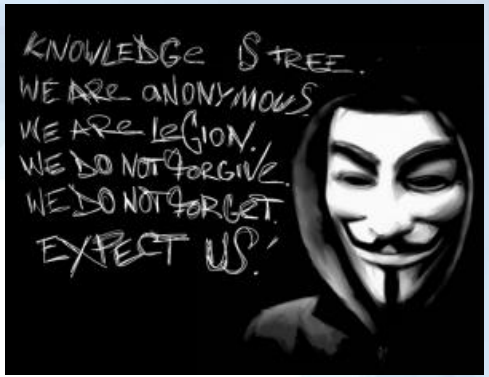
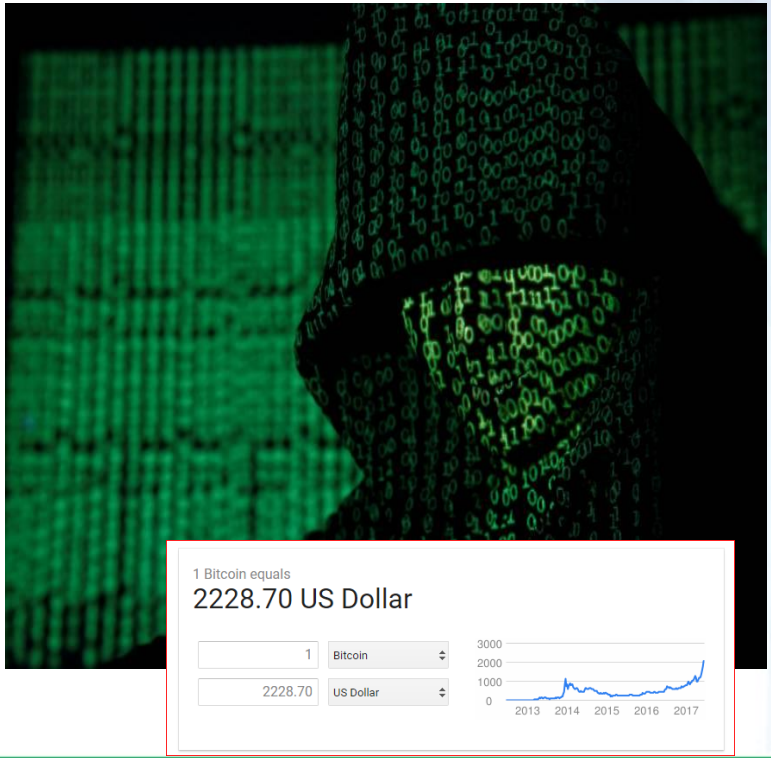
# Cyber Crime & Terrorism

## What are the threats & vulnerabilities today?

## What are we doing about it?




# WannaCry Ransomware Attack




- Started on Friday, 12 May 2017,
- 230,000 computers in 150 countries
- $300 in bitcoin within 3 days or $600 within 7 days
- Worst-hit countries were Russia, Ukraine, India and Taiwan

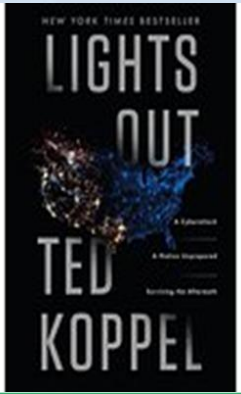
# WannaCry Ransomware Attack

# Lights Out?

## Power Grid Threats & Vulnerabilities

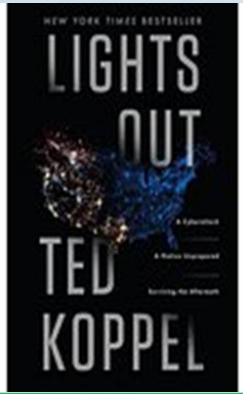
# *Lights Out?* : Key Takeaways

1. Power grids are vulnerable to attacks
   - Cyber attacks on SCADA systems
   - Physical attacks
   - EMP
2. Resiliency regulations complicated
3. Range of impacts resulting from cyber attacks on power grids: damaged power lines, persistent widespread blackouts, enormous equipment replacement costs
4. Industry & government disagree about risk
5. Frequency of cyber attacks on all businesses is increasing



# *Lights Out?* : Key Takeaways

6. **Attacks could come from world powers or extremist groups**
7. Plans for disaster response incomplete, impractical, and unknow to citizens
8. Information on preparation for a disaster and sustained outage is scarce and incomplete
9. Segments of the population are preparing



