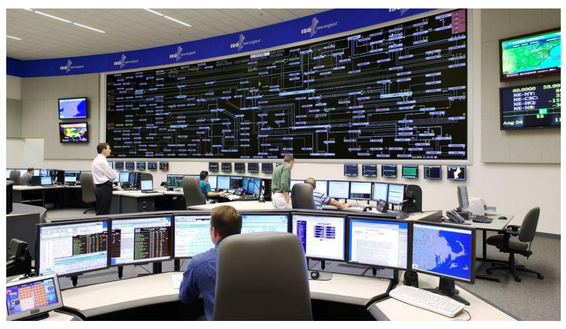
- **Critical Uncertainties**: high uncertainty, high impact, with no clear path of action, keep energy leaders most awake at night
- **Action priorities**: Keep energy leaders most busy

RESEARCH VISION

We intend to assist the EDS operator's response to a cyber attack and to improve the cybersecurity resilience.

CHALLENGE FOR OPERATIONAL RESPONSE

Challenge 1: Utility Operation vs. Cybersecurity

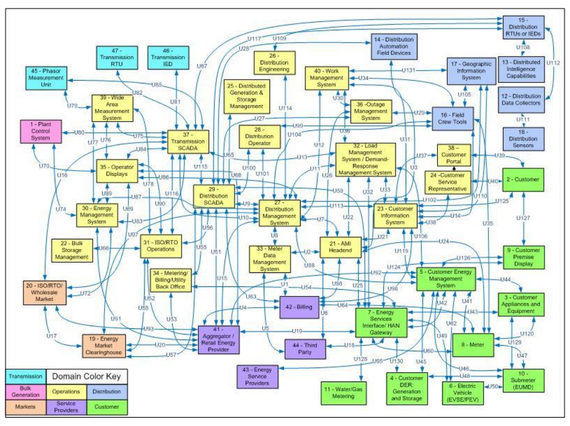


- **GOLDEN RULE 1**: SHOULD NOT expect Operators to become cybersecurity expert! Actionable Information!
- **GOLDEN RULE 2**: SHOULD NOT make things even more complex to operator

Challenge 2: Communicate in Different Language

- **GOLDEN RULE 3**: SHOULD make it easier to communicate with the expert! Talk the same language

Challenge 3: Cascaded Attack in Complex System



- **GOLDEN RULE 4**: SHOULD ensure that the operational response itself does not enable a cascading failure.

EXAMPLE SCENARIO

GridEx III: breakers for substation going on and off unexpectedly

- Disconnect the substation from the power grid
- Send field crews to investigate
- Operate the substation manually by updating firmware

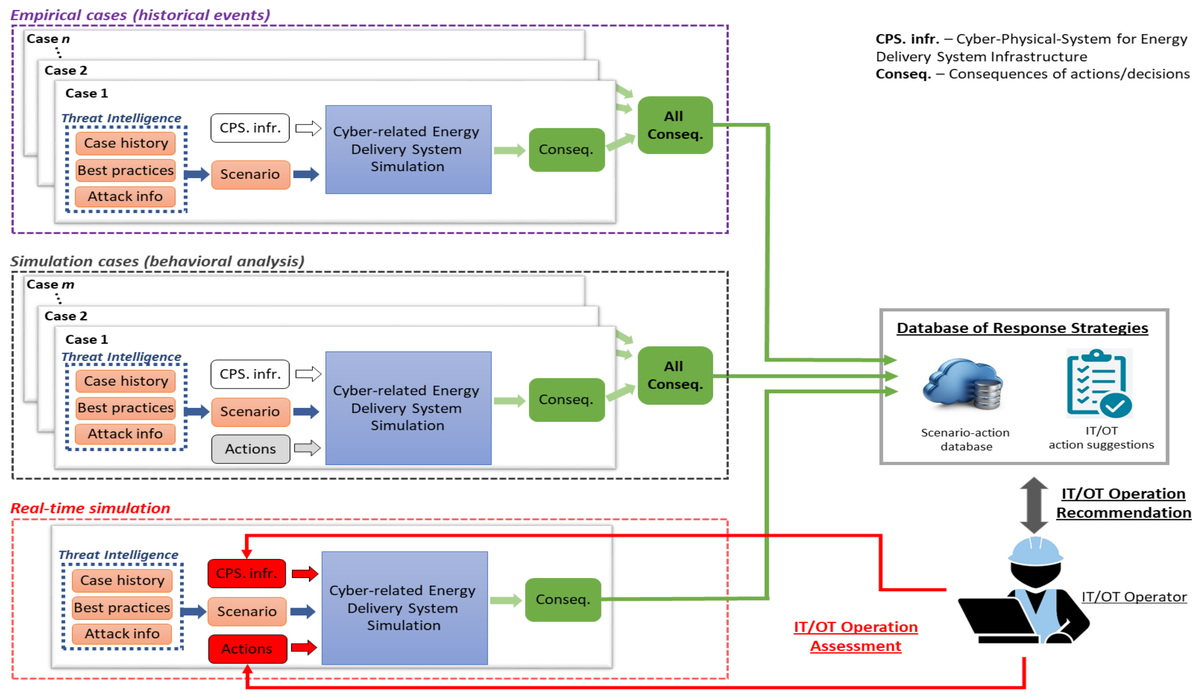
✓ **NESCOR DGM 14:** Attackers dial into modems attached to the remote terminal unit (RTU) and send fake breaker trip commands*

