# The Challenge of Cyber Security Threats

Eric Cowperthwaite

Vice President, Security & Strategy

Core Security

CORE SECURITY

# Emergency Preparedness Is Tough

- Terrorism
- Natural Disaster
- Insider Threats
- Technology Failures
- Crime
- Cyber-Security

# Some Lessons Learned

- 9/11 and Data Centers
- 9/11 and Internet
- Katrina and Data Centers
- Katrina and Sustainability
- Fukushima Reactors

# Converging Disasters: December, 2007

# Hackers: Not All The Same

- For Profit
- Nation State
- Hacktivists
- Terrorists

# Cold War Era: Siberian Pipeline

Contrived computer chips (would make) their way into Soviet military equipment, flawed turbines were installed on a gas pipeline, and defective plans disrupted the output of chemical plants and a tractor factory.

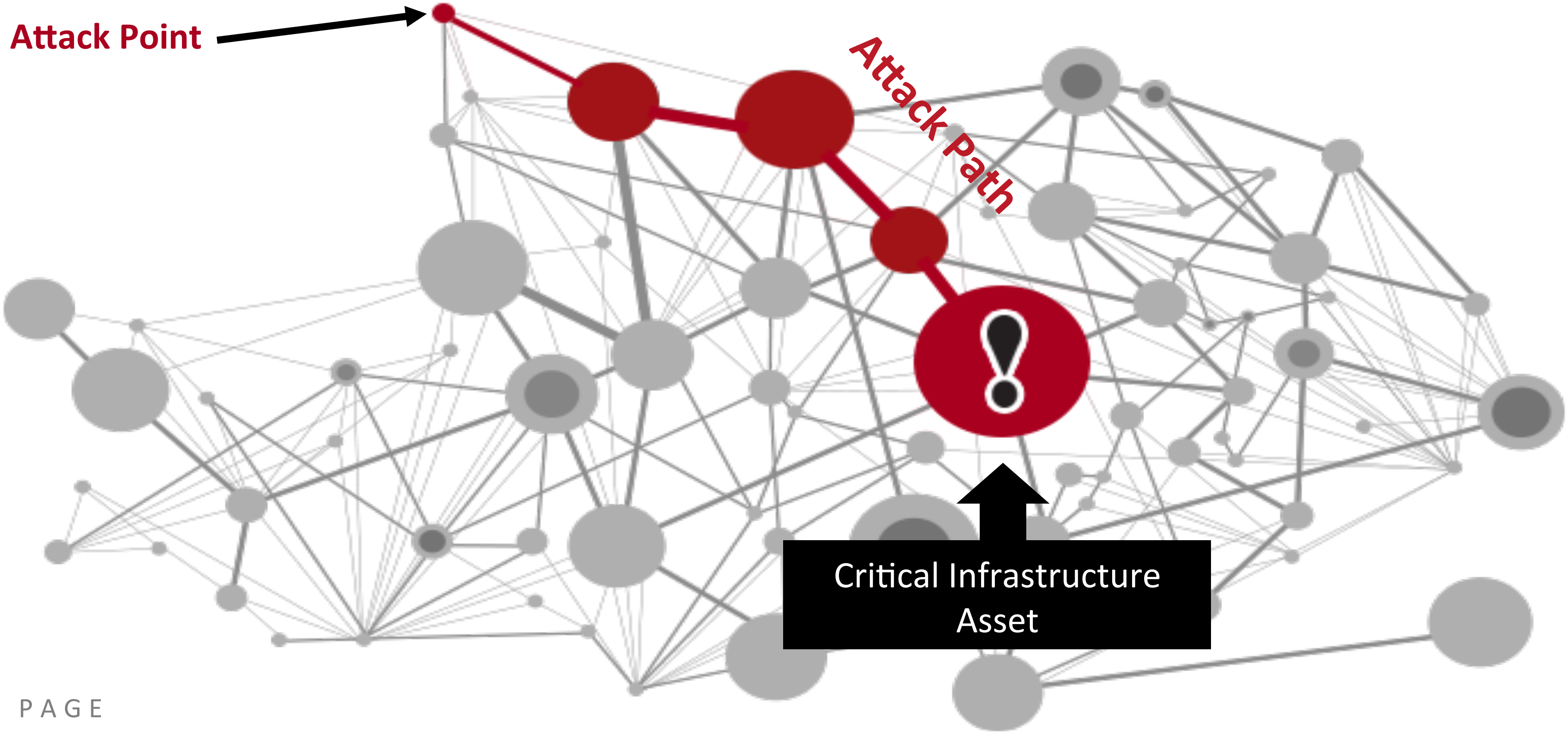
# Modern Era: Stuxnet

- Transmitted by USB flash drive
- Exploited flaws in Siemens controllers
- Targeted Iran specifically

