Rapid Attack Detection, Isolation and Characterization Systems (RADICS)

Early warning and rapid recovery of
critical power grid infrastructure
from network cyber attacks

John O. Everett, PhD
Information Innovation Office
January, 2017

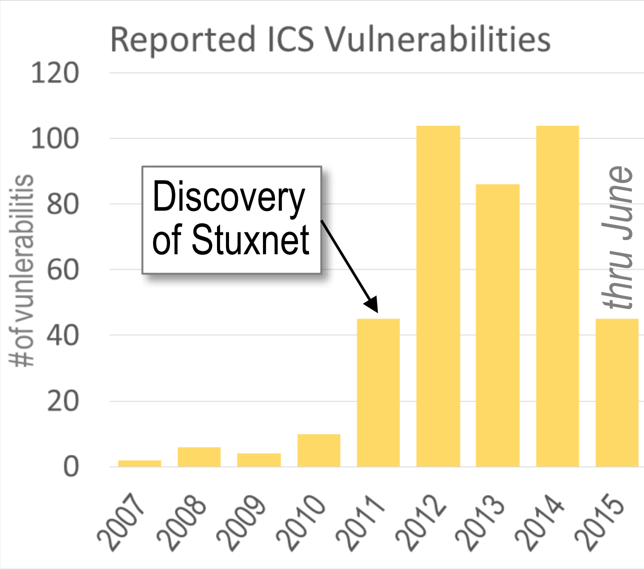
Michael A. VanPutte, Ph.D
Provatek, LLC
RADICS TA-5 Exercise Director

Cyber Risk to Critical Infrastructure

ICS: *Industrial Control System*

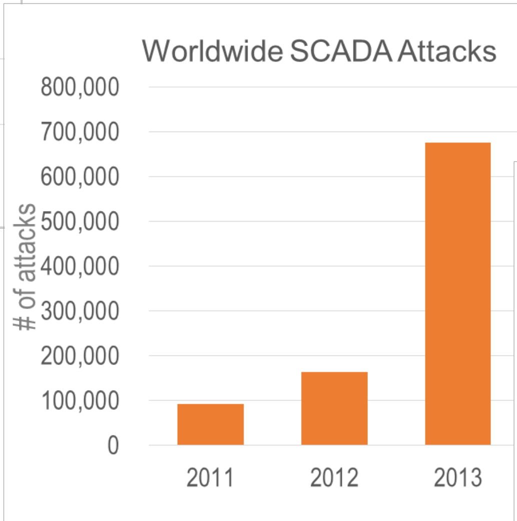
SCADA: *Supervisory Control and Data Acquisition*

SHODAN: *Search engine for devices connected to the Internet*



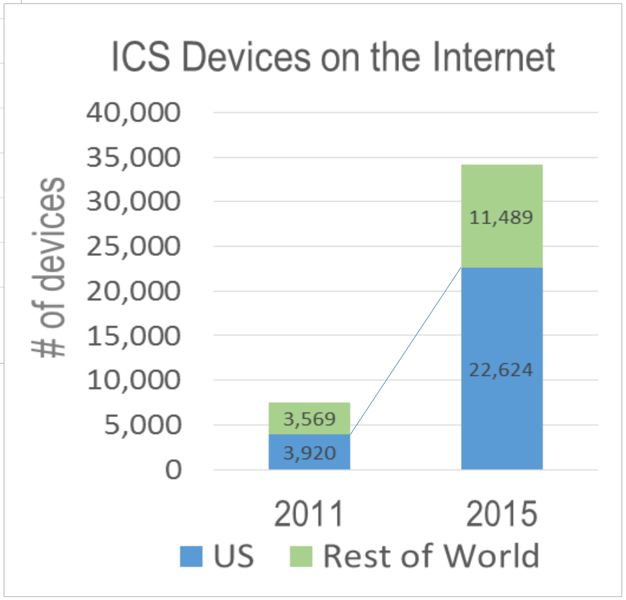
Source: Up and to the Right: ICS/SCADA Vulnerabilities by the Numbers. Recorded Future. http://goo.gl/35J19o

Stuxnet focused cyber attackers on industrial control systems (ICS)



Source: 2015 Dell Security Annual Threat Report

In the same timeframe, US ICS devices on the Internet increased 55% per year



Source: shodan.io, using 29 queries from *Quantitatively Assessing and Visualising Industrial System Attack Surfaces*, Cambridge 2011

- **Utility investment in cyber security is not enough**
  - Competing with infrastructure modernization for capital
  - Interconnection creates a tragedy of the commons
- **Adversaries are exploring US critical infrastructure**
  - Malware has been targeting the energy sector since 2012

DISTRIBUTION A. Approved for public release: distribution unlimited

Why is this a DoD Problem?