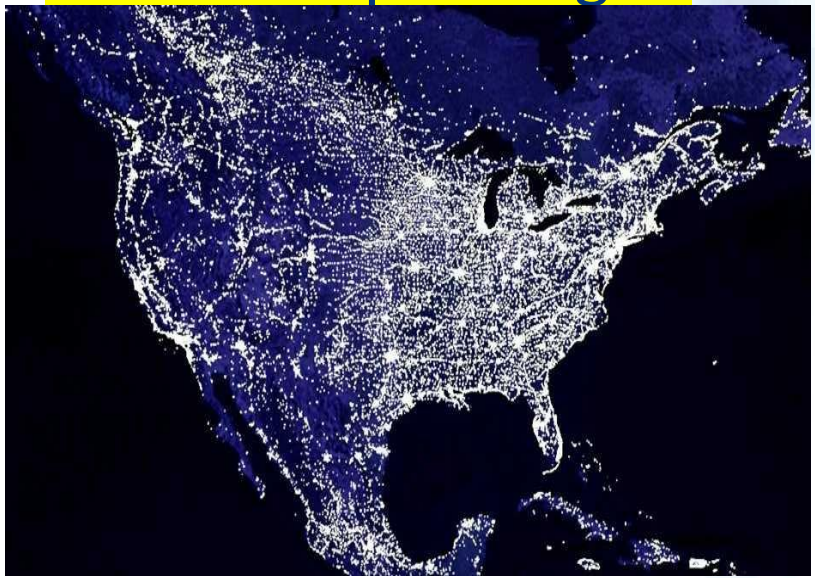
# Are power grids *truly* vulnerable?

- **Case in point #1 : Stuxnet**

**Malicious computer worm, first identified in 2010, that targets industrial computer systems (ICS – SCADA) and was responsible for causing substantial damage to Iran's nuclear program.**

**The worm is believed by many experts to be a jointly built American-Israeli cyberweapon, although no organization or state has officially admitted responsibility.**

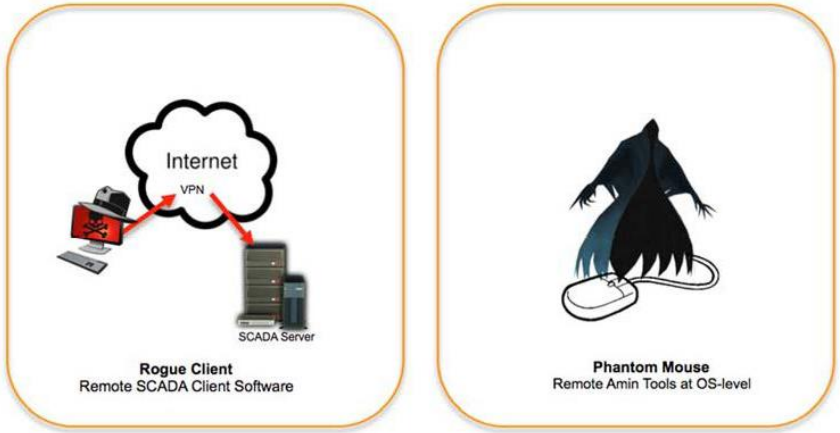
- Stuxnet – targeted centrifuges not the power grid, but …
- The same ***type*** of attack ***could*** take out a power grid



