China Dominates NSA-Backed Coding Contest
Computerworld (06/08/09), P. Thibodeau

The TopCoder Open, a National Security Agency-supported contest that tests individuals' programming and technology design skills, was dominated by competitors from China and Russia. Of the 70 finalists, 20 were from China, 10 were from Russia, and two were from the US. Approximately 4,200 people participated in the contest, which is open to anyone, with about 894 contestants being from China, 705 from India, 380 from Russia, 234 from the US, 214 from Poland, 145 from Egypt, and 128 from Ukraine, among others. The vast majority of contestants, 93 percent, were male, with 84 percent between the ages of 18 and 24. TopCoder's Rob Hughes says the success of China, Russia, and Eastern Europe is the result of the importance those countries place on mathematics and science education. "We do the same thing with athletics here that they do with mathematics and science there," Hughes says. The US needs to make greater efforts to teach and get children in middle school and high school involved in math and science, he says. Of the participants in the content, more than 57% had bachelor's degrees, mostly in computer science, of which 20% had earned a master's degree and 6% had earned a Ph.D. The winner of the algorithm was an 18-year-old student from China. TopCoder contestants are tested in design, development, and architecture, among other areas. This year, competitors were challenged to unscramble and label two scrambled and erased social networks to see if they could possibly be from the same group of people, a problem known as the network isomorphism problem. Two contestants solved the problem.

Is the Hacking Threat to National Security Overblown?
Wired News (06/03/09), R. Singel

US President Obama recently made cybersecurity a national priority, but at the ACM's Computers, Freedom and Privacy Conference, Threat Level editor K. Poulsen asked whether hacking and cyberattacks are an actual threat to the United States or simply the latest exaggerated threat to national security. Former Bush administration cybersecurity czar A. Yoran says that hacking is absolutely a national security threat, and cites stories about the denial-of-service attacks against Estonia, attacks against government contractor Booz Allen Hamilton, and the recently reported breach of defense contractor computers that gave the attackers access to information on the Joint Strike Fighter. Poulsen says the threat of cyberterrorism is "preposterous," pointing out the long-standing threat that hackers would attack the power grid, which has never happened, and arguing that calling such potential attacks national security threats means that information about any possibility of defeated attacks is unnecessarily classified. "If we can't publicly share info that the attackers already have - since it's about them - then we are doing far more harm than good," says Poulsen, who argues that classification makes it impossible for the security community to, as a whole, prepare defenses for such attacks. Furthermore, Poulsen points out that the Joint Strike Fighter attack involved only unclassified information. However, security expert B. Schneier says there will be cyberattacks that affect the real world, though the current threat is exaggerated. "Passive defenses alone are not sufficient," says National Research Council cyberattack expert H. Lin. "You ha-

ve to impose costs on an attacker and maybe the only way to do that is a cyberattack yourself."

China Faces Criticism Over New Software Censor
New York Times (06/10/09), A. Jacobs; X. Yang

A government directive that all PCs sold in China come with software that can censor pornography and other "vulgar" content from the Internet has sparked howls of outrage among industry executives, proponents of free speech, and computer users. Manufacturers are facing a July 1 deadline to preinstall the software on machines, and US PC makers say meeting this deadline is impossible. They note that it raises a complicated issue as to whether manufacturers would be held accountable if the software clashes with operating systems or causes computers to crash. Computer experts are worried that the software could enable the Chinese government to watchdog Internet use and collect personal information. The designers of the filtering software, which is called Green Dam, insist that it cannot function as spyware. Green Dam uses image recognition technology and text filtering to block content, and its designers say the software can be disabled or deleted. Critics claim the software underperforms, censoring perfectly innocent content while allowing objectionable material to slip through. Also inspiring criticism is the Chinese government's decision not to consult computer users on the regulations or allow other companies to submit comparable software.

Social Networks Keep Privacy in the Closet
Technology Review (06/11/09), E. Naone

Social networks are being encouraged to downplay the privacy settings they build because of the tension between the desire to have users share as much personal information as possible and the need to protect that information and restrict how it is shared between users and outside their own borders. Privacy rights groups and activists are pressuring the networks to embed tools for users to control their information, but the networks also have an interest to keep privacy out of users' minds, according to research that will be presented at the 8th Workshop on the Economics of Information Security. "Their goal is to create a very free-flowing environment where everybody is constantly sharing everything and seeing all this data on other people," says University of Cambridge researcher J. Bonneau. "The best way to achieve that is to not bring up the concept of privacy." The researchers studied 45 social-networking sites and determined that more popular sites did better with privacy overall because they face greater pressure to shield user data and also have more resources to address the problem. Bonneau says the disclosure of all sites' privacy practices could help put pressure on major sites to enhance the protection of users' information. Another researcher, S. Preibusch, speculates that standardizing privacy settings could help users understand and control their information. University of Texas at Austin professor V. Shmatikov is concerned that social networks will exacerbate the situation if they start focusing less on drawing new users and more on reaping profits from the ones they have.

Experts Urge Federal Efforts on Cybersecurity
Federal Computer Week (06/10/09), B. Bain

The US federal government needs to step up its cybersecurity efforts, experts from industry and academia recently told the House Science and Technology Committee's Research and Science Education Subcommittee. Information technology users are largely responsible for their own defense against cyberattacks, said Georgia Institute of Technology professor S.