- **DoD mission effectiveness is inextricably dependent on civilian infrastructure**
- **A large-scale, sustained blackout would**
  - Hamper mobilization
  - Disrupt military logistics and supply chain
  - Deny access to reach-back capabilities
  - Reduce strategic options
- **2015 DoD Cyber Strategy addresses the risk**

> Strategic Goal III: Be prepared to defend the U.S. homeland and U.S. Vital Interests from disruptive or destructive cyberattacks of significant consequence

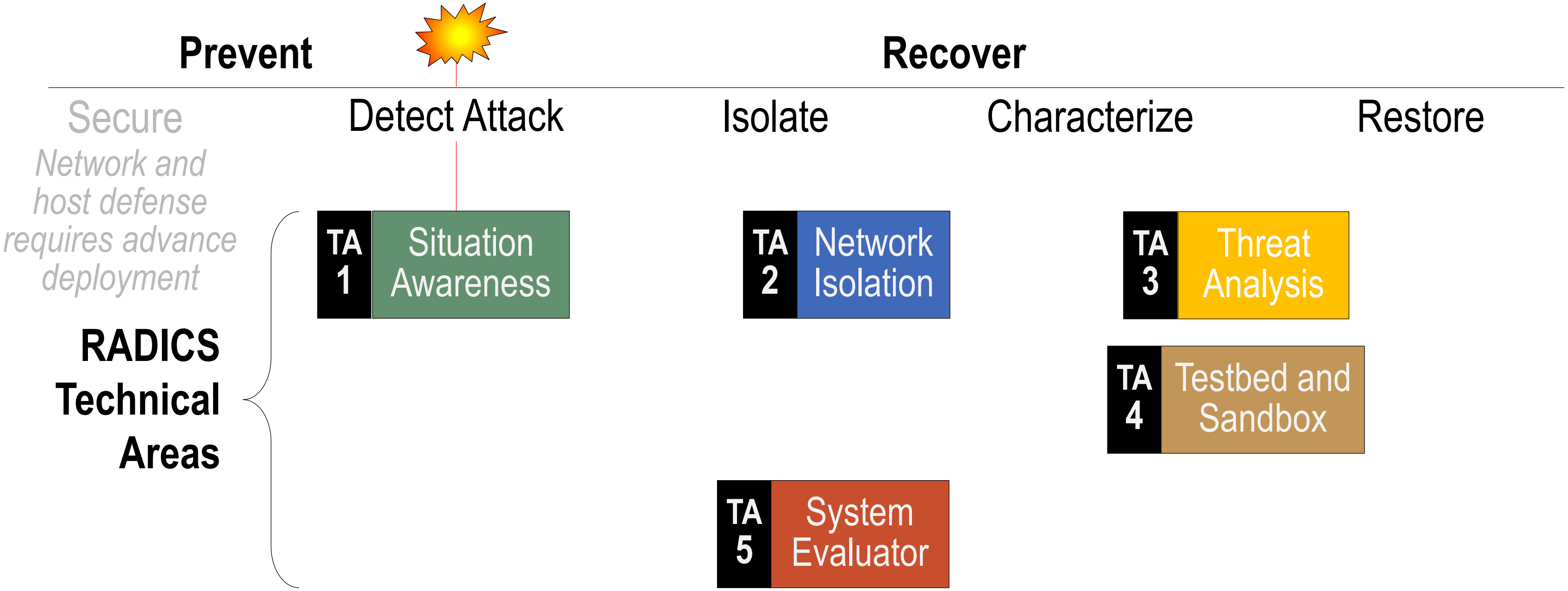
Program Research Objective

Develop early warning and rapid recovery techniques

to thwart or blunt the impact of cyber-attacks on the US power grid

without requiring 3,200 utilities to deploy new technologies

RADICS Focus is on Recovery



Prevent

Recover

Secure

Network and host defense requires advance deployment

Detect Attack

Isolate

Characterize

Restore

RADICS Technical Areas

TA 1 Situation Awareness

TA 2 Network Isolation

TA 3 Threat Analysis

TA 4 Testbed and Sandbox

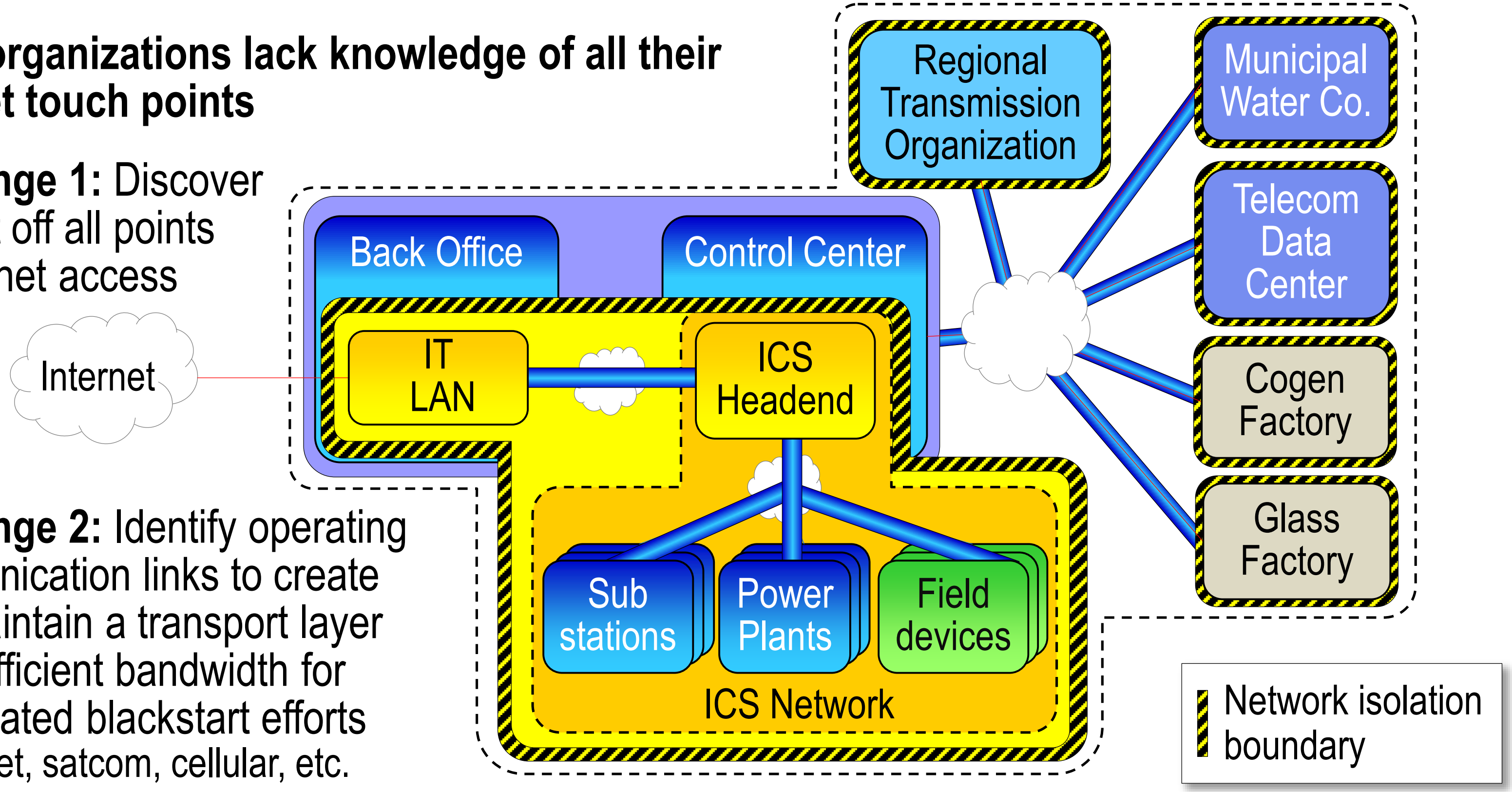
TA 5 System Evaluator

TA-1: Situation Awareness

- **Detect indications and warnings of malicious actions on the power grid**
  - Early warning of an impending attack could thwart or blunt the impact of physical damage
  - Out-of-band information could enable grid operators to detect spoofing
  - Accurate understanding of grid state in the aftermath would accelerate recovery efforts
- **Sources of data**
  - Streams of power grid sensor data
  - Streams of SCADA data
  - Wholesale power market data
  - Micro-weather forecasts and actuals
  - Patterns of life
- **Maintain and expand situation awareness after an attack**
  - The aftermath of an attack will be in continual flux
  - Some telemetry may be inaccurate or unavailable
- **Enable fine-grained, timely, geolocated awareness of power grid state**
  - Advance the state of the art (e.g., social media mining, crowdsourcing, repurposed sensors)
  - Gather and analyze this data without providing a conduit for adversary spoofing
- **Note: Government will make available power grid modeling expertise as a service**
  - Proposals that don't rely on this expertise should explain the advantages of their approach

