RSAConference2017
Abu Dhabi | 7–8 November | Emirates Palace

POWER OF OPPORTUNITY

SESSION ID: CCT-T09

Cyber Insecurity: Unique Threats in the Middle East and the Need for Collective Defense

Jamil N. Jaffer
Founder
National Security Institute – George Mason University
@jamil_n_jaffer

Key Worldwide Cyber Threat Trends

Rapid Technology Change

- IoT + Smart Devices + Connected Devices

Communications Explosion

- Massive Increase in Quantity + Speed + Criticality

Cyber as an Element of National Power

- Key Actors Conducting Deliberate Attacks
- Key Actors Looking to Establish Long-Term Footholds

Economic Effects

- Business + Individual Losses

Growth in Attack Surface and Speed

Attack Surface is Growing Rapidly

- Global IP traffic: **2.3 zettabytes** in 2020 (**95x increase** since 2005)
- Wireless and Mobile Devices: **66% of total IP traffic** by 2020

Attacks Happen Fast

- 98% of breaches took attackers **minutes or less** to compromise systems
- Average time from breach to obtaining administrative rights: **3 days**

Defenders are Slow

- In 68% of cases, victims took **weeks or longer** to identify breach
- Median time from breach to discovery of breach: **99 days**

Massive Losses Worldwide

Companies are Suffering Huge Losses

- Cost of cybercrime estimated at **$6 trillion in 2021** (up from $3 trillion in 2015).
- Business email losses of **$5.3B+ in last 3 yrs**. (up 2,370% from 2015-16)
- Ransomware losses of **$5B+ in 2016 alone** (up from $325M in 2015)
- **7.1 billion identities** exposed in **last 8 years** (1.1B in ‘16 vs. 564M in ‘15).
- **IP theft is rampant; billions of dollars a year in economic + non-econ losses.**
- Destructive attacks are on the rise.

Major Cyber Attacks

Monetary Theft:

- Bangladesh Bank (2016)
- Odinaff (2016)

Data Theft:

- Experian (2017)

Critical Infrastructure:

- Ukrenergo (2015)

Intellectual Property Theft:

- Worldwide (ongoing)

Broad Range of Attackers

- Nation-States
- Hacktivists
- Criminal syndicates with resources
- Small groups with key capabilities

Destructive Attacks:

- Las Vegas Sands (2014)
- Sony (2015)
- Regional Gov’ts (2017)

Media Focused Efforts:

- Ukraine (2015)
- United States (2016)

Ukrenergo – 2015

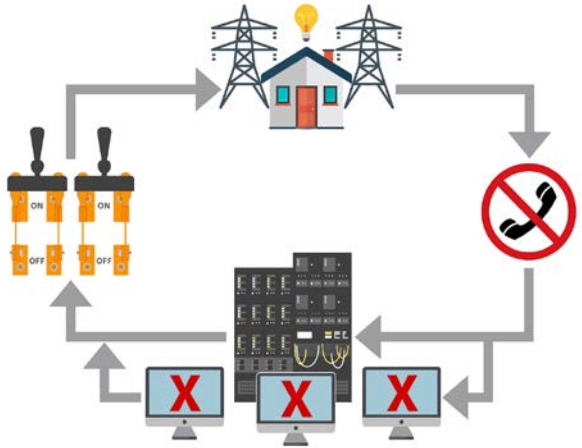
Ukraine Blackout:

- December 23rd, 2015: half the homes in a region w/ 1.4 million residents left w/o power.

Operation Highlights:

- Extensive phishing attacks to gain access.
- Traverse the network into OT systems
  - Operations disrupted at substations
- Telephone DDoS attack.

