## Space Weather Frontline (1/2)

### Squo solves – laundry list of new technology currently protects earth from solar storms

R.I.T. - 8/01/11, “Warning System Could Protect Power Grid, Satellites from Space Storms” http://www.rit.edu/news/story.php?id=48456

Dube and his group of seven students have made significant advances in the ability to predict space weather storms affecting Earth. Their research agenda has expanded to include a variety of solar physics and stellar physics objectives: • Recognizing features on the sun for use in a predictive process • Studying different aspects of coronal mass ejections • Linking activity on the sun (such as sunspots) with other types of impacts on Earth (such as the aurora borealis and radio storms) • Studying solar-wind drag on coronal mass ejections • Tracking the movement of spots on stars to determine rotational speed The essence of Dube’s research lies in complex pattern recognition problems. The neural network his team developed digests the massive amount of data taken from different types of variables, such as electricity and magnetism. Another variable includes the concentrations of nitrates from the upper atmosphere that have settled in ice cores taken at the North Pole. “What’s happening is that we’re able to recognize these precursors in this data that’s within half a day of the event. That’s good, but we’d really like to have it several days in advance so that you could do something about it,” Dube says. “For example, with enough warning we can turn our satellites away from the sun so they don’t get hurt by the particles that hit them as the storm passes.”

### Massive alt causes – cyber hacking, system gaps, poor coding

WSJ – 10, “Grid is Vulnerable to Cyber-Attacks” 8/3/11 http://online.wsj.com/article/SB1000142405274870490 5004575405741051458382.html

Computer networks controlling the electric grid are plagued with security holes that could allow intruders to redirect power delivery and steal data, the Energy Department warned in a recent report.

Many of the security vulnerabilities are strikingly basic and fixable problems, including a failure to install software security patches or poor password management. Many of the fixes would be inexpensive, according to the Idaho National Lab, an Energy Department facility that conducted the study.

The report reinforces concerns that intelligence officials have raised in recent years about growing surveillance of the electric grid by Chinese and Russian cyber-spies, which The Wall Street Journal reported last year. One worry is that a foreign country could shut down power in parts of the U.S.

The report's release comes hot on the heels of a report from [Siemens](http://online.wsj.com/public/quotes/main.html?type=djn&symbol=SI) AG, the German engineering firm, which said it had detected an attack targeting critical infrastructure, the collective term for systems such as electric grids, subways and air-traffic control. Siemens issued a tool to detect and fix the security gap July 22, an unusual acknowledgment of the threat. The company said none of its customers has sustained damage.

"The Siemens attacks from a couple weeks ago, in addition to evidence from several private firms that utilities are being attacked…change the imperative," said Alan Paller, director of research at SANS Institute, a cyber-security training group. He suggests the U.S. needs to adopt a more urgent response.

The Energy report is based on the findings of 24 assessments of computer-control systems performed between 2003 and 2009. It was completed in May, released July 22 on the Energy Department's website and first noted by Steven Aftergood, a government secrecy specialist at the Federation of American Scientists.

The security gaps highlighted include "well-known unsecure coding practices" for software used by these control networks; and permitting an "excessive" number of portals access into the networks.

"Poor code quality leads to vulnerabilities and bugs in the code that not only make it vulnerable to attack, but also fragile and unstable," the report said.

Ineffective passwords are also a major problem, the report said. That issue was borne out in the Siemens attacks, because the attack software took advantage of preset passwords that Siemens advised clients not to change. "Passwords are often the weakest link," the report said.

A lack of sufficient encryption for communications lines used by these computer networks was another security gap the report identified, with the warning that "unfortunately there is no drop-in replacement currently available."

Databases that archive information about the systems were also vulnerable to penetration, the report found.

Such security gaps have been known inside security circles for years, but it is unusual for a government agency to publicly acknowledge them.

"We have so many known vulnerabilities that have not been patched," said Mischel Kwon, a former senior Homeland Security official and now a vice president at computer security company RSA. "The report offers common sense and best-practice recommendations that have been available for years."

## Space Weather Frontline (2/2)

### Power grid resilient and failures can be good – strengthens resistance

Ghosh – 9, Bobby Ghosh, journalist and TIME Magazine's World Editor, 4/15/09 “How Vulnerable Is the Power Grid?” http://www.time.com/time/nation/article/0,8599,1891562,00.html

The most critical power users — the military, hospitals, the banking system, phone networks, Google's server farms — have multiple contingencies for uninterrupted power supply and backup generation. In the event of a cyberattack on the grid, they would be able to operate for long periods — days, weeks and, in some cases, indefinitely — without much difficulty.

