Threat: Nature and Magnitude of EMP Threats Within the Next 15 Years

- EMP is one of a small number of threats that may
  - Hold at risk the continued existence of today’s US civil society
  - Disrupt our military forces and our ability to project military power
- The number of US adversaries capable of EMP attack is greater than during the Cold War
- Potential adversaries are aware of the EMP strategic attack option
- Threat not adequately addressed in US national and homeland security programs

Vulnerability may be an invitation to attack

- Wide area coverage
  - A million square miles
- Intensity depends on:
  - Weapon design
  - Height of burst
  - Location of burst
- Broad frequency range
- Threat to all electronics in exposure
The Vulnerability and Interdependence of US Military and Civilian Systems

- One or a few high-altitude nuclear detonations can produce EMP, simultaneously, over wide geographical areas.

- Unprecedented cascading failure of our electronics-dependent infrastructures could result:
  - Power, energy transport, telecom, and financial systems are particularly vulnerable and interdependent.

- Both civilian and military capabilities depend on these infrastructures.

- Without adequate protection recovery could be prolonged—months to years.
What is EMP?

- **Electro Magnetic Pulse** is a burst of electromagnetic radiation from an explosion or a suddenly fluctuating magnetic field.
- **EMP from a nuclear explosion** high above the atmosphere.
- **EMP from a solar storm**.
Types of EMP

- **E1 Pulse** – very fast component of nuclear EMP. It is too fast for ordinary lightning protectors and destroys computers and communications equipment.

- **E2 Pulse** – many similarities to pulses produced by lightning. Least dangerous type of EMP because of the widespread use of lightning protection.

- **E3 Pulse** – much slower pulse caused by the Earth’s magnetic field being pushed out of the way by the nuclear explosion or solar storm followed by the field being restored to its natural place. This process can produce geomagnetically induced currents in long electrical conductors (like power lines) which can damage or destroy power line transformers.
Causes of EMP

• High altitude nuclear explosion
  Line of sight effects
  Simple fission bomb more effective than hydrogen bomb

• Geomagnetic solar storm
  Only E3 pulse
Effects of E1 Pulse

- E1 Pulse travels at 90% of the speed of light
- Peaks after 5 - 10 nanoseconds, over in 1 microsecond
- Normal circuit breakers do not work this fast
- Amplitude up to 50,000 volts/meter
- Circuit boards are 1 million times more sensitive than vacuum tubes
- Will cause integrated circuits connected to cables to overheat and give false readings, be damaged or destroyed
SCADA

• Supervisory Control and Data Acquisition (SCADA) systems are electronic control systems that control electrical transmission and distribution, water management and oil and gas pipelines across the United States.

• Tests indicate that the electronics would experience 100 to 700 ampere currents during an E1 pulse, impacting a significant portion of these systems.
Effects of E2 Pulse

• E2 Pulse is very similar to the electromagnetic pulse produced by lightning.

• Because of the widespread use of lightning protection technology, E2 probably is the least dangerous type of EMP.

• Effect would be similar to thousands of lighting strikes hitting power lines simultaneously.

• Damage from E1 Pulse immediately previously could partially degrade lightning protection.
Effects of E3 Pulse

- E3 Pulse lasts from tens of seconds to several minutes
- Produces direct current Ground Induced Currents (GIC) in conductors
- Long distance electrical power transmission lines make excellent conductors
- The longer the conductor and the lower its resistance, the easier the GIC can flow
- Direct currents of hundreds to thousands of amperes will flow into transformers, potentially causing overheating and fires
Nuclear EMP Tests

- **US – Starfish Prime (1962)**
  - 1.44 Mt burst, 250 mi altitude over Johnston Island in the South Pacific
  - 5.6 kv/m E1 pulse in Honolulu

- **USSR – Test 184 (1962)**
  - 300 kt burst, 180 mi altitude over Kazakhstan
  - 1,000 to 1,300 nT/min E3 pulse
  - Power station 300 mi distant set on fire by E3 Pulse effects and destroyed within 10 seconds
  - 2,500 amp current induced in overhead phone line
Consequences

- Light, heating, cooking
- Water and sewage pumping
- Oil and gas pipeline pumps, gas stations
- Transportation
- Telecommunications
- Banking and finance
- Food production, refrigeration and distribution
- Emergency services
Health Consequences

