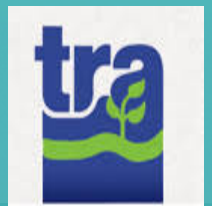
# ICS Cybersecurity: Hype and Reality

Doug Short

Robert M. Lee
Twitter: @RobertMLee
Email: rlee@dragos.com
Web: www.dragos.com




# Who We Are

- CIO and CISO at Trinity River Authority of Texas
- Previously:
  - US Air Force Cyber Operations Officer
  - US Air Force Communications (IT) Officer

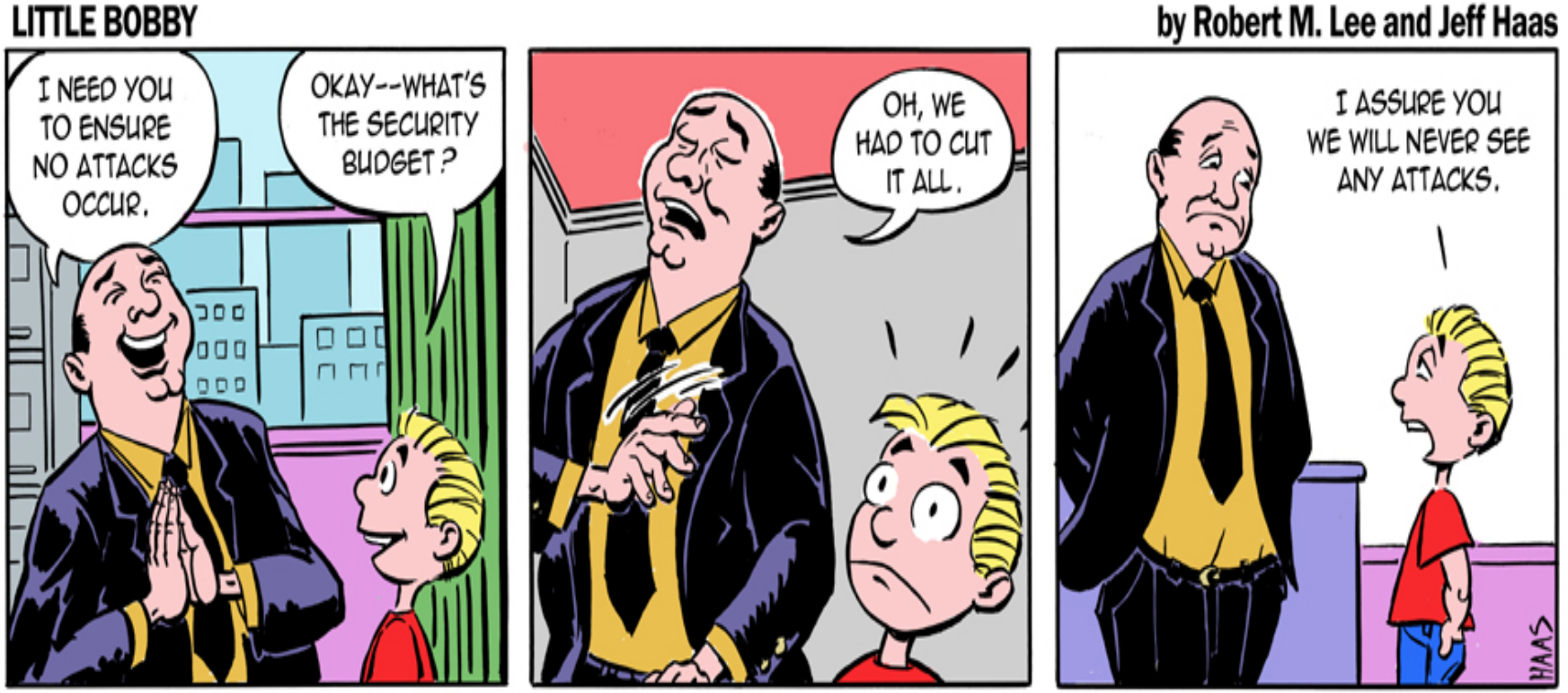
Email: shortd@trinityra.org

- CEO and Founder of Dragos, Inc
- SANS Institute Course Author (ICS515 & FOR578)
- Non-resident National Cyber Security Fellow at New America
- Previously:
  - US Air Force Cyber Warfare Operations Officer
  - US Intelligence Community

# Agenda

- Media Hype and Reality of SCADA Cyber Threats
  - Sliding Scale of Cyber Security
- Trinity River Authority Experiences
  - Case-Study: Broadcast Storm
- Strategic Intelligence for Guidance
  - Case-Study: CRASHOVERRIDE
- What Executives Should be Asking

