3.16 RISK ASSESSMENT: CYBER DISRUPTION

DESCRIPTION

Large-scale disruptions limiting operations in cyberspace may be related to solar flares and magnetic storms, power disruption, or cyber threats. Cyber terrorism is a deliberate act of computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or computer system or information. Cyber disruption is a hazard that touches many aspects of our communities: industry, government, health, business, and private. Cyber security has shifted its focus from preventing initial entry to limiting damage once a system has been penetrated by identifying breaches and isolating the malware to stop it from spreading. A state cyber-security group is working to address risk to state agencies' systems. Centralized systems like Supervisory Control and Data Acquisition (SCADA) are used to control infrastructure such as: communications, utilities, transportation, medical facilities, law enforcement, business, financial systems, and personally identifiable information (PII), all which may be compromised by cyber disruptions.

Geomagnetic storms are "disturbances in the geomagnetic field caused by gusts in the solar wind that blows by Earth". (NOAA / Space Weather Prediction Center, 2005) Solar Radiation Storms are "elevated levels of radiation that occur when the numbers of energetic particles increase Radio Blackouts are "disturbances of the ionosphere caused by X-ray emissions from the Sun." (NOAA / Space Weather Prediction Center, 2005). The National Oceanic and Atmospheric Administration (NOAA) monitors space weather and has developed scales listing potential space weather impacts. These can be found at http://www.swpc.noaa.gov/NOAAscales/.

The sun is the source of space weather. Systems that utilize GPS are at risk from disruptions to magnetic storms. The currents produced during magnetic storms may damage transformers and corrode energy pipelines. The societal and economic impacts of a geomagnetic disturbance scenario have been mapped below (see Map 3.16.A) and show areas in Idaho prone to system collapse. An at-risk transformer capacity in Idaho is estimated at 47%.

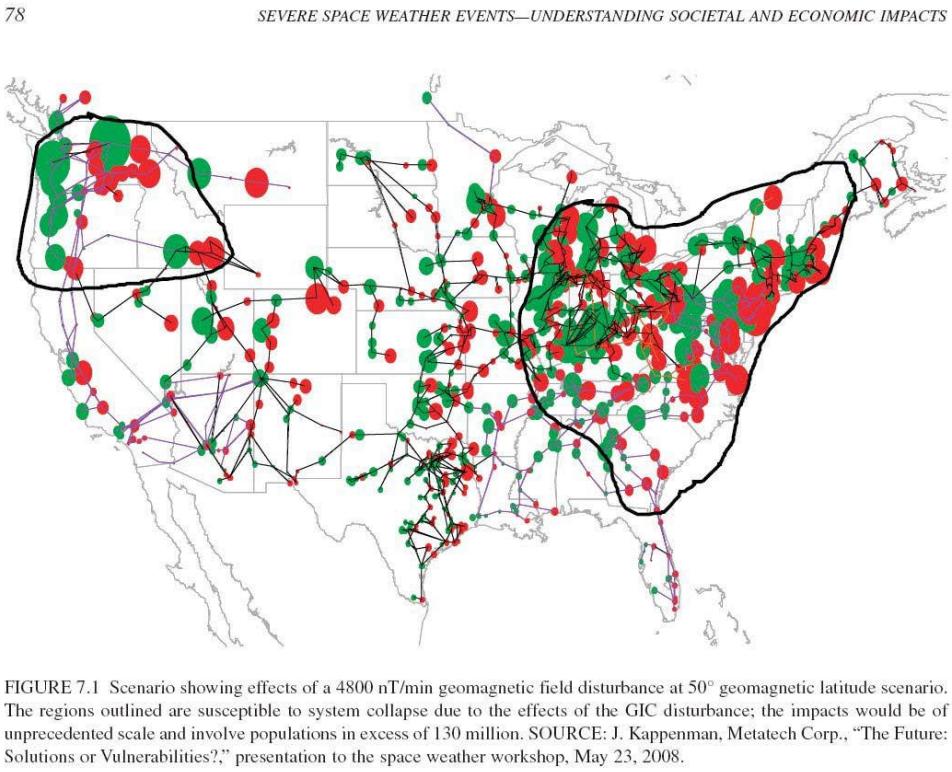

FIGURE 7.1 Scenario showing effects of a 4800 nT/min geomagnetic field disturbance at 50° geomagnetic latitude scenario. The regions outlined are susceptible to system collapse due to the effects of the GIC disturbance; the impacts would be of unprecedented scale and involve populations in excess of 130 million. SOURCE: J. Kappenman, Metatech Corp., "The Future: Solutions or Vulnerabilities?," presentation to the space weather workshop, May 23, 2008.

