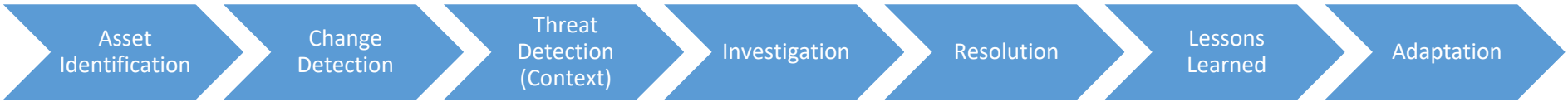
NARUC Winter Policy Summit

Critical Infrastructure Committee

NARUC Winter Policy Summit

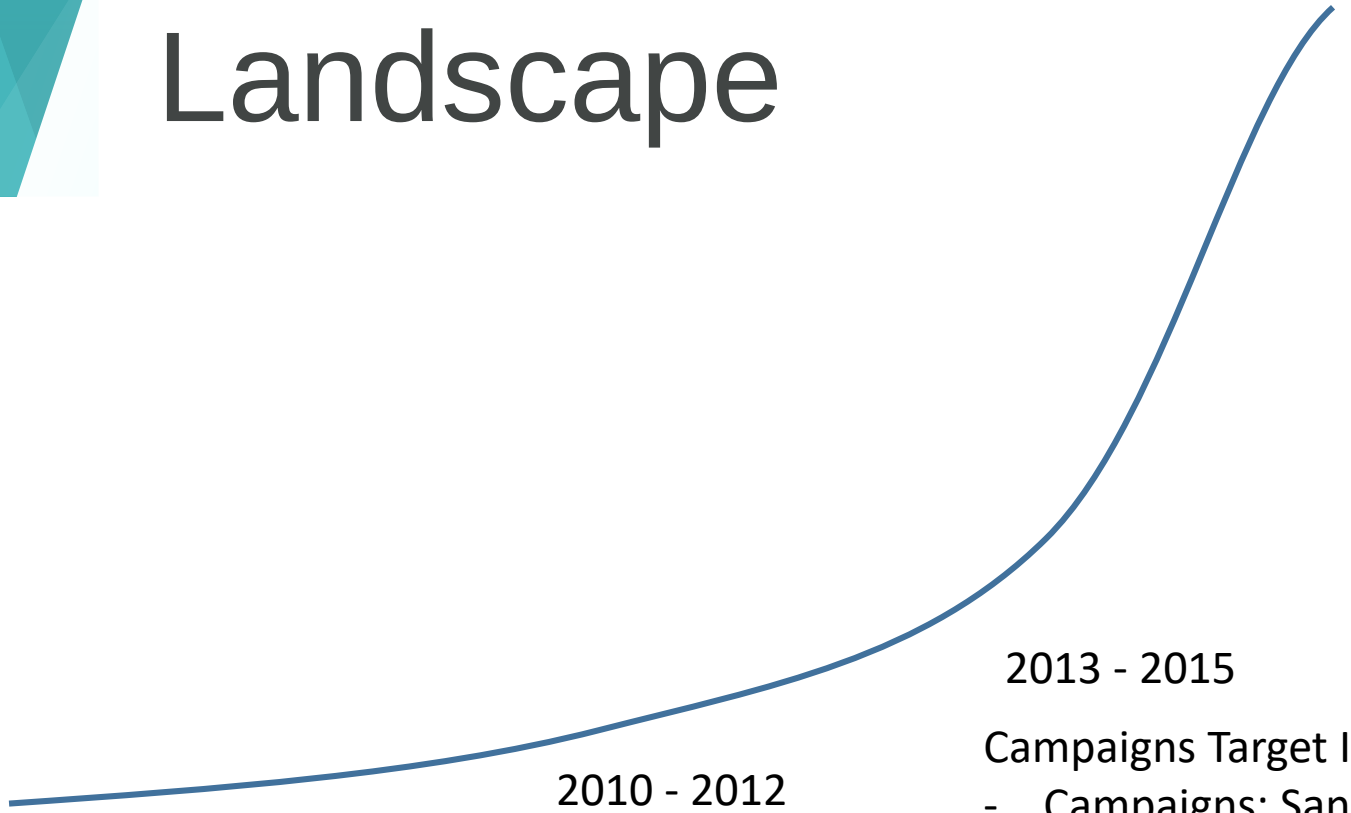
After Ukraine: Assessing Risk from Control Rooms to Wall Street

Identifying and Responding to Intrusions



DRAGOS

The Industrial Threat Landscape



1998 - 2009

Lack of Collection
- Campaigns: APT1
- ICS Malware: None

2010 - 2012

New Interest in ICS
- Campaigns: Cleaver
- ICS Malware: Stuxnet

2013 - 2015

Campaigns Target ICS
- Campaigns: Sandworm and Dragonfly
- ICS Malware: BlackEnergy 2 and Havex
- First attack to cause physical destruction on civilian infrastructure (German Steel)

2015-2017

Adversaries Disrupt ICS
- Campaigns: 8 from 5 Teams
- ICS Malware: CRASHOVERRIDE and TRISIS
- First and second ever electric grid attacks that disrupt power
- First malware to target human life

DRAGOS

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

NARUC Winter Policy Summit

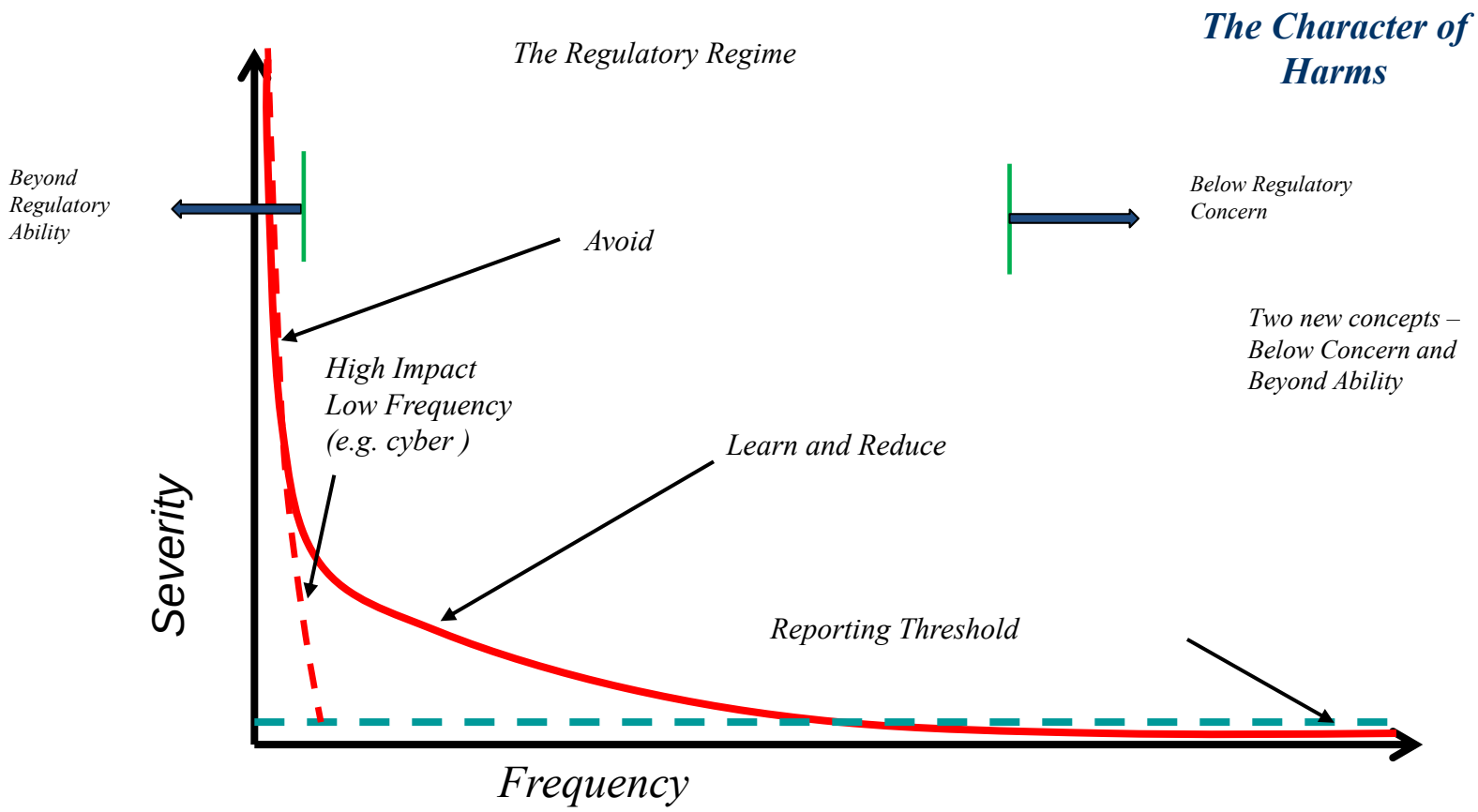
Tim Roxey
NERC Vice President
Chief Security Officer
February 11th 2018

TLP: GREEN

RESILIENCY | RELIABILITY | SECURITY




Character of Harms



Critical Infrastructure protection is beyond physical security and now includes a robust dimension of cyberspace – particularly in the energy sector

Security Elements

Threats, Vulnerabilities and Consequences

Mitigation and Response Policies

National/Multi National

Multi-National

Advanced Threat Actors

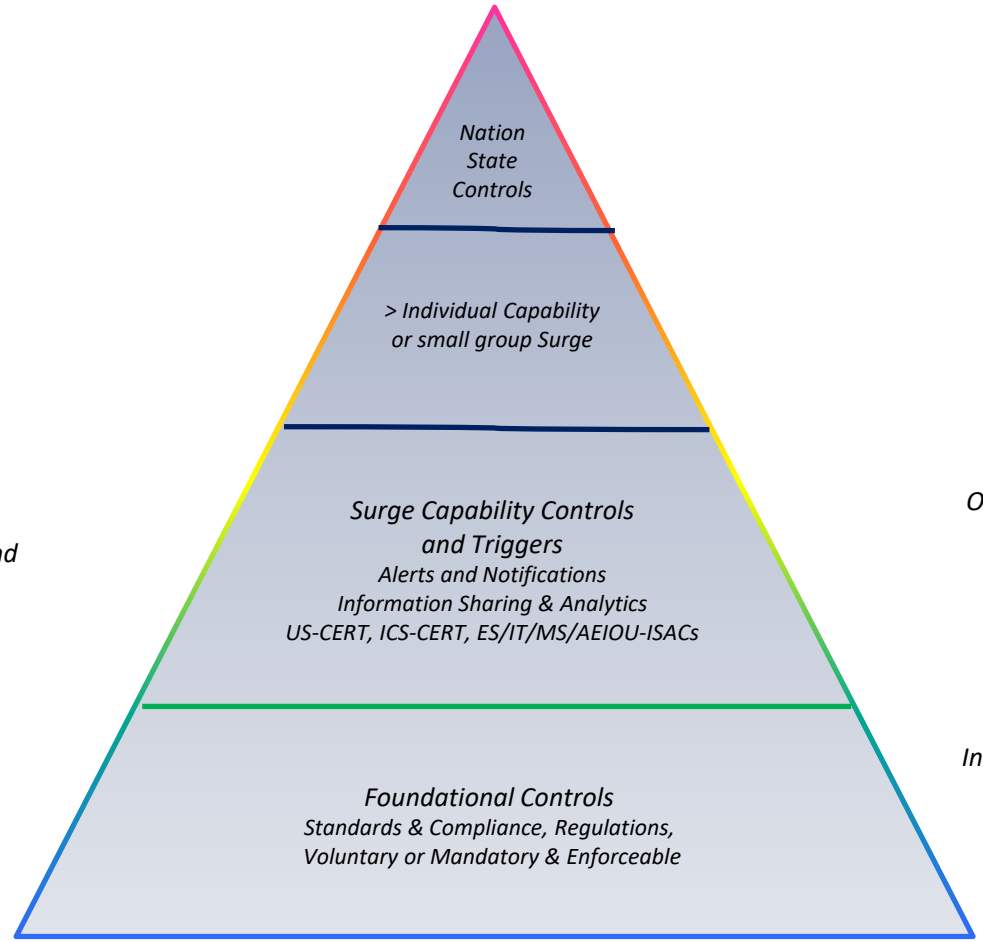
National, Regional

Newly Discovered Vulnerabilities and Consequences

Organizational, Regional, National

Vulnerability Consequences

Individual, Organizational, Regional

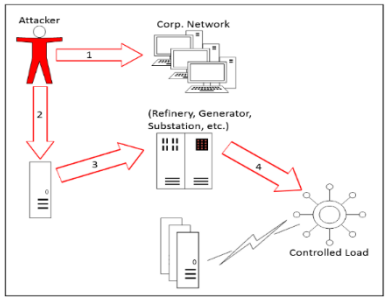


Primary Observations

Present State

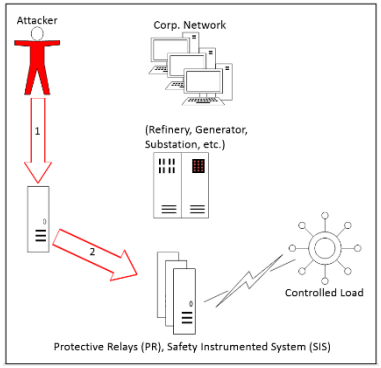
- Many skilled adversaries with interests in Electric Sector
- Many complex relationships
  - Within the sector
    - Federal Regulators and State Regulators
    - GenCo, TransCo, DisCo, ControlCo
  - and between CIKR sectors
    - Electric/Finance/Communications (NIAC Recommendation stress)
- Arguably the largest most complex System on the planet
- Critical Infrastructure is aging
  - Aging Infrastructure being replaced very quickly
    - **New** equipment means **new** attack surfaces
- Information Sharing and Analysis Framework
  - Robust and Growing!!

A Conjecture



Ukraine

1. *Steal credentials*
2. *Access control systems*
3. *Utilize access to affect substation*
4. *Controlled load affected*

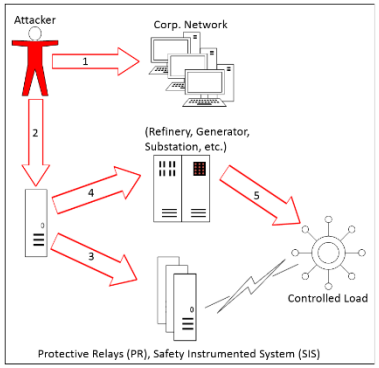


MENA

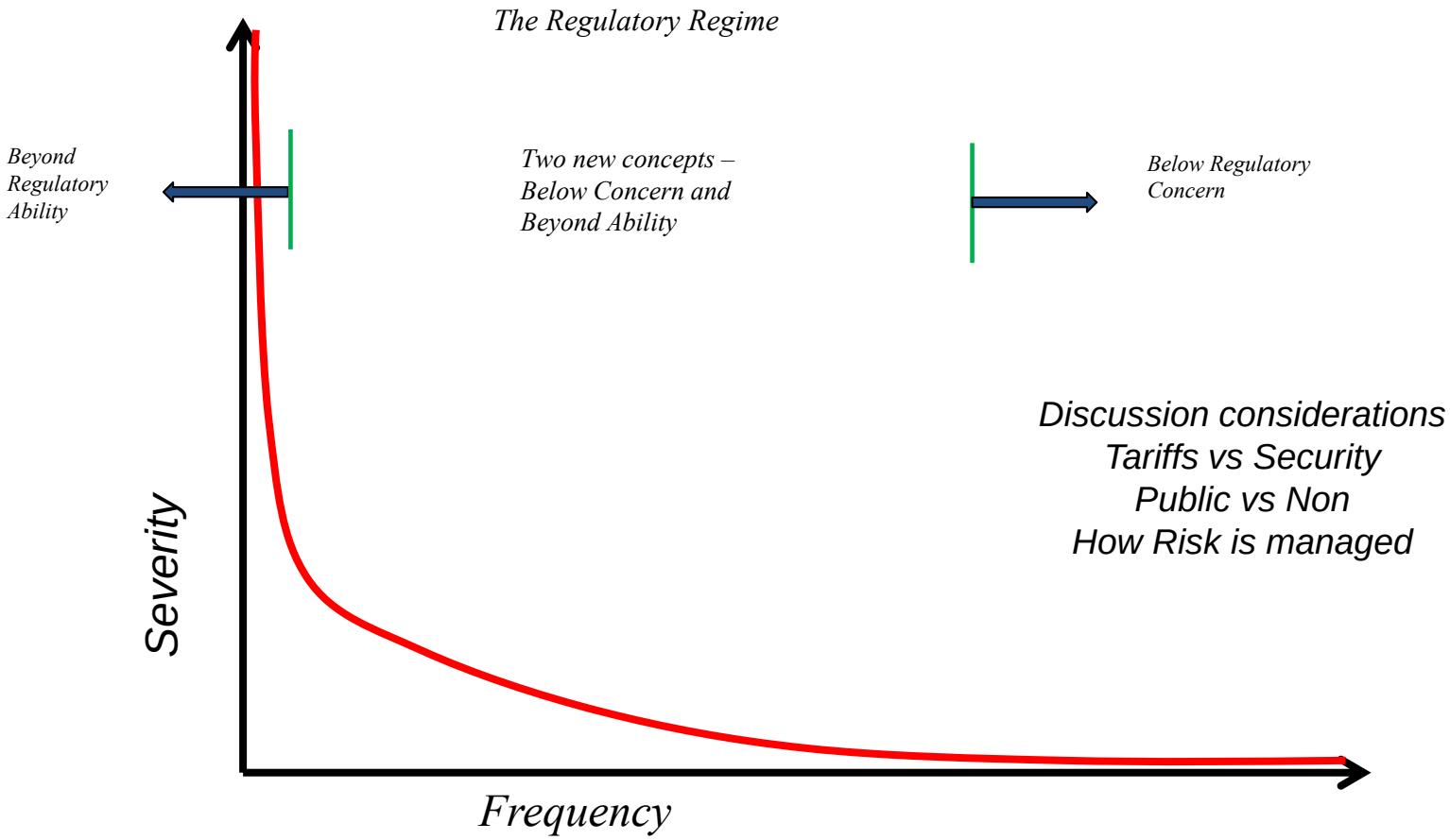
1. *Access OT network*
2. *Utilize access to then access and disable SIS*
3. *Plant responded. Possible goal not achieved*

Conjecture

1. *Steal credentials*
2. *Access control systems*
3. *Utilize access to then access and disable PR*
4. *Utilize access to affect substation*
5. *Controlled load affected*



Concepts for Regulatory Regimes



Discussion considerations
Tariffs vs Security
Public vs Non
How Risk is managed

NARUC Winter Policy Summit

Critical Infrastructure Committee