# Are power grids *truly* vulnerable?

- **Case in point #2 : Ukrainian Power Grid**

## SCADA Hijacking Techniques



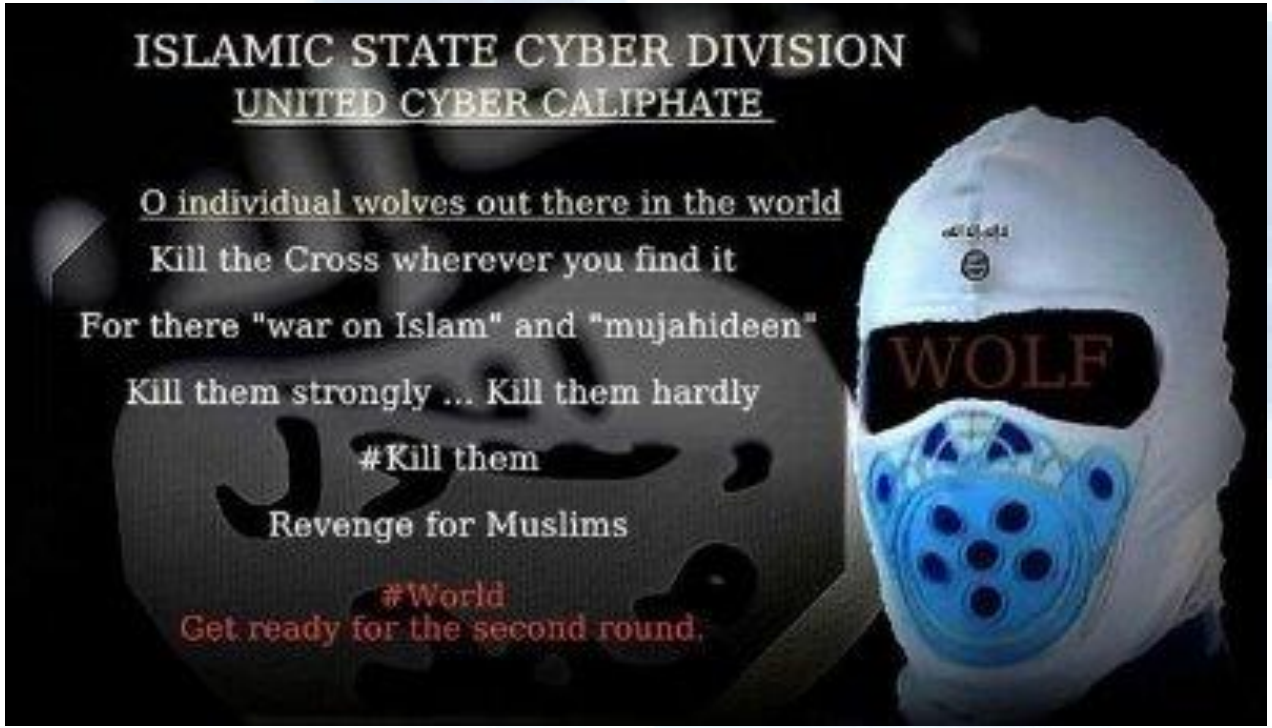

The attackers develop two SCADA Hijack approaches (one custom and one agnostic) and successfully used them across different types of SCADA/DMS implementations at three companies

# Cyber-terrorism: Threats to Individuals & Organizations

- **Does ISIS have cyber capability?**
- **Is ISIS a serious cyber threat?**
- NEVER under estimate anybody or anything
  - That makes over a million USD a day
  - That will DIE to make a point

# Cyber Terrorism: Threats to Individuals & Organizations

- **Caliphate Cyber Army (CCA) formerly Islamic State Hacking Division or United Cyber Caliphate**

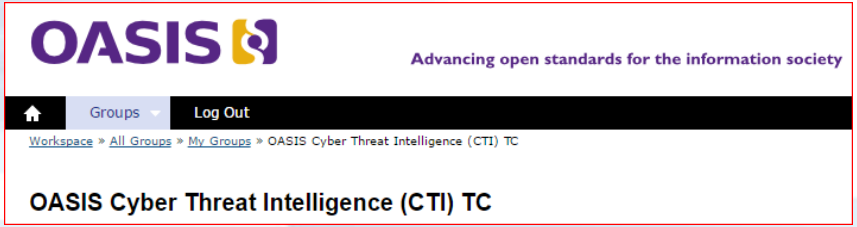


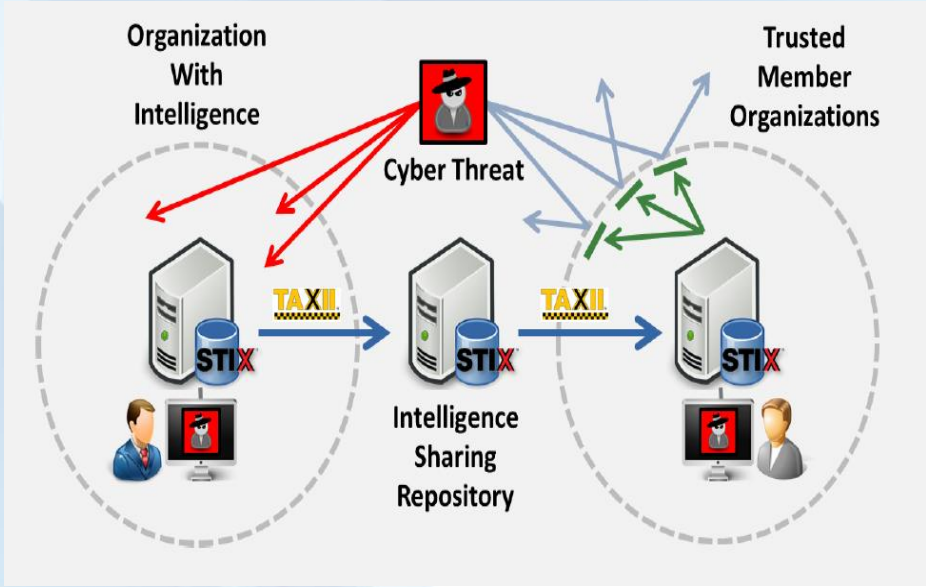
# Cyber Threat Intelligence Standards

- Trusted Automated Exchange of Indicator Information (TAXII)
- Cyber Observable Expression (CybOX)
- Structured Threat Information Expression (STIX)

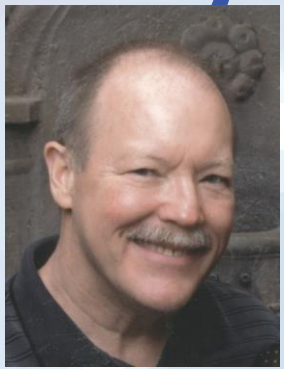
They are an open community driven effort and a set of free, available specifications that help with the automated exchange of cyberthreat information.

Reference: OASIS Cyber Threat Intelligence (CTI) TC
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti



# Thank you!




**Dave Darnell**

***Systrends***

CEO/CISO/Founder

CISA CISM CISSP BSIE MBA PE

1001 E. Warner Road, Suite 102

Tempe, AZ  85284

www.systrends.com

Phone: 480.756.6777x201

Mobile: 602.432.3353

eFax: 480.383.6591

email: david.darnell@systrends.com

LinkedIn: https://www.linkedin.com/in/dave-darnell-53110


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~