# Media Hype and Reality of SCADA Cyber Threats

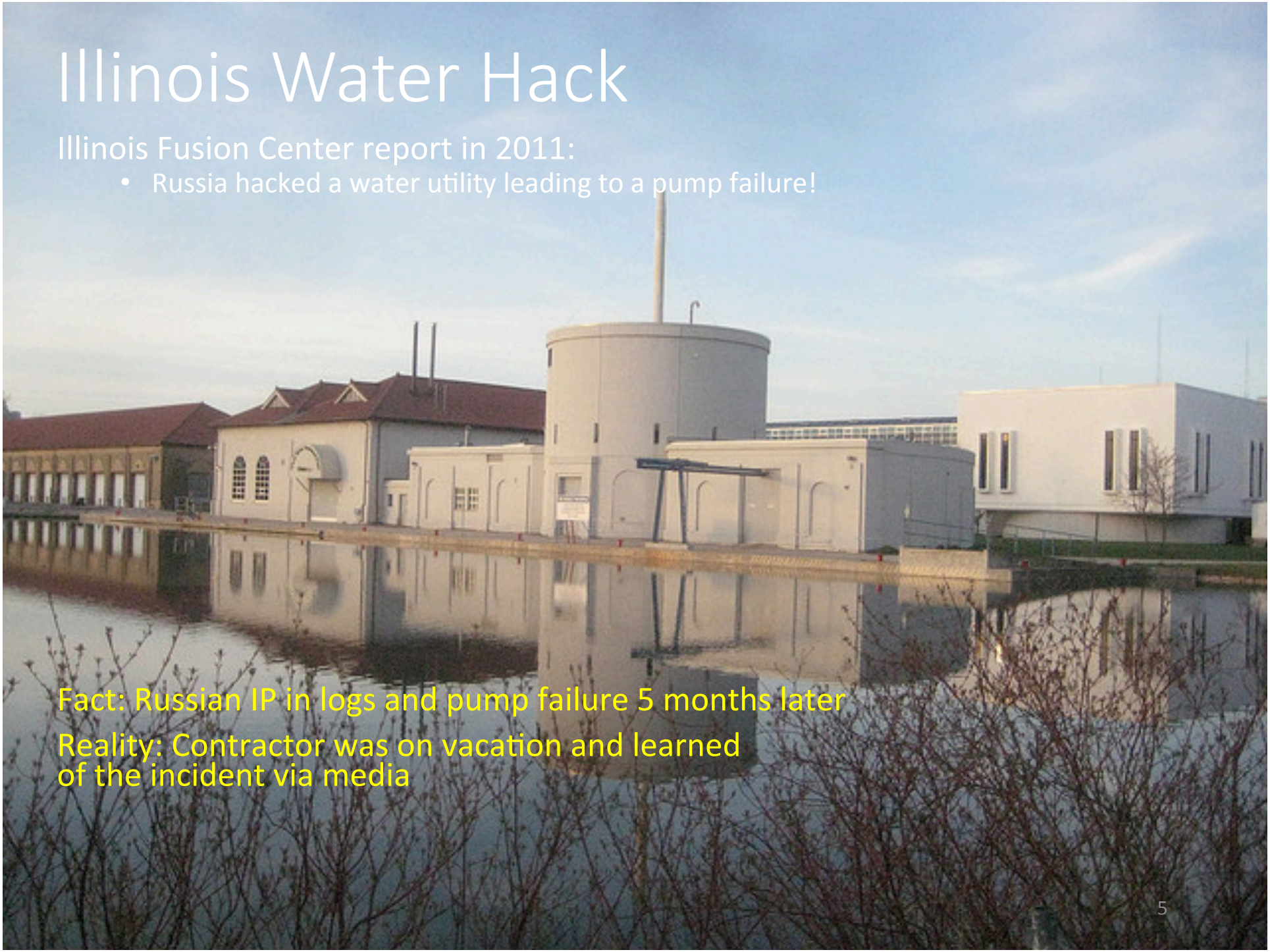



@_LittleBobby_
www.LittleBobbyComic.com

# Illinois Water Hack

Illinois Fusion Center report in 2011:

- Russia hacked a water utility leading to a pump failure!