TA-2: Isolated Emergency Networks

- **Need to stop continued cyber attacks, but recovery will require secure communications among geographically dispersed organizations without advance coordination**
- **Many organizations lack knowledge of all their Internet touch points**
- **Challenge 1:** Discover and cut off all points of Internet access



- **Challenge 2:** Identify operating communication links to create and maintain a transport layer with sufficient bandwidth for coordinated blackstart efforts
  - Internet, satcom, cellular, etc.
- **Challenge 3:** Create a secure emergency network overlay on this transport layer that nation-state adversaries cannot penetrate
- **Note: TA-2 performers must provide their own development, test and evaluation ranges**
  - Virtualized ranges should be sufficient

TA-3: Rapid Threat Characterization

- **Characterize a wide range of cyber threats**
  - Attacks on conventional IT systems in control centers
  - Malicious code in industrial control system devices (PLCs, relays, etc)
  - Changes to ICS equipment configurations
- **Localize cyber-weapons that have gained access to power grid systems**
  - Develop ways to actively map ICS networks without bricking devices
  - Cope with the vast installed base of ICS equipment
- **Develop ICS threat characterization tools that can:**
  - Understand dozens of protocols
  - Generate device emulations for sandbox dynamic analyses
  - Rapidly characterize the threat while preserving forensic evidence
  - Produce plans, scripts for remediation
- **Automate the process of developing these tools**
  - Generalize from initial prototypes
  - Research innovative approaches for analyzing legacy ICS devices
- **Develop approaches to support safe restart of affected systems**
  - Automate monitoring for signs of continued attack
- **Note: Some hardware acquisition for hands-on experience is in scope**
  - Acquiring used equipment may be a cost-effective strategy
  - TA-4 will provide primary testbed, and acquired equipment may be integrated into it

TA-4: Testbed and Sandbox

- **Provide TA-3 R&D, testing and formal evaluations with a high-fidelity ICS testbed**
  - Too expensive and time-consuming for TA-3 performers to set up their own labs
  - Must support a wide range of ICS equipment and protocols
  - Must be remotely accessible by multiple teams concurrently starting day one of the program
  - Virtualization/emulation to enable R&D that could damage physical equipment
  - Configurable to present realistic environments (e.g., a complete control room)
- **Provide TA-3 with a sandbox environment for dynamic testing of ICS malware**
  - High fidelity and breadth of ICS device coverage are essential
  - Bid as an option supporting one TA-3 performer
- **Collaborate with the System Evaluator**
  - Provide instrumentation for formal evaluations of TA-3 systems
  - Sandbox performance will be subject to evaluation