- Electronic Medical Records
- Medical Supply Chain
- Pharmaceuticals
- Billing/ Administration
- Imaging
- Lab results
- Certain medical equipment
- Health communication
- Emergency response
- Light, heat, cooling, elevators and security inside facilities
Geomagnetic Storms

- March 1989 (Quebec)
  - 480 nT/min
  - Knocked out power to 6 million people in 92 seconds
- May 1921
  - Up to 4,800 nT/min
- Sept. 1859 (Carrington event)
  - 2,000 to 5,000 nT/min
Transformer; 1989 Solar Storm
Solar electromagnetic radiation and energetic particles impact Earth’s Magnetosphere and Ionosphere, causing space weather disturbances.
The Sun at solar maximum

2003/10/20 00:00

The Sun today
Solar Flares (Radio Blackouts – R Scale)

- A violent explosion in the Sun’s atmosphere with an energy equivalent of a hundred million hydrogen bombs.

- Arrival: 8 minutes from Sun to Earth
- Duration: minutes to 3 hours
- Daylight-side impact
**Solar Radiation Storms** *(S Scale)*

- Arrival: 30 minutes to several hours
- Duration: hours to days
- Mostly high-latitude communication and exposure impact

**Impacts...**
- High latitude communications
- Satellite Operations (range from loss of data to loss of satellite)
- Manned spaceflight (exposure concerns)
- Spacecraft launch operations
- Aviation (communications and exposure concerns)
Geomagnetic Storms (G Scale)

Coronal Mass Ejections (CMEs) create geomagnetic storms

- Arrival: 20 – 90 hours
- Duration: hours to a day
- Creates Ionospheric storms
Current Solar Activity

- **Solar activity**
  - Indicated by Sunspot number (SSN) & F10.7
    - Predicted peak in 2013
  - Storming – increase in both frequency and strength
    - 14 Feb 2011 – 1st X-Class solar flare since 2006
    - 7 Jun 2011 – 1st proton event of solar cycle
  - U.S. dependence on space assets up considerably since last solar max in 2001
Capability to Repair and Recover from Damage to Civilian Systems

Other Civilian Infrastructures Dependent Upon Availability of Power

- **Telecommunications:**
  - May be significantly impacted, at least at the outset
  - Recovery will be dependent on prompt restoration of power

- **Financial system:**
  - Vulnerable to an EMP induced disruption of telecommunications and computers

- **Remote controls in infrastructures are at risk of disruption and damage**
  - *Transportation* infrastructure is vulnerable to disruption.
  - **Oil and gas supplies** likely disrupted due to failures of pump and valve controls
  - **Potable water** likely disrupted in the region affected by the EMP
  - **Distribution of food** may be degraded
Military Forces

• Strategic Forces
  – EMP survivability remains a strategic necessity
    • Offensive forces, Defensive forces, Responsive Infrastructure
  – End of Cold War relaxed discipline for meeting capability for EMP hardness

• General Purpose Forces
  – Hardened equipment embedded in soft systems
  – Increased dependence on high reliability electronics, not just components but supporting infrastructure
Danger of EMP Attack Can Be Mitigated

• Our free, modern society has inherent vulnerabilities that cannot be completely eliminated

• Catastrophe can be averted by practical and affordable steps to
  – Prevent attacks,  
  – Prepare to recognize and respond to an EMP attack  
  – Protect critical infrastructure elements and strategic military capabilities, and  
  – Recover following attack

• National security and homeland security are Federal responsibilities that should be funded by the Federal government

In just a few years we can make significant, affordable improvements to protect society even if an EMP attack is carried out against us
Recommendations I

- Protect high value assets through hardening
- Protect the use of emergency power supplies and fuel delivery
- Assure adequate communications assets dedicated or available to system operators
- Separate the present interconnected systems into several non-synchronous connected sub-regions or electrical islands
Recommendations II

• Install substantially more black start generation units coupled with specific transmission that can be readily isolated to balancing loads
• Improve, extend, and exercise recovery capabilities
• Understand system and network level vulnerabilities
• Develop national and regional restoration plans
Final Comments

It is mostly about the Electrical Grid

For the Grid, it is more about its vulnerability than the EMP threat. It is vulnerable to several threats capable of simultaneous, wide area attack such as SOLAR STORMS, CYBER ATTACK and physical sabotage.
Back-up Slides
Quad Chart: SPIDERS Battle Space

Operational Problem:
The ability of today’s warfighter to command, control, deploy, and sustain forces is adversely impacted by a fragile, aging, and fossil fuel dependent electricity grid, posing a significant threat to national security.