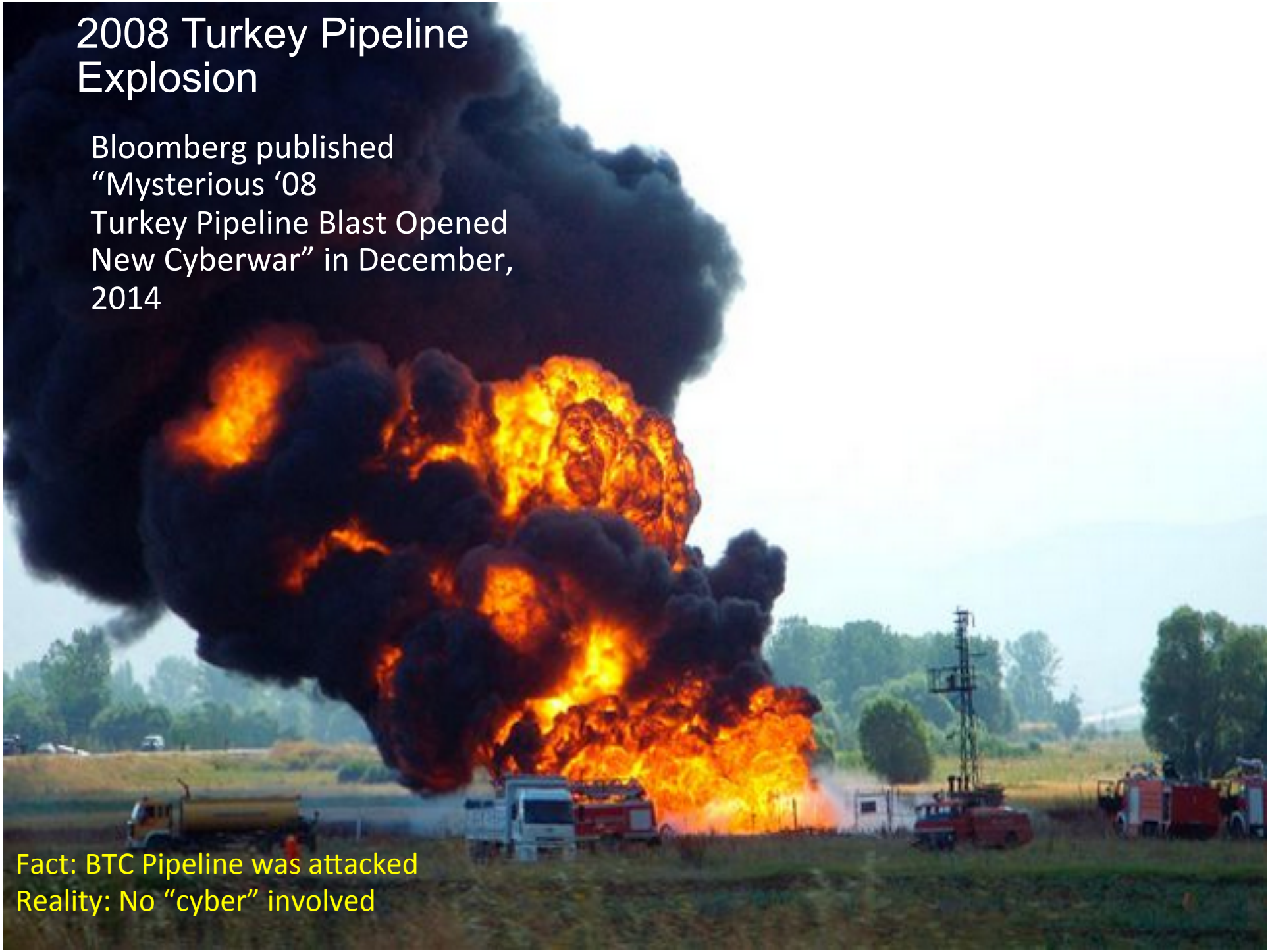


Fact: Russian IP in logs and pump failure 5 months later

Reality: Contractor was on vacation and learned of the incident via media

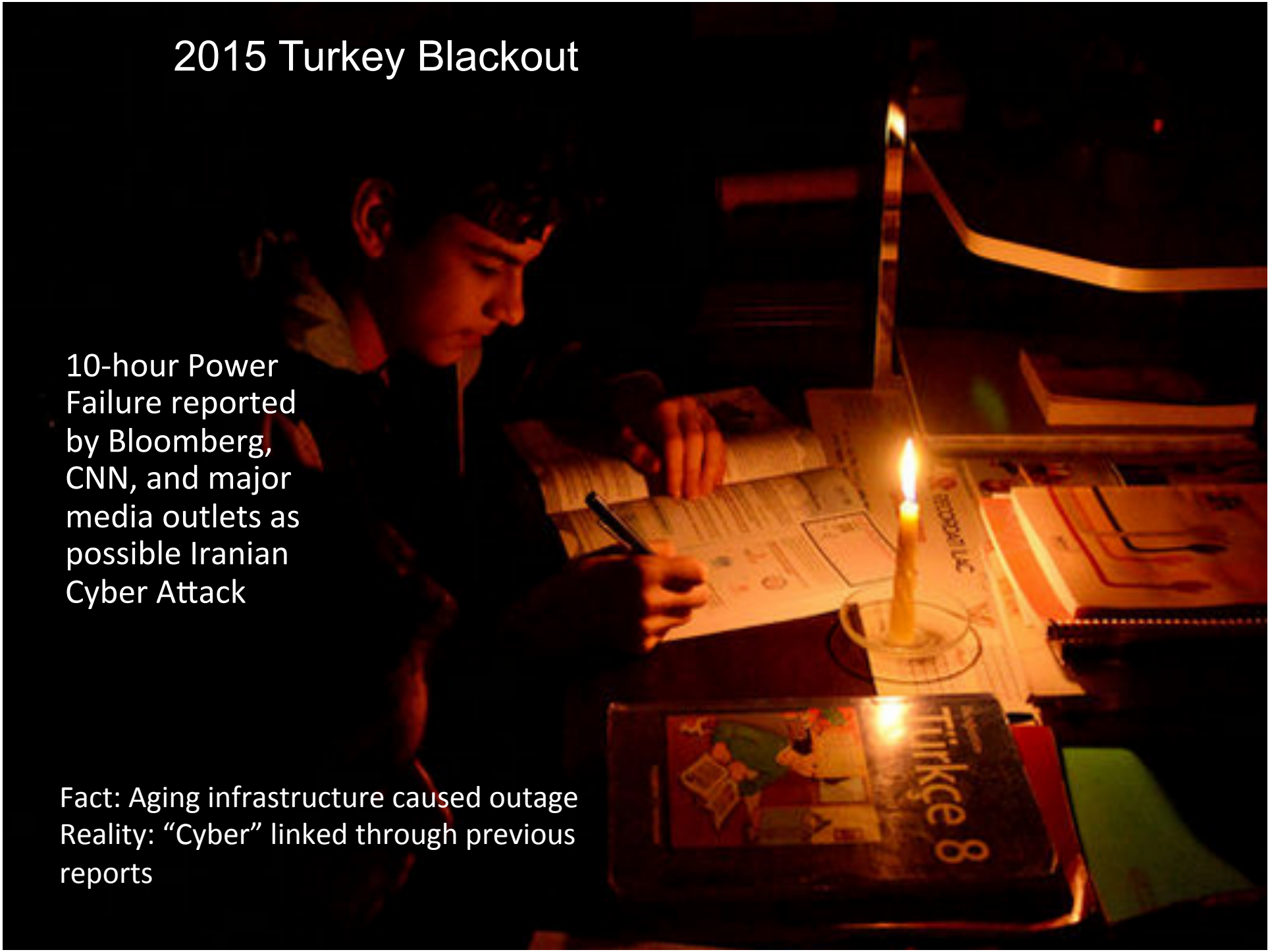
# 2008 Turkey Pipeline Explosion

Bloomberg published "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar" in December, 2014



Fact: BTC Pipeline was attacked
Reality: No "cyber" involved

# 2015 Turkey Blackout




10-hour Power Failure reported by Bloomberg, CNN, and major media outlets as possible Iranian Cyber Attack

Fact: Aging infrastructure caused outage
Reality: “Cyber” linked through previous reports