# Cyberthreat #1: The Distraction

- For Profit Bad Guy
- Malicious Software introduced into network
- Opportunistic Attack
- Distraction from real emergency

# Cyberthreat #2: The Main Event



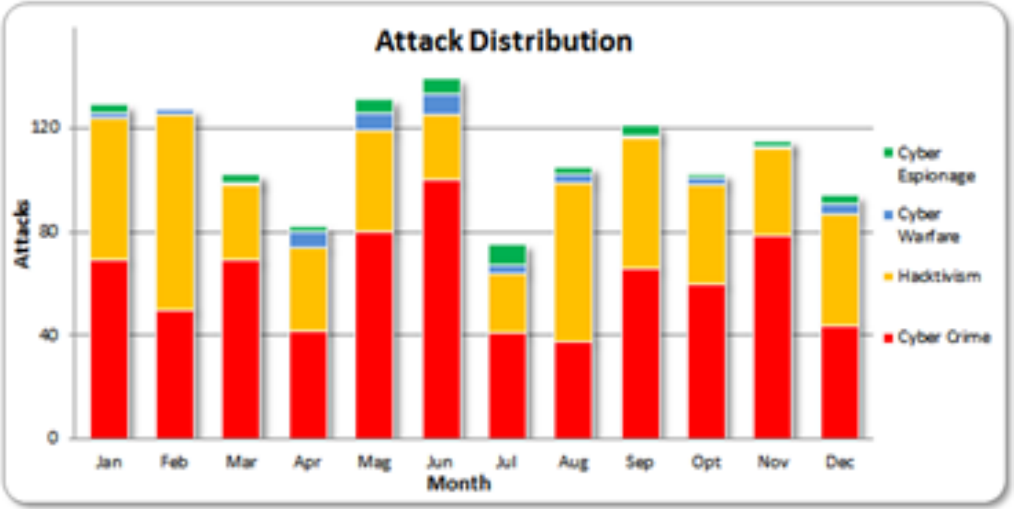
Attack Point

Attack Path

Critical Infrastructure Asset

# Cyberthreat #3: Hacktivism

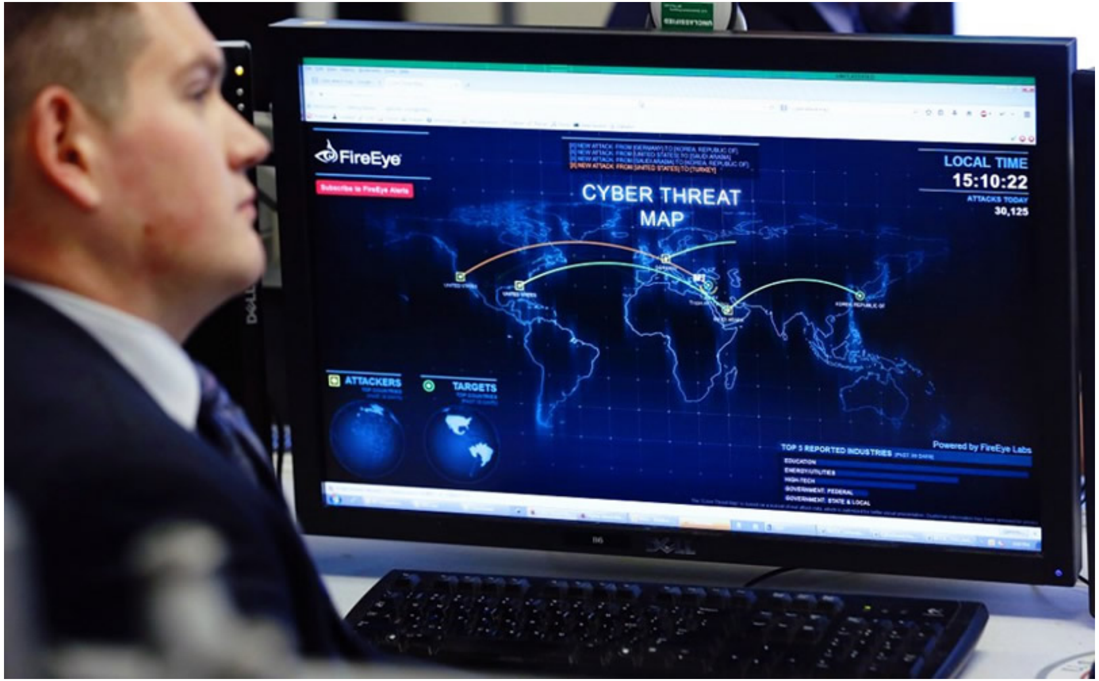
- Trying to “change the world”
- Often focused on headline events
- Many different attack types
- Targets have included Global1000, governments, churches, hospitals, more



Known Cyber Attack Distribution, 2012

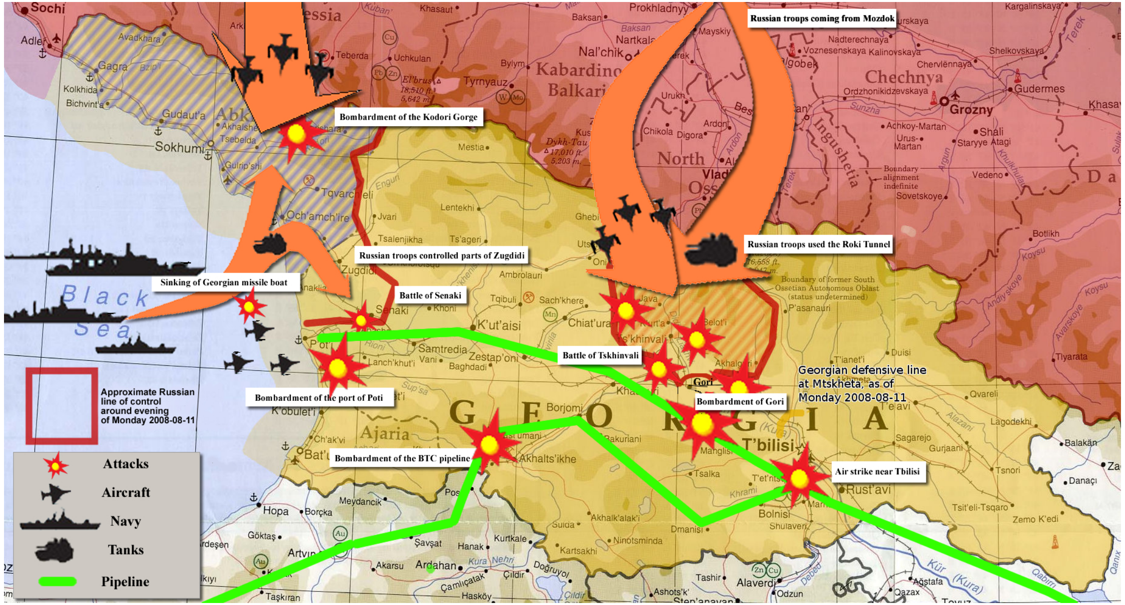
# Cyberthreat #4: The Nightmare Scenario

- Converged Attack
- Coordinated across the physical and cyber spectrum
- Disrupts communications, command and control
- Empowers physical attacks



# Is This Real: Russo-Georgia War 2008

- Integrated attack
- Georgian websites attacked and taken down
- Media and communications companies disrupted, unable to report news
- Georgia's access to Internet re-routed through Russian controlled systems
- Georgian oil pipeline SCADA systems attacked



Russian troops coming from Mozdok

Bombardment of the Kodori Gorge

Russian troops controlled parts of Zugdidi

Russian troops used the Roki Tunnel

Sinking of Georgian missile boat

Battle of Senaki

Battle of Tskhinvali

Bombardment of the port of Poti

Bombardment of Gori

Georgian defensive line at Mtskheta, as of Monday 2008-08-11

Bombardment of the BTC pipeline

Air strike near Tbilisi

🟥 Approximate Russian line of control around evening of Monday 2008-08-11

| | |
|---|---|
| ✹ | Attacks |
| ✈ | Aircraft |
| ⛴ | Navy |
| ■ | Tanks |
| 🟩 | Pipeline |

# Preparing For The Future

- Integrated Defenses and Coordinated Processes
  - Cyber security, IT, Physical Security, Law Enforcement
- Resilient Capabilities
  - Multiple types of communication
  - Electronic systems able to resist denial of service attacks
- Prepared for electronic intrusion
- Computer Downtime Plans
- Table top exercises
- Increase staff skills