This is the first known instance of a cyberattack being directly involved in a blackout and coordinating multiple phases/effects



Sony Pictures – 2015

Attack Vector:

- Spear-phishing emails + compromised passwords (brute force + pass-the-hash)

Access:

- UPnP to identify devices + SMB worm to spread + altered host firewall allowing inbound connections

Action:

- 11,000 files exfiltrated + exposed → emails + financial documents + four movies + 47,000 unique Social Security Numbers
- Wiper destroyed data → $35 million in remediation

SONY PICTURES

Las Vegas Sands – 2014

Reconnaissance:

- Initial probing activity
- Brute force password attack on VPN at slots casino in PA

Access:

- Web dev server breached
- Obtained password access – open source tool

Command and Control:

- Live, interactive attack

Action:

- Data exfiltrated + malware bomb written in Visual Basic → overwrite hard drives and reboot

Unique Challenges Facing the Middle East

Regional Challenges

- Evolving Economics
- Population Dynamics
- Dynamic Political + Security Situation

Rapid Growth in Technology

- Central Economic Role
- Speed of Evolution v. Security
- Government + Privately Funded Efforts

Asymmetric Environment

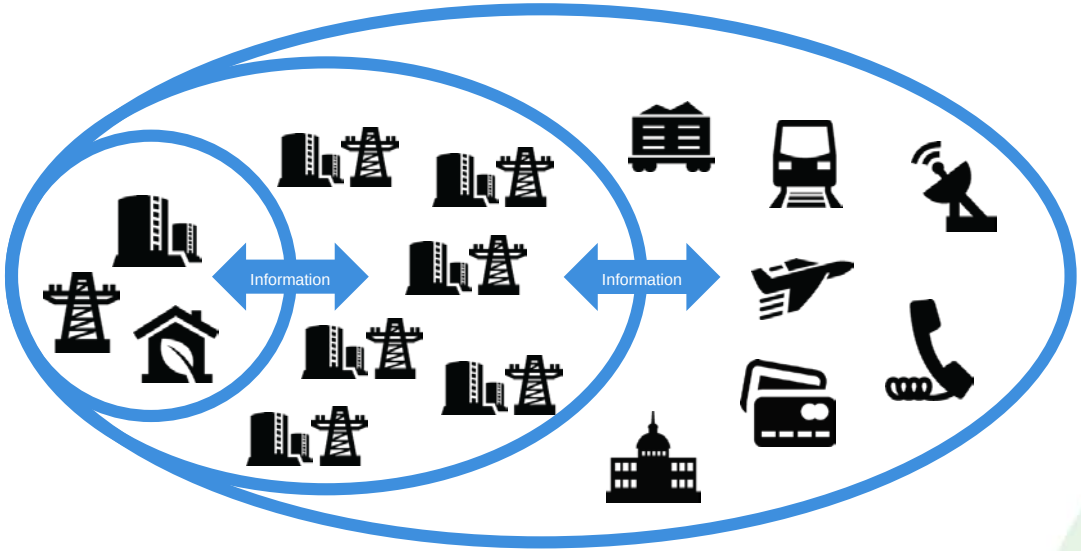
- Increasing Use of Cyber in Region
- External Actors

Need to Defend Nations + Region

- Public-Private Interactions
- Regional Interactions

Collective Defense: Industry – No Sector An Island

- Massive commercial attack surface
- Comprehensive approaches needed: speed and response
- Threat sharing is key: models + categories of threats
- Network speed sharing can enhances collective security



Collective Defense: Government Efforts

- Overall government cyber hardening
- Focused, limited regulatory environment for industry is key
- Employing carrots, not sticks
- Provision of direct government assistance to industry
- Regional collaboration

Collective Defense: Public-Private Partnerships

- Government access to information + understanding of national threat
- Private sector view into threats confronting industry
- Cross-training of public-private teams
- Interoperable systems + joint exercises

Key Lessons Learned

Prior Attacks

- Ease + speed of access → administrator privileges → action
- No such thing as an air gap + real IoT/OT threat vector
- Diversity helps; not panacea + threat growing; less deterrable

Collective Defense

- Central role of both government and industry
- Importance of appropriate government regulation
- Criticality of public-private relationships + regional efforts