# Different Types of Incidents and Actors

**Thrillseeker**

**Criminal**


**Nation-State**

**Hacktivist**

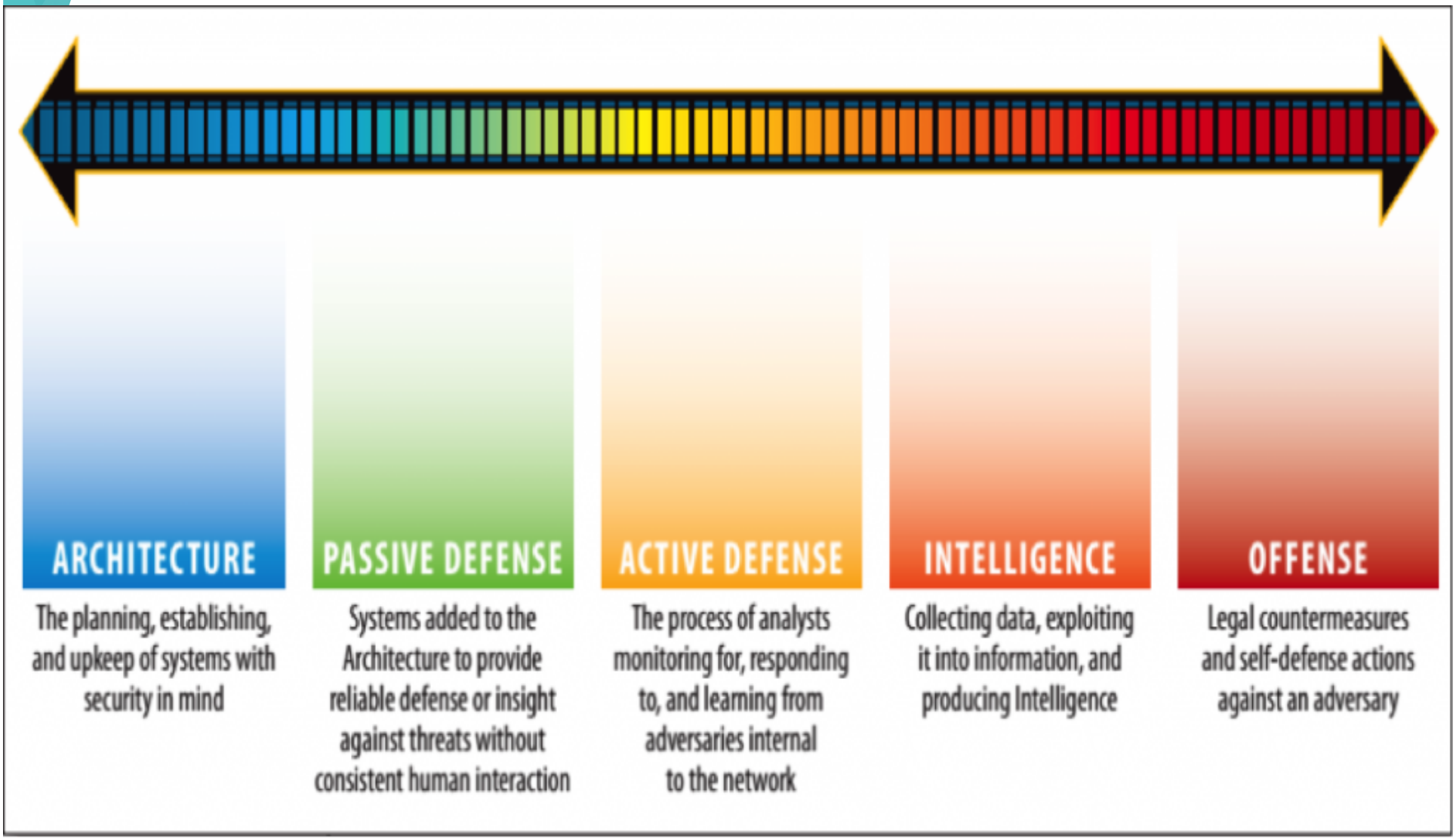

**Terrorist**

# Different Types of Incidents and Actors

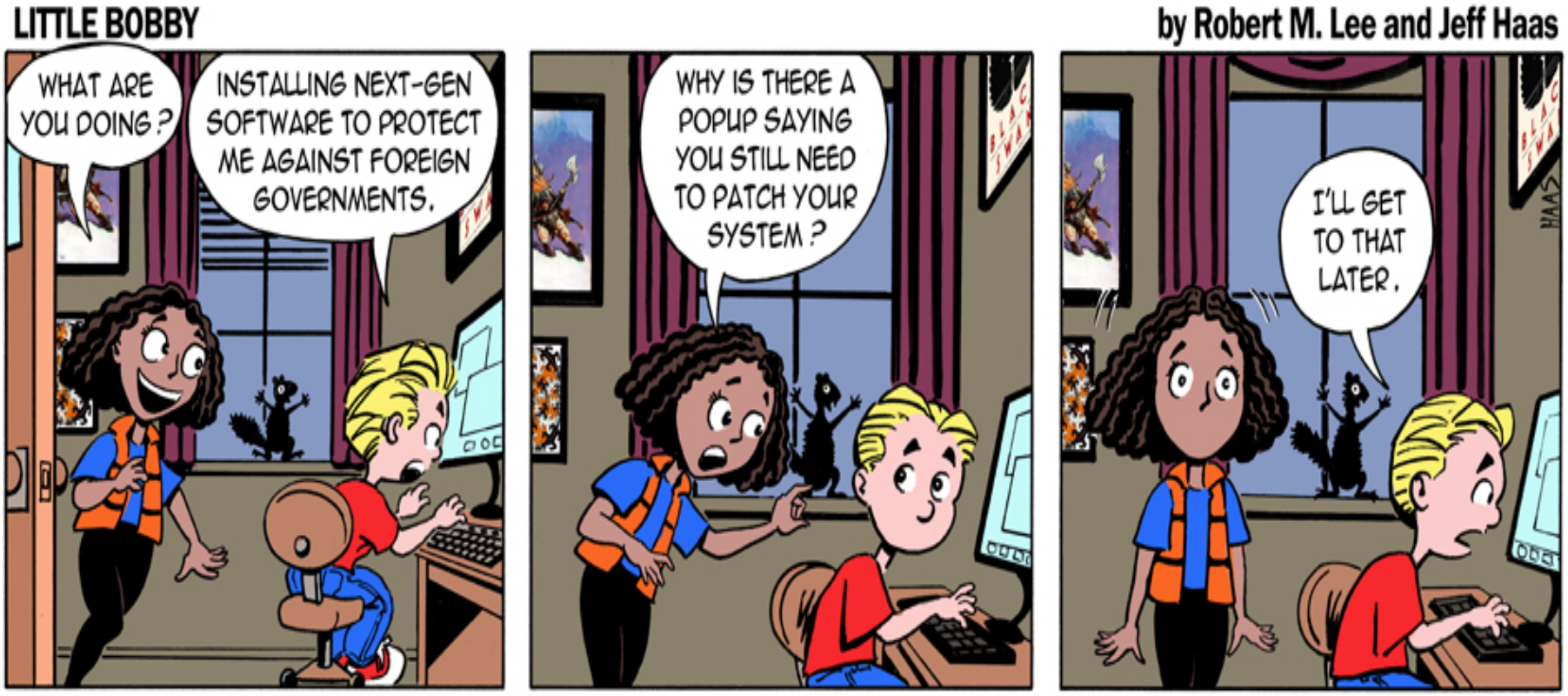
**Disgruntled Employee**

**Well-Meaning Employee**

# The Sliding Scale of Cyber Security



# Trinity River Authority Experiences



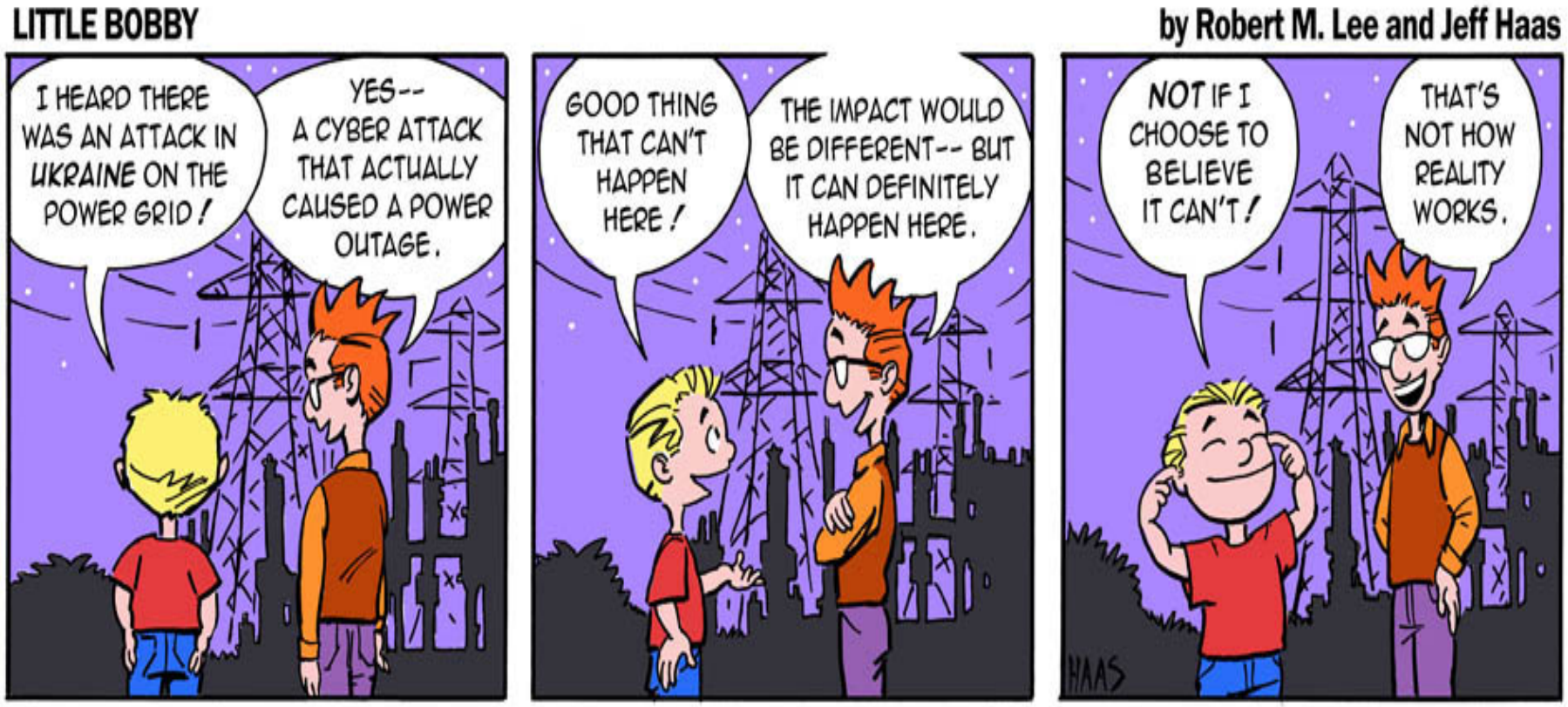
# A Real World Example

- 0800 – Planned power outage for construction project
- 1200 – Power restored; soon followed by comm failures; Operations Center down; Plant initiates manual operations
  - Troubleshooting begins with Contractor
- 72 hours and $15K in unplanned labor cost
  - After Action Report reveals a series of cascading failures
    - D-Link switch
    - PLC battery power
    - Updated documentation
    - No diagnostic capability



The importance lies in the effects generated and timely mitigation… The action and actors are secondary.