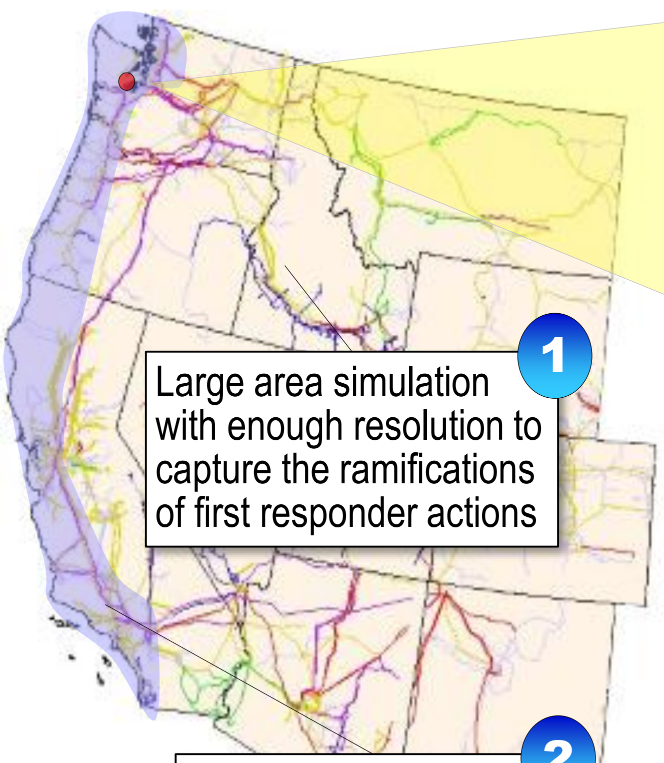
TA-5: System Evaluator

- **Technical progress assessment**
  - Regular code drops to TA-5 for automated system testing
    - Source code, development environment, build tools and scripts, unit and integration tests
  - Start with functional tests, expand to cover regression, performance, and scalability
  - Provide specific, constructive feedback to all performers developing code
- **Formal evaluations**
  - Develop relevant test cases for each TA performer system and measure performance against system-specific metrics defined in collaboration with the PM
  - Conduct evaluations in advance of PI meetings to inform the technical discussion
- **Exercises**
  - Plan, develop and coordinate exercise participation
  - Exercises will increase in complexity and duration
  - RADICS performers will operate their systems in initial exercises
  - Potential transition partners will operate RADICS systems in later exercises

Metrics

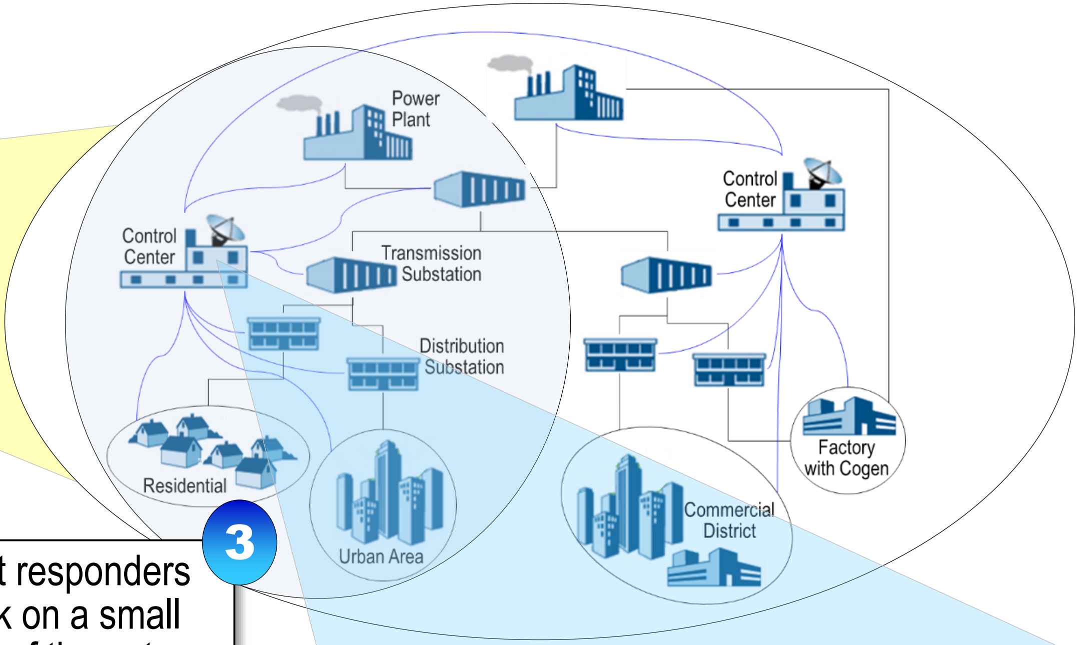
- **Proposers presented metrics relevant to the proposed approach**
  - Performers collaborate with the System Evaluator to produce tailored test plans
- **Anomaly Detection (TA-1)**
  - Best possible sensitivity with an extremely low false alarm rate
  - Earliest possible detection
- **Network Isolation (TA-2)**
  - Percent of Internet connections discovered
  - Efficiency of transport-layer planning
  - Robustness of secure emergency network
- **Threat Characterization (TA-3)**
  - Percent of ICS devices mapped in an ICS network
  - Number of protocols, device types that systems can analyze
  - Time to characterize threats
- **Sandbox (TA-4)**
  - Range of environments supported
  - Effectiveness in characterizing test and actual ICS malware