•The power grid is far from perfect. On any given day, 500,000 Americans experience an outage, says Arshad Mansoor of the Electric Power Research Institute, which is funded by the utility industry. Why is this a good thing? Because it means the grid deals with breakdowns all the time, and the industry knows how to fix them. The grid has built-in redundancies and manual overrides that allow for restoration of supply. Mansoor is careful to point out that these are "not defenses against cyberattacks, but for dealing with the consequence of such attacks."

•The larger point is that in most cases, damage done to the power supply can be undone. "In the banking system, if someone hacks the system and steals information about 500,000 credit cards, it's incredibly tough to undo that damage," says Mansoor. "But if a section of the power grid goes down, we start it up again."

### If a solar storm as bad as the aff predicts actually does hit, there’s nothing we can do – we’re all doomed

Lovett – 11, Richard A. Lovett, NASA writer, 3/02/11, “What If the Biggest Solar Storm on Record Happened Today?” http://news.nationalgeographic.com/news/2011/03/110302-solar-flares-sun-storms-earth-danger-carrington-event-science/

To begin with, the University of Colorado's Baker said, electrical disturbances as strong as those that took down telegraph machines—"the Internet of the era"—would be far more disruptive. (See ["The Sun—Living With a Stormy Star"](http://science.nationalgeographic.com/science/space/solar-system/sun-stormy-star.html) inNational Geographic magazine.)

Solar storms aimed at Earth come in three stages, not all of which occur in any given storm.

First, high-energy sunlight, mostly x-rays and ultraviolet light, ionizes Earth's upper atmosphere, interfering with radio communications. Next comes a radiation storm, potentially dangerous to unprotected astronauts.

Finally comes a coronal mass ejection, or CME, a slower moving cloud of charged particles that can take several days to reach Earth's atmosphere. When a CME hits, the solar particles can interact with Earth's magnetic field to produce powerful electromagnetic fluctuations. (Related: ["Magnetic-Shield Cracks Found; Big Solar Storms Expected."](http://news.nationalgeographic.com/news/2008/12/081217-solar-breaches.html))

"We live in a cyber cocoon enveloping the Earth," Baker said. "Imagine what the consequences might be."

Of particular concern are disruptions to global positioning systems (GPS), which have become ubiquitous in cell phones, airplanes, and automobiles, Baker said. A $13 billion business in 2003, the GPS industry is predicted to grow to nearly $1 trillion by 2017.

In addition, Baker said, satellite communications—also essential to many daily activities—would be at risk from solar storms.

"Every time you purchase a gallon of gas with your credit card, that's a satellite transaction," he said.

But the big fear is what might happen to the electrical grid, since power surges caused by solar particles could blow out giant transformers. Such transformers can take a long time to replace, especially if hundreds are destroyed at once, said Baker, who is a co-author of a National Research Council report on solar-storm risks.

The U.S. Air Force Research Laboratory's Cliver agrees: "They don't have a lot of these on the shelf," he said.

The eastern half of the U.S. is particularly vulnerable, because the power infrastructure is highly interconnected, so failures could easily cascade like chains of dominoes.

"Imagine large cities without power for a week, a month, or a year," Baker said. "The losses could be $1 to $2 trillion, and the effects could be felt for years."

Even if the latest solar maximum doesn't bring a Carrington-level event, smaller storms have been known to affect power and communications.

### Solar storms can be deflected and change direction

NASA Science News – 10, “Solar Storms can Change Directions, Surprising Forecasters” 9/21/10, http://science.nasa.gov/science-news/science-at-nasa/2010/21sep\_zigzag/

"This really surprised us," says co-author Peter Gallagher of Trinity College in Dublin, Ireland. "Solar coronal mass ejections (CMEs) can start out going one way—and then turn in a different direction." The result was so strange, at first they thought they'd done something wrong. After double- and triple-checking their work on dozens of eruptions, however, the team knew they were onto something.

"Our 3D visualizations clearly show that solar storms can be deflected from high solar latitudes and end up hitting planets they might otherwise have missed," says lead author Jason Byrne, a graduate student at the Trinity Center for High Performance Computing.