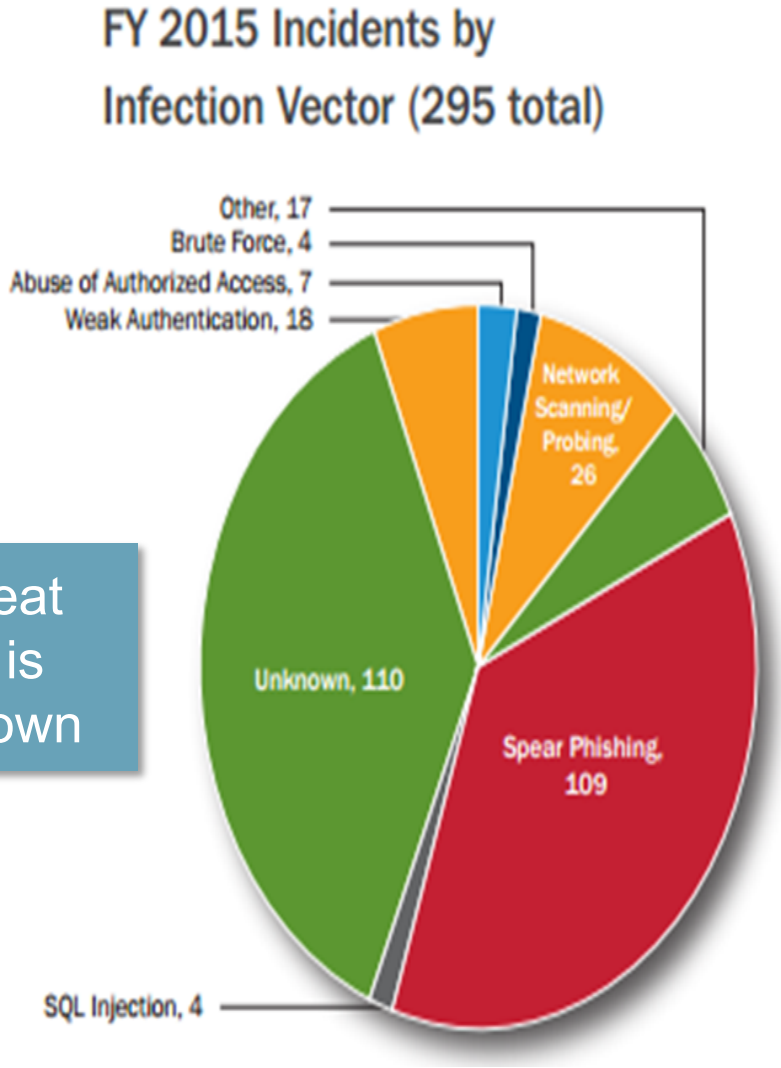
# Strategic Intelligence for Guidance



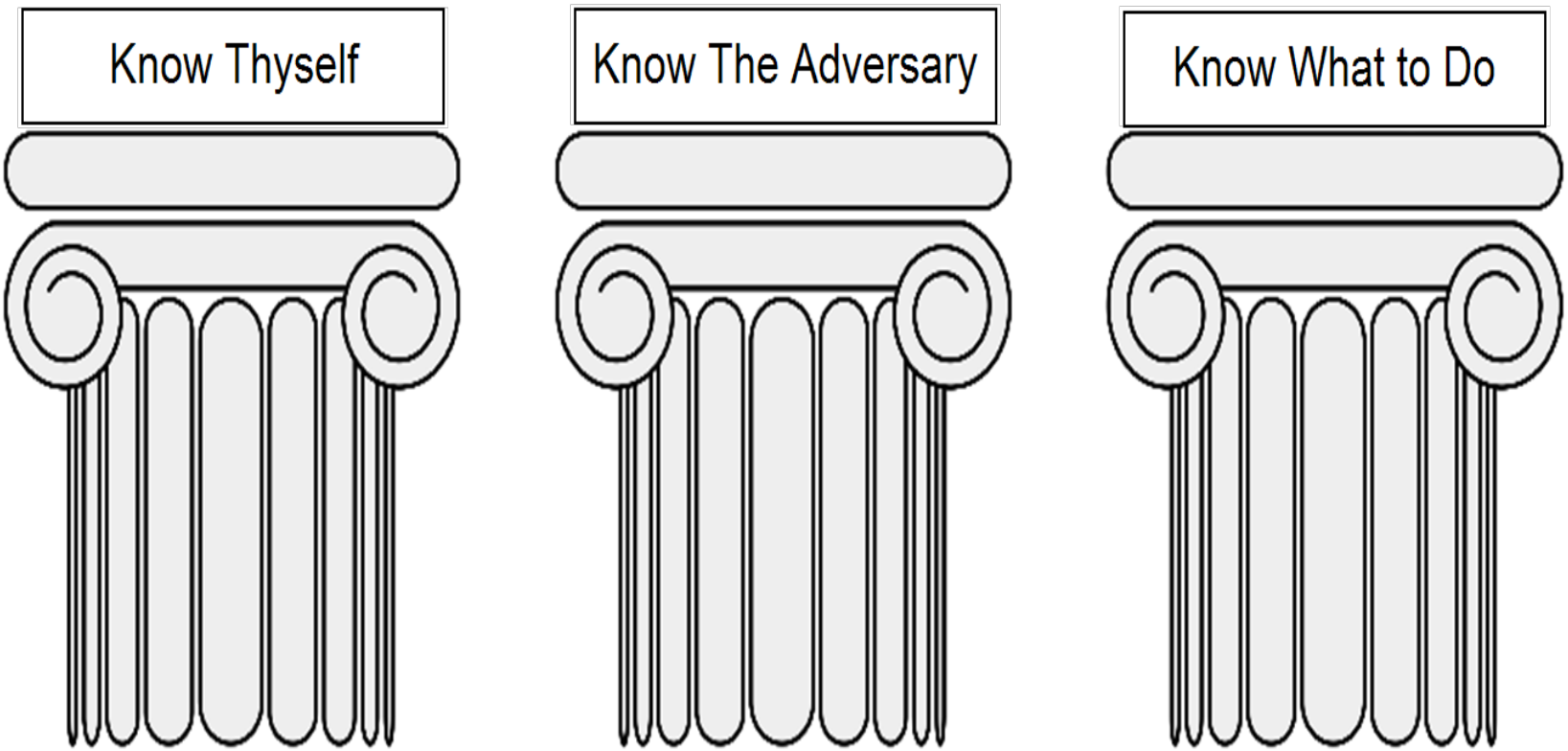
# Overarching Problem

Few People Know How to Protect the ICS that Run Our World

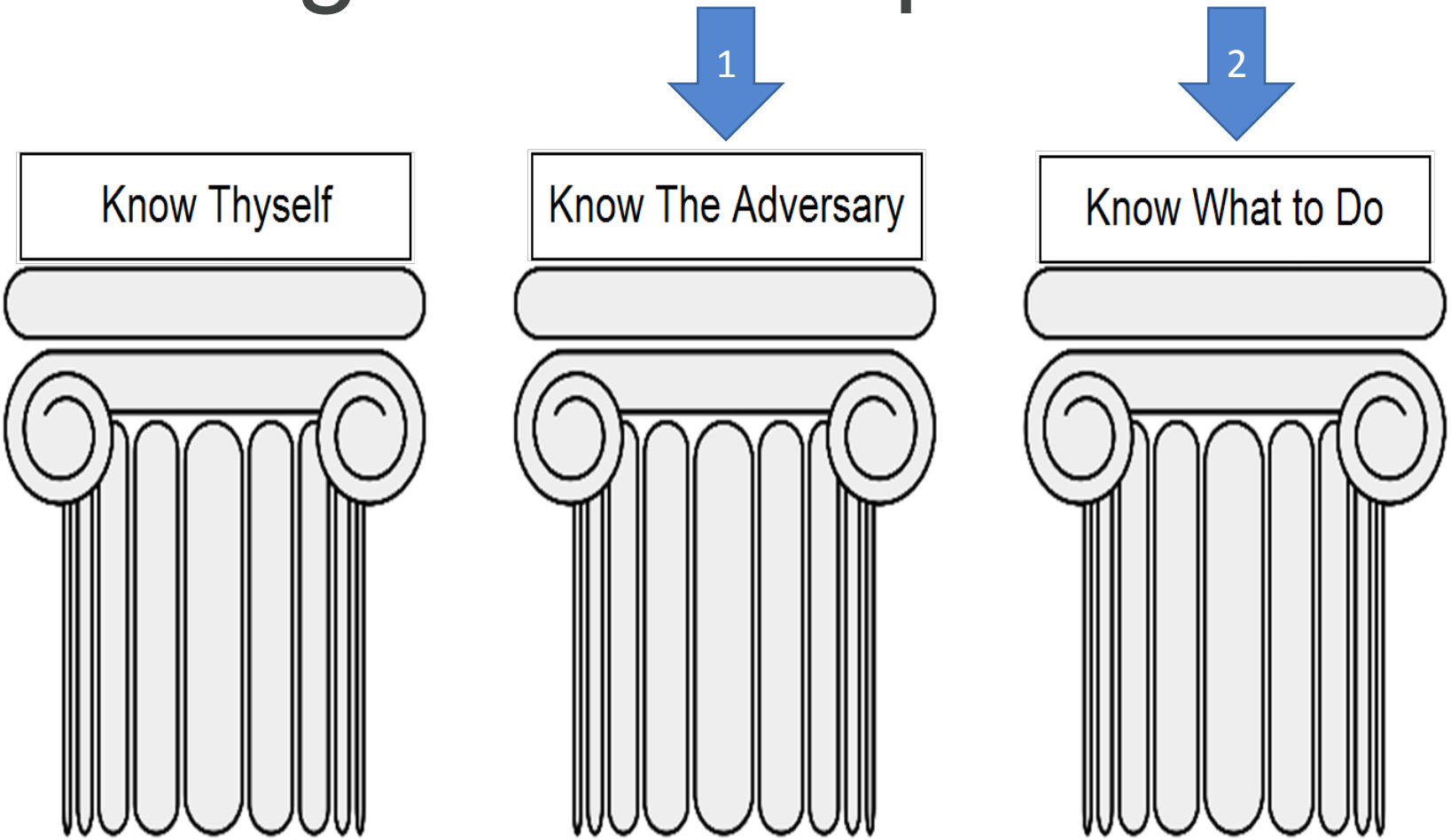