Evaluation via Multi-Resolution Simulation

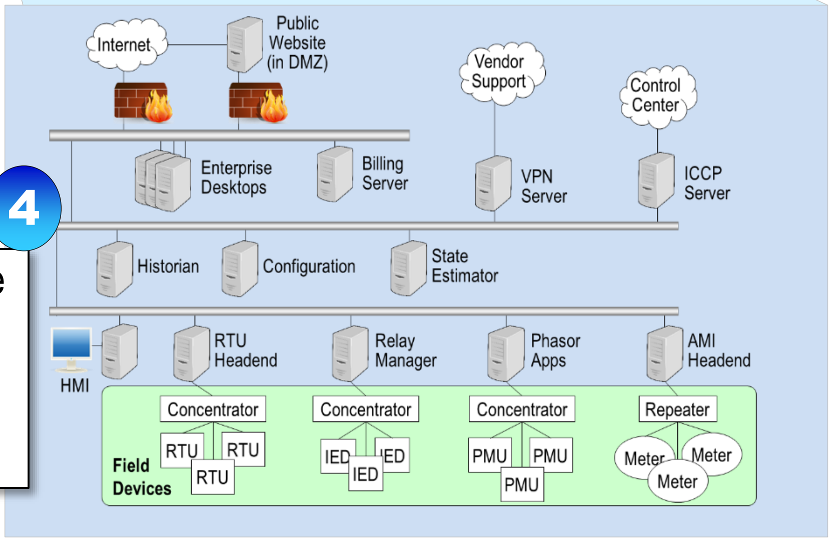


1 Large area simulation with enough resolution to capture the ramifications of first responder actions

2 Outage results from White Team application of effects consistent with a particular attack scenario



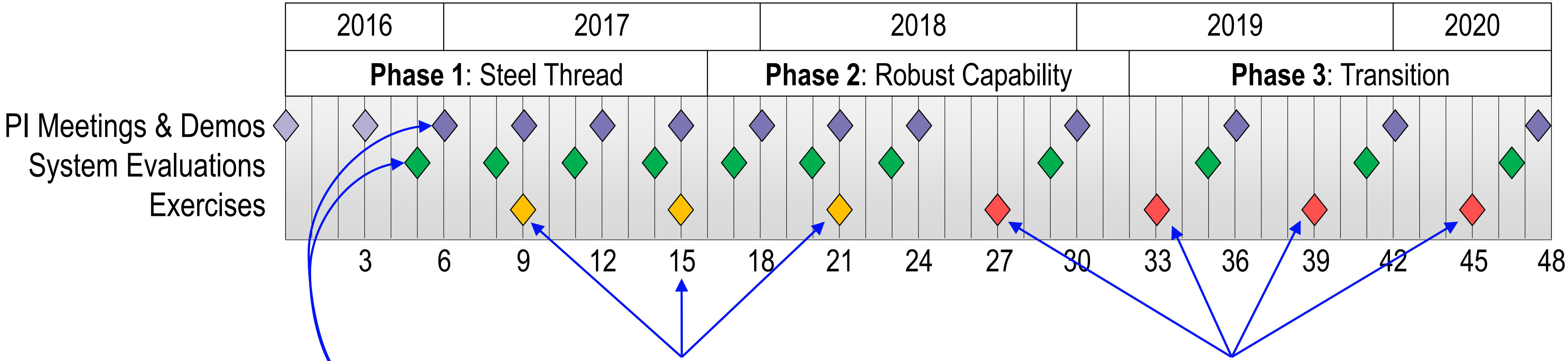
3 First responders work on a small part of the outage, simulated at higher fidelity



4 Attacked systems are simulated/emulated down to the level of applications and components

DISTRIBUTION A. Approved for public release: distribution unlimited

Program Schedule



First evaluation will provide information for debugging the evaluation process at the third PI meeting

2 to 4 day PI meeting and exercises

These exercises could be 2 to 3 weeks in duration

To Summarize

- **Approaches that require industry adoption prior to attack are out of scope**
  - Prepare for extreme events that are beyond the reach of private sector investment

- **Silver bullet solutions are unlikely**
  - Viable approaches will likely combine innovations with get-it-done engineering
  - Note any apparent shortcomings in technical areas and propose innovative solutions

- **The goal of RADICS is to reduce time to recovery to 7 days or less**
  - Think through the ramifications of a major attack on critical infrastructure
  - What software tools and information would cyber first responders want to have on hand?
  - Take advantage of things available to first responders, such as smart phones
  - Design solutions to cope with the exigencies of real-world deployment