Map 3.16.A: Societal and Economic Impacts / Source: Severe Space Weather Events – Understanding Societal and Economic Impacts

Cyber disruptions may be driven by criminal motives for profit, extortion, or theft, or as deliberate attacks to destroy, damage, or interfere with infrastructure systems. The assessment for the likelihood of an event involving this tactic is moderate, based on a review of threats and trends related to this type of attack methodology both nationally and at the state level. Intelligence also indicates this this methodology has been used in limited attacks and attempted attacks both overseas and within the United States with some level of success as a viable tactic. (State of Idaho THIRA 2012 authored by David Jackson)

LOCATION, EXTENT, AND MAGNITUDE

A cyber disruption could occur anywhere across the State where technological systems exist or are utilized. There is no associated magnitude ranking at present.

PAST OCCURRENCE

The 1859 Solar Flare is the largest magnetic explosion recorded and is referred to as the Carrington Event, named for British Astronomer Richard Carrington, who witnessed growing sunspots and

documented a bright white flash that lasted about five minutes. The impacts on Earth were colorful and bright auroras were seen as far south as Hawaii and Cuba. Telegraph operators experienced sparks from telegraph equipment that started fires. Scientists predict that such an event today would be devastating to the internet, communications, and power transformers, as well as satellites, airplanes, or any GPS guided system. Solar activity is closely monitored as the sun storms have increased since 2011. Cyber-attacks have increased nationwide during 2011 and 2012, particularly targeting the energy sector. Cyber-attacks have also increased in the banking and finance sectors. Hackers have attacked company computers, distracting employees and interfering with Internet Security Providers (ISP) to divert resources, take proprietary information, and steal PII. Small devices can wreak havoc and disrupt systems. Some USBs have been manufactured with viruses or may become infected and spread viruses to multiple computers. Firewalls, access via signatures, and anti-virus are becoming antiquated security methods.

FUTURE OCCURRENCE

Cyber Disruptions are expected to continue in the near future. Solar storm activity is expected to increase in 2013 (Solar Max) and is being mapped by NASA's Solar Shield Project to show strong currents and warn power companies to protect their systems. Recent cyber-attack trends seem to indicate that these types of events will continue to increase in the coming years.

RELATIONSHIPS TO OTHER HAZARDS

Cyber Disruptions have an almost limitless potential to impact all of the human-caused hazards in both numerous and unforeseen ways. In regards to natural hazards, while cyber disruptions cannot directly influence those events, it is possible for related systems to be affected. For instance, any computerized systems that manage flood control systems could potentially be impacted by a cyber-event, thereby possibly causing a flood event.

ENVIRONMENTAL IMPACTS

Cyber disruptions could impact the environment in a number of ways, as affected systems could to stop functioning as intended. It is difficult to predict such impacts as the systems that could be possibly involved are so numerous and complex.

DEVELOPMENT TREND IMPACTS

Development trends across the State will have a relatively minimal influence or impact to future cyber events.

CRITICAL INFRASTRUCTURE AND STATE FACILITY IMPACTS

The rapid growth of social media use and technology has increased the potential of cyber disruption exponentially. The commonplace use of computers in practically every office and system contributes to

the complexity of protecting and mitigating cyber threats. Government and industry are striving to use continuous monitoring and limiting the data that may be accessed once a system is breached.

Executive Order 13636 states, "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cyber security. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats." The use of classified information will be expanded from defense industries to include critical infrastructure industries "enabling near real-time sharing" to assist in security efforts. (Rockwell, 2013)

A small number of experts "qualified to protect the nation's infrastructure from a concerted cyber-attack" are hosted by the Idaho National Labs, which is a Department of Energy nuclear research and development facility. (Top U.S. Cyber Defenders Work in Idaho Falls, 2012) A national organization, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), reaches out to assist the technology community. The team is composed of experts who often provide on-site support to organizations, publications, and mitigation briefings.

VULNERABILITY ASSESSMENT

Government and industry have been reluctant to publically report any type of vulnerability information on a large scale. As mentioned in some of the previous sections, some vulnerability assessments have occurred as they relate to very specific systems (i.e. - An at-risk transformer capacity in Idaho is estimated at 47%). But no specific, statewide vulnerability assessment yet exists for the hazard of cyber disruption.

LOSS ESTIMATION

Government and industry have been reluctant to report and share information in the past to protect public image and suppress the release of information to the attackers. No specific, statewide loss estimation exists for the hazard of cyber disruption. According to the State of Idaho, State of Idaho Department of Administration, the majority of state agencies have not consistently reported incidents in the past. It is just recently that agencies are reaching out, reporting issues, and asking for help.

MITIGATION RATIONALE

Due to the universal application of cyber communications, cyber disruptions from natural or human-caused sources will have far reaching impacts. Solar flares are being monitored closely to predict future geomagnetic storms in time to issue warnings. Power companies, for example, could mitigate damages by taking transformers off-line for a few hours.

GENERAL MITIGATION APPROACHES

Constant vigilance is required to limit cyber-attacks and automated monitoring is replacing former methods. Information sharing is encouraged to mitigate the spread of known cyber-attacks despite the possibility of making attackers aware of vulnerabilities. It is vital to implement and maintain processes to verify identity and authorize, grant, or deny access to specific locations, information, and networks. Development of risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cyber security initiatives and efforts is recommended. Other approaches could include updating procedures to detect malicious activity and to conduct technical and investigative- based countermeasures, mitigations, and operations should. Efforts to coordinate cyber incident management and reporting capabilities are also an action to be considered to help mitigate this hazard.

Mitigation approaches may include:

- Security appliances and applications
- Backup & restore
- Encryption capabilities
- Authentication, Access, and Accounting (AAA)
- Redundant equipment & networks
- Alternate delivery methods
- Cyber security training and exercises
- Educate public, state employees, and officials
- Contingency planning
- ISP and web hosting reviews
- Share malware signatures
- Coordinate automated responses
- Map suspicious activities
- Anticipate attacks

“Now computer scientists are devising guardians they call symbiotes that could run on embedded computers regardless of the underlying operating systems. In doing so, they may not only help protect the critical infrastructure of nations and corporations but reveal that warfare against these devices may have been going on unseen for years.” (Auto-Immune: "Symbiotes" Could Be Deployed to Thwart Cyber Attacks, 2012-11-26, pp. 9 ICS-CERT Monitor) The Federation of American Scientists addressed cyber security and recommended mitigation actions to engage the public in planning and policy development in a 2012 symposium. “Damaging consequences of cyber warfare will go well beyond military installations and assets, and the public has a right to know how cyber-attacks and counter attacks might affect financial, power, and transportation systems that they depend on every day for their basic needs….Effective cooperation… requires clear definition of responsibility and assignment of liability – whether to private companies or public authorities-to provide positive

incentives for adequately protecting critical infrastructure." (Abrams, Ahearne, Benedict, Blair, Drell, Franz, Feguson, Garwin, Koonin, Kristensen, Norris, Ovshinsky, Schroeder, Walker, 2012)

The ICS-CERT team monitors vulnerabilities to critical infrastructure, responds to intrusions, raises awareness levels, and addresses the need for assessing risk through the Common Vulnerability Scoring System (CVSS). "The CVSS score is an indicator of the severity ranging from 0, meaning no vulnerability present, up to 10, which indicates the highest severity vulnerability. ICS-CERT provides the base CVSS score in advisories as an indicator to asset owners and operators of the severity of the vulnerability. By providing the base metric, readers can use the base metric as a tool to quickly determine the seriousness of the vulnerability associated with the affected system" and "to aid them in prioritizing their mitigation strategies." (ICS-CERT Monitor, 2012) ICS-CERT briefs critical infrastructure owners and stakeholders on threats, security measures, and mitigation actions to reduce risk.