OV-1:
- Critical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the electric grid.
- Aurora threat revealed the possibility that sophisticated hackers could seriously damage the grid by destroying mechanisms downstream from the initial point of attack.
- DoD will conduct a coordinated energy assessment, prioritize critical assets, and promote investments in energy efficiency to ensure that critical installations are adequately prepared for prolonged outages caused by natural disasters, accidents, or attacks.

Increased cyber attacks against critical infrastructure:
- Stuxnet
- DuQu
- Wiper
- Flame
- Gauss
- Mahdi
- Shamoon
- Tevent
- DDoS on Banks

Funding - $31 M + $4.5 In-Kind Support

Electricity is our “national engine”
- Reliability
- Efficiency
- Security
- Resiliency

UNCLASSIFIED
What Is SPIDERS?

Reduce the “unacceptably high risk”* of mission impact from an extended electric grid outage by developing the capability to maintain energy delivery for mission assurance

• **Demonstrate:**
  – Cyber-security of electric grid
  – Smart Grid technologies & applications
  – Secure microgrid generation & distribution
  – Integration of distributed & intermittent renewable sources
  – Demand-side management
  – Redundant back-up power systems

• **Results in:**
  – Technically sound, commercially viable secure microgrid demonstration with mixed generation including renewables
  – First complete DoD installation with a secure, smart microgrid capable of islanding
  – Template for mission critical asset energy security for an entire installation and transition to commercial use

Notional Power Reliability

- Tier 1 – Mission Critical
- Tier 2 – Support Facilities
- Tier 3 – Non-Critical

Time (t) vs. Reliability (R):
- SPIDERS
- Current Configuration
Expected SPIDERS Outcome

**Phase 1**
- FT CARSON MICRO-GRID
  - Large Scale Renewables
  - Vehicle-to-Grid
  - Smart Micro-Grid
  - Critical Assets
  - Mission Assurance Demo
  - COOP Exercise

**Phase 2**
- CAMP SMITH ENERGY ISLAND
  - Entire Installation
  - Smart Micro-Grid
  - Grid-tied & Islanded Operations
  - High Penetration of Renewables
  - Demand-Side Management
  - Ancillary Services
  - Makani Pahili Hurricane Exercise

**Phase 3**
- PEARL-HICKAM CIRCUIT LVL DEMO
  - Solar (wind) Renewable
  - Flow Battery Storage
  - Energy Management Sys
  - Cyber architecture SCADA evaluation at Sandia National Labs

**Transition**
- Template for DoD-wide implementation
- New Uniform Facility Codes
- CONOPS
- TTPs
- Training Plans
- DSIA Certification
- Transition to Electric Utility Sector
- Transition Cyber-Security to Federal Sector and Utilities

**Cyber Security Best Practices**

**Rigorous Assessment With Red Teamming in Each Phase**
SPIDERS Participants

- USPACOM, USNORTHCOM
- DOE, and DHS

- 5 DOE Nat’l Labs

- USACE/ERDC-CERL

- Military Services

- Naval Facilities Engineering Command

- Local Utility Companies

- States of Hawaii & Colorado

- Private Sector
Objectives:

1. Identify physical and cyber security gaps, seams, and disconnects in electric grid information systems and industrial control systems between the private sector companies that own the grid and the government agencies that are responsible for protecting and regulating it.

2. Determine how gaps and seams impact the capabilities of both the private and public sectors to respond to various types of physical or cyber-attacks directed against the grid's information systems or industrial control systems.

3. Identify actions and responsibilities to improve information sharing between government and the private sector.

Partners: OSD, DHS, DOE, & Utility Industry

SG-10 – Regional power outage caused by cyber attack
SG-11 – Major power outage caused by solar weather

- Deliverables: Hosted by USNORTHCOM
- Quick Look
- After Action Report published 20 Dec 2011