✓ **NESCOR DGM15.** Attackers gain access to the control room and then energizes distribution lines or equipment that are under maintenance by linemen to elicit injury or death by electrocution

✓ **WAMPAC.8:** Malware in PMU/PDC Firmware Compromises Data Collection

* The Ukraine 2016 attackers triggered malicious breaker trips, but by a different attack path

RESEARCH FRAMEWORK & BENEFIT

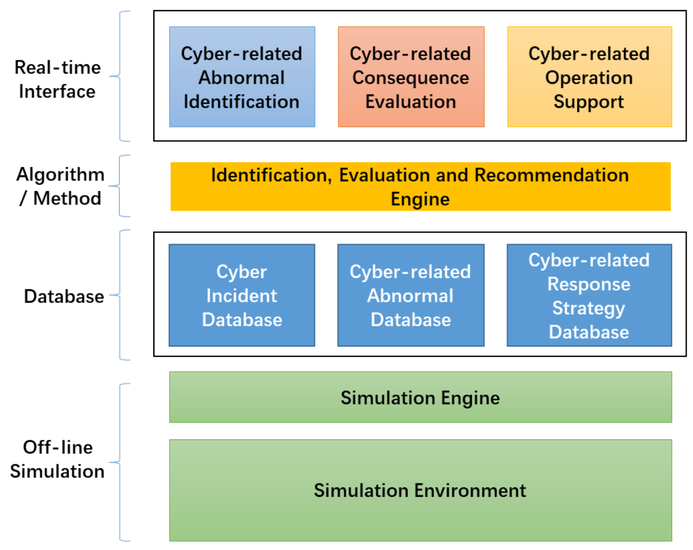


➢ ***Prepare Operators for potential cyber attacks.***

➢ ***Make Overwhelming Guidelines ready for operators when they are needed***

➢ ***Improve Response Capability and Cyber Resilience***

ARCHITECTURE



- ✓ whether the observations are related to the potential cyber security attacks
- ✓ the potential cyber-related consequences given the standard response procedure
- ✓ consequence tree to help the operator choose the response

- ✓ **Cyber Incident Database:** existing cyber attack incidents to the energy sector
- ✓ **Cyber-related Abnormal Database:** abnormal observations and potential mitigate strategies from potential cyber attacks
- ✓ **Cyber-related Response Strategy Database:** standard/cyber-related response strategy for abnormal observation

COLLABORATION OPPORTUNITIES

Cooperation, support, feedback and involvement from industry partners would benefit this research:

- Cyber attack scenarios Discussion to make them specific
- Response plans or procedures for database enrichment
- Cyber attack cases sharing for learning
- Feedback or suggestion to improve this research activity

Contact: keman@mit.edu, msiegel@mit.edu

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY