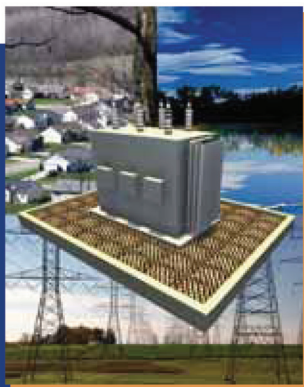


The SorbWeb™ Plus Solution



- Proven system that effectively contains oil spills from equipment and transformers
- No pumps, no oil water/separator, no maintenance
- Engineered and designed around site requirements
- SPCC Compliant

USA
Tel: 207-786-0424
Toll Free: 1-877-786-0424

CANADA
Tel: 705-737-0551
Toll Free: 1-866-269-8275



sorbwebplus@albarrie.com
www.sorbwebplus.com

SES has again raised the standard for grounding and electromagnetic interference analysis software with...

AUTOGRID PRO®

Finally, you don't need to settle for second class grounding software because of a small budget...

Affordable software from SES, the world leader in grounding and EMI. Licenses start at \$999.

- CAD-based, fully automated design of multiple grounding systems of any shape buried in arbitrary soil
- Schlumberger, Wenner or General resistivity measurement method.
- Detailed fault current distribution between ground and neutral circuits.

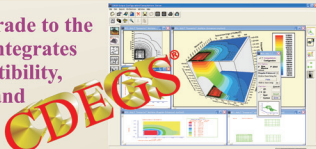
- Modular and inexpensive. Add powerful modules as needed.
- GUI interface, context-sensitive help & exceptional technical support.
- Flexible report and plot tools vividly illustrate any computed results.
- Compatible with CAD software. Use SES's databases or add your own.

For even more capabilities, upgrade to the full power of CDEGS, which integrates grounding, electromagnetic compatibility, corona, radio noise, audible noise and lightning / surge analyses.



RIGHT-OF-WAY

- The only proven tool for computing currents and voltages caused by induction and conduction anywhere along the right-of-way.
- Automated fault simulations yield maximum interference levels such as pipeline or rail GPRs, rail-to-rail voltages, induced longitudinal & leakage currents, telecom line noise, tower GPRs, etc.
- Multiphase networks, pipe-enclosed cables, pipelines, rails or insulated & bare conductors.



Toll Free: 1-800-668-3737 Tel.: 1-514-336-2511; Fax: 1-514-336-6144
email: info@sestech.com web site: www.sestech.com

NEWS

Even if the contract had been awarded on a competitive basis, it's likely AMSC would have easily won it. The company owns the first commercial second-generation HTS factory, which is the technical and practical foundation for its current-limiting concept. And Southwire, its partner in Secure Super Grids, has set the record—2700 A—for an HTS cable in a working transmission grid using a cable it designed with AMSC's first-generation wire. Southwire, in Carrollton, Ga., conducted that test with American Electric Power in Ohio. As for fault-limiting

cables, Malozzoff says "we're the only company out there that has come up with this"—a claim nobody disputes.

AMSC expects to survive the Dingell probe with its reputation essentially intact. But the investigation may be a shot across its bow. With superconductors on the eve of commercialization and set to become a big business, AMSC's claims will be subjected to ever closer scrutiny. Its days as a no-bid government contractor may be coming to an end, and increasingly it may have to cope with normal competitive pressures.

—WILLIAM SWEET

WHAT THEY DON'T SEE: China is one of the 25 countries found to systematically filter its citizens' Internet content.



Internet Censorship: As Bad As You Thought It Was

Maybe a bit worse, actually

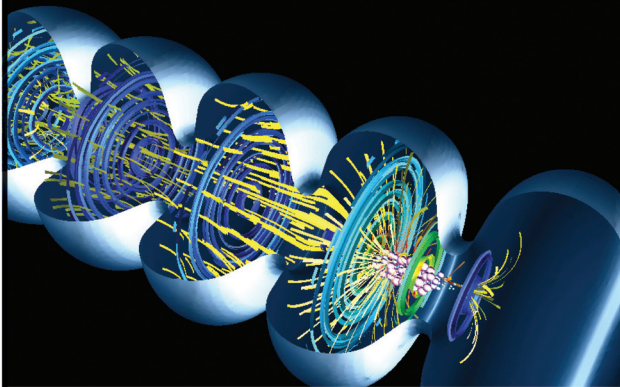
"In the dot-com heyday of the '90s and early 2000s... there was a myth that the Internet can't be controlled," says Ronald Deibert, a researcher at the University of Toronto's Citizen Lab. "There was some mysterious, magical property associated with it that will route around censorship." The most exhaustive study yet of

Internet censorship—*Access Denied: The Practice and Policy of Global Internet Filtering*, published this month by the MIT Press—pretty much disproves that notion.

The report's authors, the OpenNet Initiative—a multidisciplinary team at the University of Toronto, and Cambridge, Harvard, and Oxford universities—

Fluids
Plasmas
Particle Beams
Electromagnetics
High Performance Computations

VORPAL



VORPAL simulation of the superconducting Tesla cavity. The electron beam (spheres) moving to the right in the cavity creates an electromagnetic wakefield (electric field: yellow, magnetic field: blue) as well as a leading precursor.



<http://vorpal.txcorp.com>

2008 IEEE-USA/AAAS Mass Media Science and Engineering Fellows Program



Increasing Public Understanding of Science and Engineering

IEEE-USA is looking for two U.S. IEEE student members to help strengthen the connections between engineers and journalists by working for 10 weeks during the summer as reporters, researchers and production assistants in newsrooms across the country. The goal is to increase public understanding and awareness of science and engineering.

To apply, you must be at least a senior in college majoring in a technical field, mathematics or social sciences. A weekly stipend of \$450 is provided.

Applications must be received by 15 January 2008.

Visit www.aaas.org/programs/education/MassMedia for more information, or contact Stacey Pasco at spasco@aaas.org, or +1 202 326 6645.



NEWS sent investigators to 41 countries that had been rumored to filter Internet content, whether to silence political dissent or to block access to pornography or religiously and culturally divisive material.

ONI set out to objectively confirm or invalidate the reports. It found that the situation was worse than the rumor mill suggested. “The big thing is that the scope, scale, and sophistication of Internet content filtering is on the rise worldwide, and it’s really an alarming increase,” says Deibert, one of the book’s editors and contributors.

ONI discovered systematic Internet filtering in 25 countries, with nine of them—China, Ethiopia, Iran, Myanmar, Saudi Arabia, the United Arab Emirates, Uzbekistan, Vietnam, and Yemen—blocking content in every category it investigated.

“The vast majority of content [around the world] that is blocked is pornography,” Deibert says. “But what we’re seeing now is many countries broadening the scope of their filtering to political opposition movements, human rights information, Web sites of minority groups, secessionist movements, gay and lesbian information, translation services, and encyclopedias.”

On the other hand, five countries—Azerbaijan, Jordan, Morocco, Singapore, and Tajikistan—that were rumored to broadly filter the Internet turned out to block just one or a few select Web sites.

ONI researchers travel to each country they test and, wherever possible, employ Internet-savvy locals who know the ISPs and cybercafés most likely to be targeted by the government. Using a Web browser in the Internet cafés, on the local ISPs, or both, they attempt to access

approximately 1000 Web sites that might be targeted by any government. The sites include top human rights, activism, and pornography destinations, as well as ones that offer tools that let you surf the Web without being traced.

In-country researchers also run local lists of sites that might be targeted by the relevant authorities. In China, for example, they tried to access sites associated with Falun Gong and local democracy activists. In Arabian and Persian Gulf countries, ONI attempted to access women’s rights and Islamic dissident sites.

Testing over a span of weeks, at various times of night and day, ONI researchers concluded that a site had been filtered if it was persistently unavailable in the country but accessible elsewhere in the world.

ONI has noted that censorious governments have become increasingly subtle about the way they filter Internet content.

One new frontier of Internet censorship, Deibert says, is “just-in-time filtering.” For instance, ONI detected no noteworthy filtration in Kyrgyzstan in general. But in the weeks leading up to the country’s February 2005 elections, Web sites of the country’s opposition newspapers were regularly taken down by denial-of-service attacks. ONI traced those attacks back to Ukrainian hackers for hire but was never able to establish a direct link to the Kyrgyz government.

In a more recent instance, the Cambodian government blocked SMS messaging over the country’s cellular network for the two weeks before elections last April. “One would have to surmise,” Deibert says, “that they were doing this to prevent mobilization of opposition, especially street demonstrations.”

—MARK ANDERSON