And the Threat Landscape is Mostly Unknown



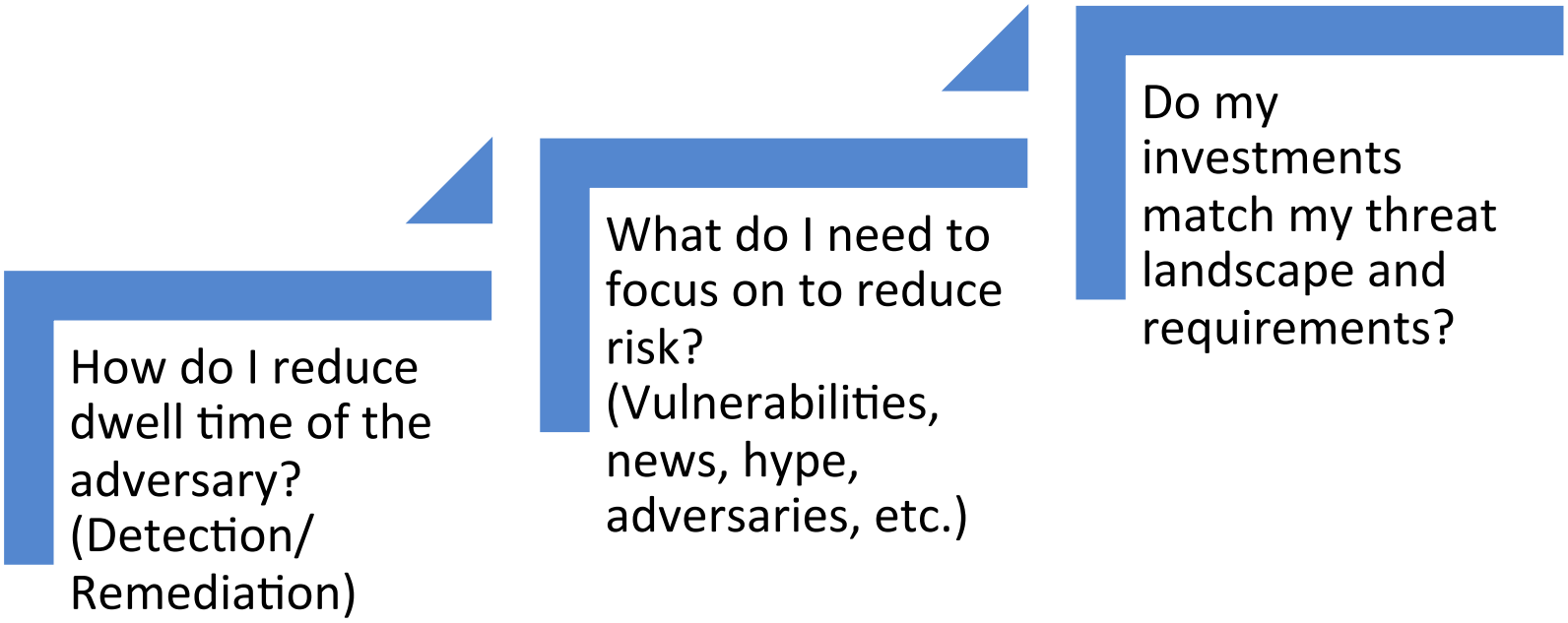
# The Three Pillars of Security



# Intelligence's Purpose



# What Intelligence Should Provide

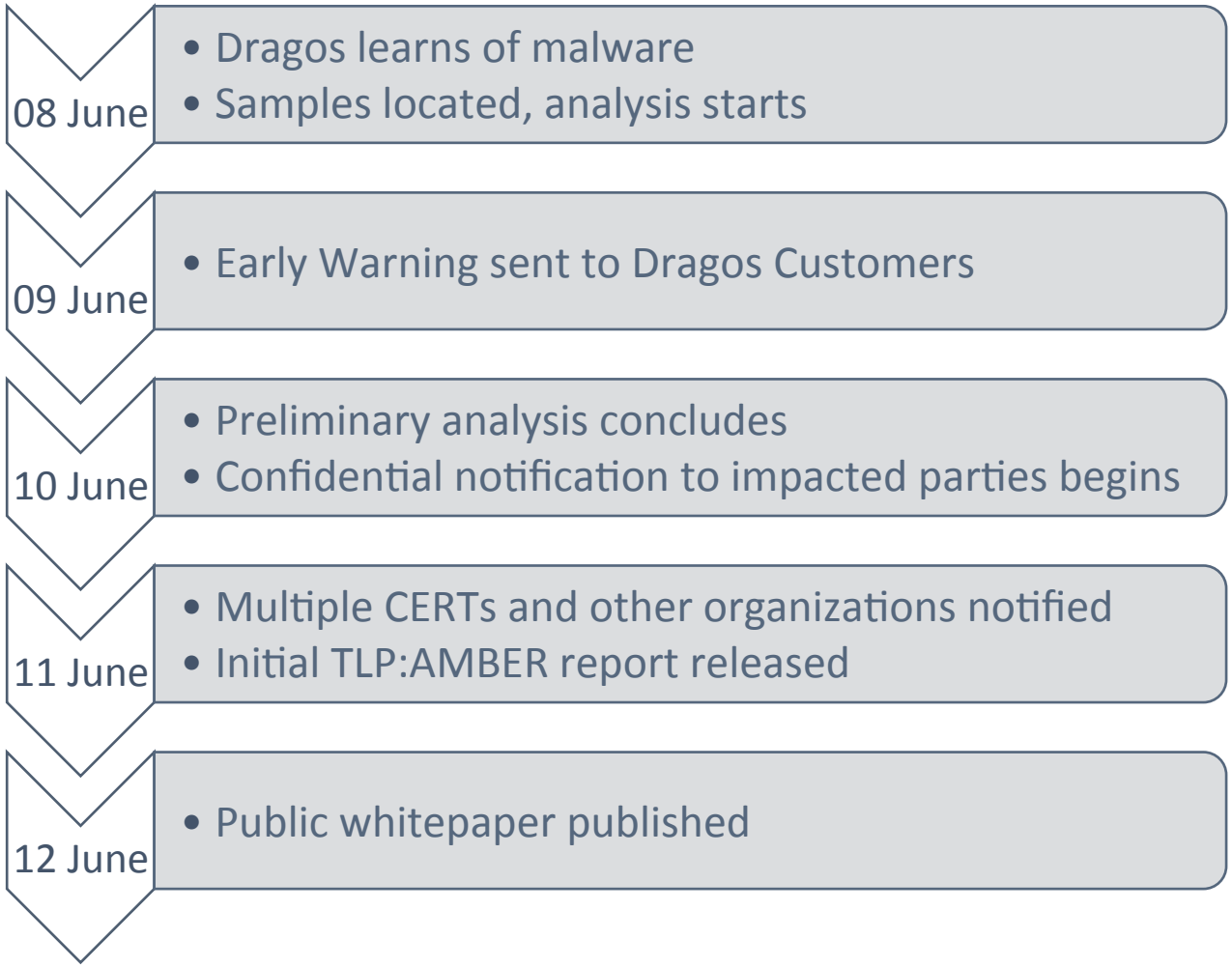


# Ukrainian Power Outage

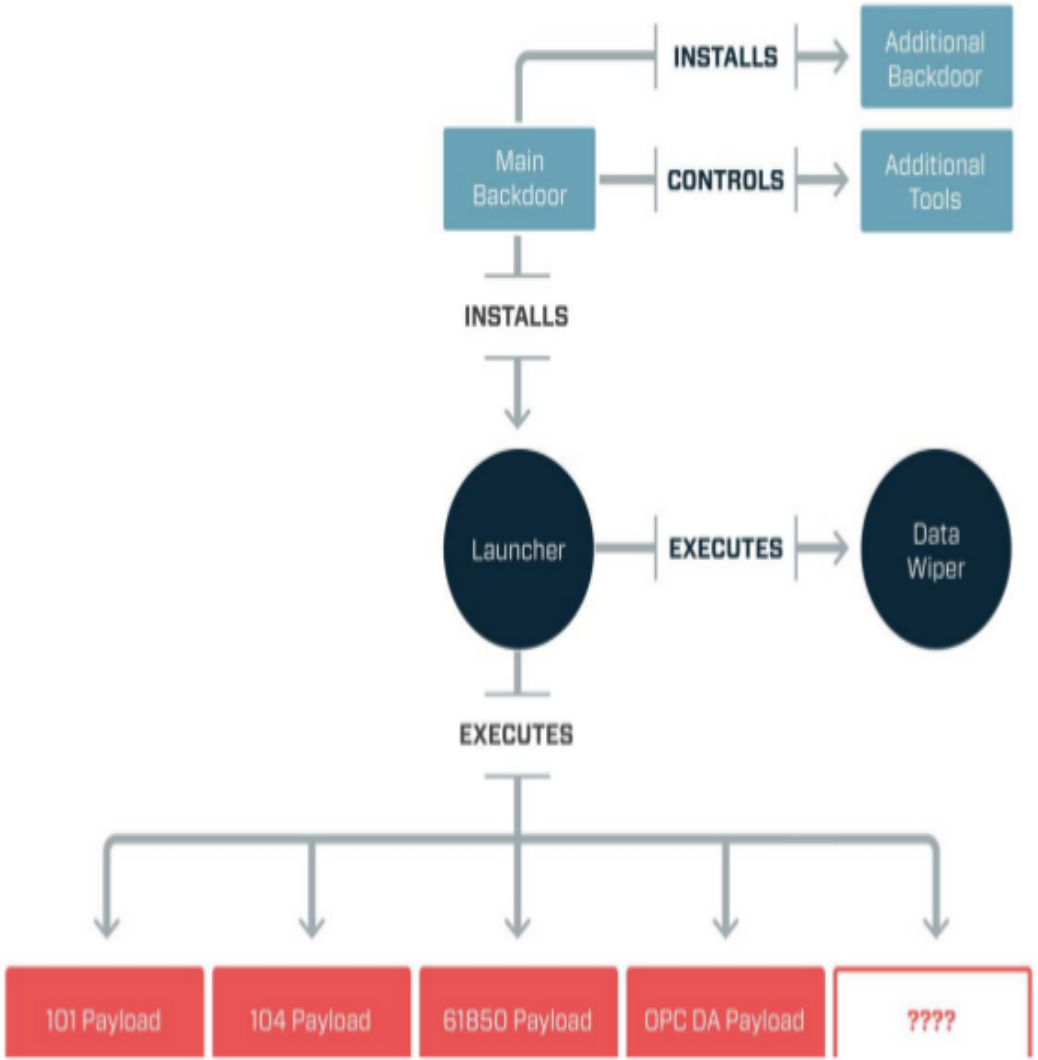

17 Dec 2016, 23:53 Local Time:

- Ukrenergo substation de-energizes
- Resulted in outage for service area
- Utility transferred into manual mode
- Began restoring power in 30 minutes

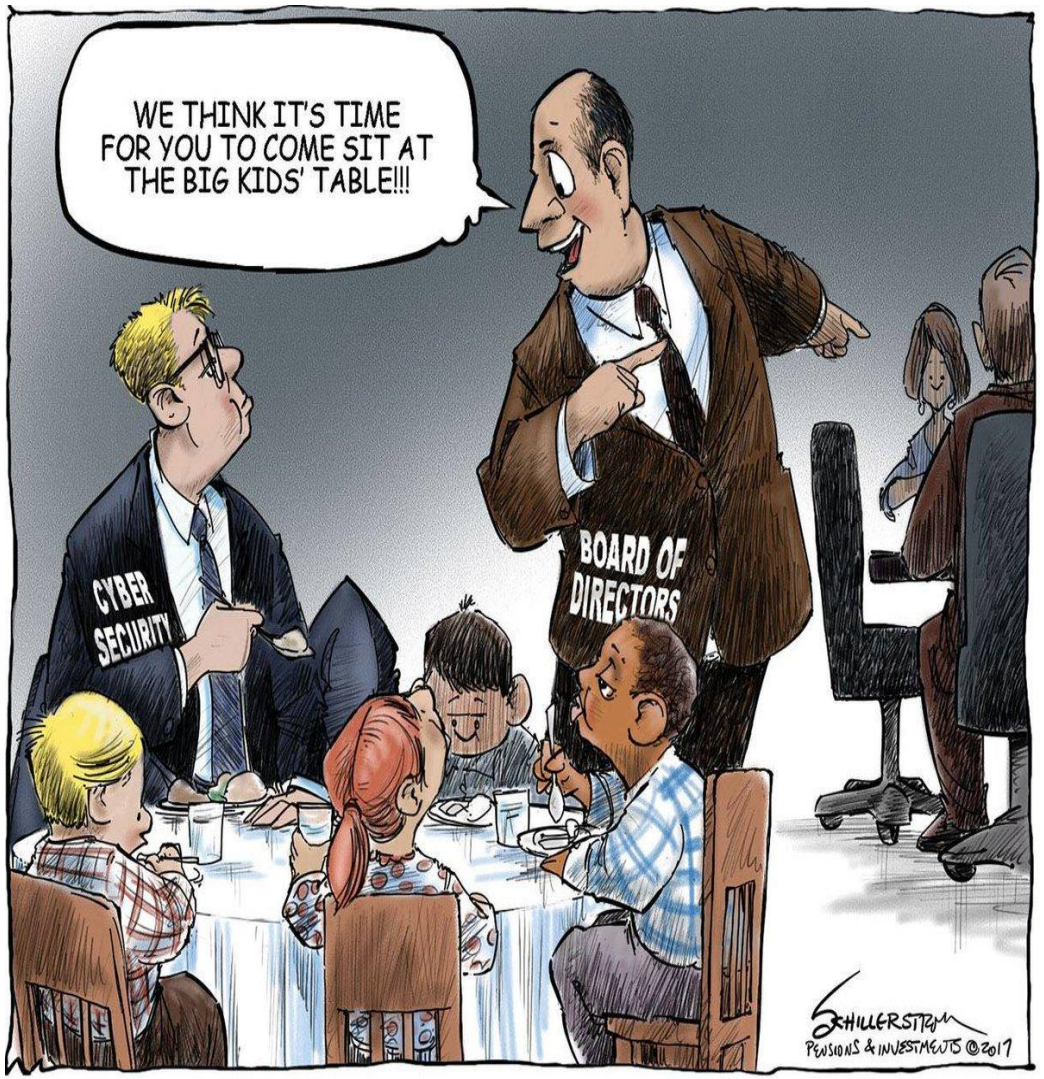
# Dragos Timeline



# CRASHOVERRIDE Framework



# The Executive Perspective



# It's Always a Management Problem!

# Questions?

Doug Short
Email: shortd@trinityra.org

Robert M. Lee
Twitter: @RobertMLee
Email: rlee@dragos.com
Web: www.dragos.com


DRAGOS