Goodman. He said the widespread use of cell phones and other mobile devices could lead to a tsunami in insecurity. "An effort must be made to get those people who are in the best position to mitigate risk to do so, and I think what should be done--and it's been done in other areas--industry and government need to get together, and they need to get together under some perhaps formal forum or other kind of an institutional mechanism with the mandate that they come up with greater security in cyberspace," Goodman said. Meanwhile, Applied Visions' A. D'Amico said the government should put more money into research and development programs so that more projects can turn their work into products. Cornell University professor F. Schneider said better formal and public cybersecurity education programs are needed. "We're not going to solve this problem only with Ph.D.s or only with bachelor's [degree] graduates," he said.

Privacy May Be a Victim in Cyberdefense Plan
New York Times (06/13/09) P. A1; T. Shanker; D. Sanger

The US Obama administration's cyberdefense strategy includes the formation of a new Pentagon cybercommand that critics warn may end up compromising personal privacy in order to fulfill its objective to monitor the myriad daily assaults on US security systems. Pentagon and military officials say there is no way to effectively run computer operations without penetrating networks within the United States, where the military is banned from operating, or traveling electronic pathways through countries that are not themselves US targets. Officials say the interception and analysis of some email messages may be necessary to guard against computer viruses or potential terrorist action, and supporters say the procedure could eventually be accepted as a digital version of customs inspections. M. Leed with the bipartisan Center for Strategic and International Studies says there needs to be a broad debate "about what constitutes an intrusion that violates privacy and, at the other extreme, what is an intrusion that may be acceptable in the face of an act of war." US General J. Cartwright with the Joint Chiefs of Staff admitted in a recent speech that the military's legal establishment of an early warning system for cyberattacks remains an unresolved issue. Leed notes that although the US Defense Department and related intelligence agencies are the only organizations capable of cyberattack protection, they are not the best-equipped entities to assume such duties "from a civil liberties perspective." The expectation is that the new cybercommand will be helmed by a four-star general who also will direct the National Security Agency in an effort to heal the rift between the spy agency and the military over who has authority to conduct offensive operations.

Secret War on Web Crooks Revealed
Financial Times (06/15/09) P. 18; M. Palmer

Three times a year, leaders from the world's major technology and communications companies meet to discuss strategies for preventing the Internet from becoming overrun with attacks, spam, viruses, and hackers, though the specifics of these meetings is often kept secret. "Some people might get nervous if they knew all the things we talked about," says Messaging Anti-Abuse Working Group (MAAWG) chairman M. O'Rierdan. "It's our job to make the Internet safe, but we don't want to put people off using the Web." MAAWG participants also are nervous about being targeted by the criminals they are trying to stop. Most of the spam and hacking online is now perpetrated by organized crime. Within the United States, retaliation against MAAWG generally comes in the form of lawsuits, but in other countries organized criminals in Russia and the Ukraine use more violent methods. MAAWG founder S. Linford has been advised by the police not to open any unexpected packages. The MAAWG confe-

rences attract approximately 270 delegates from 19 countries, and although the press has usually been kept out of the conferences, that trend is starting to change as participants feel the industry needs to reach out to consumers and get them to help fight spam and cybercrime. Nearly 90% of spam is sent from computers that have been hacked and are remotely programmed to send spam. More than 9.4 million computers have been hijacked for this purpose, and cleaning up all of these machines will be impossible without the public's help.

Experts Say Chinese Filter Would Make PCs Vulnerable
New York Times (06/13/09) P. A6; A. Jacobs

Computer security experts say the filtering software that China has required for all new computers is so technically flawed that it would be easy for hackers to infiltrate a machine and monitor Internet activity, steal personal data, or insert harmful and dangerous viruses. "It contains serious vulnerabilities, which is especially worrisome given how widely the software will be adopted," says University of Michigan professor J. Halderman, who examined the filtering program. "What we found was only the tip of the iceberg." Called Green Dam-Youth Escort, the software must be preinstalled on all personal computers sold in China by July 1. The Chinese government says it will pay for the software for at least a year as part of a campaign against "unhealthy and vulgar" content on the Web. Computer manufacturers outside of China have asked Chinese officials to reconsider the new rules. They argue that there are too many unanswered questions about the software, including whether it could damage operating systems. Human rights advocates and China's Internet users say Green Dam is really a thinly veiled attempt to expand censorship. "Their goal is to limit the access of information, not just pornography," says Beijing rights lawyer L. Fangping. "I feel like, as a citizen, my right to know has been violated." Opponents of the software hope that its technical deficiencies will delay its release, or even completely destroy the program. Halderman says the program is so poorly designed that in only a few hours he and his students were able to infiltrate a Green Dam-loaded computer and force it to crash.

E-Mail Surveillance Renews Concerns in Congress
New York Times (06/16/09), J. Risen; E. Lichtblau

A National Security Agency (NSA) operation involving surveillance of American residents' communications, especially domestic emails, is fueling debate in the US Congress about its legal and logistical ramifications, with current and former officials calling such monitoring much broader than previously admitted. Emails have been a particularly thorny issue for the NSA because of technological problems in drawing a distinction between messages by US citizens and foreigners. Several former intelligence officials note that email traffic from all over the world is frequently channeled through US-based Internet service providers, and when the NSA monitors a foreign email address, it does not know when the person using that address will send messages to someone inside the United States. A representative of national intelligence director D. Blair says that due to the complicated nature of surveillance and the need to comply with the rules of the Foreign Intelligence Surveillance Court and "other relevant laws and procedures, technical or inadvertent errors can occur." Agency advocates say the process of collecting millions of electronic messages by computer inevitably leads to the examination of innocent emails. Such messages are supposed to be filtered out, but critics say the NSA is not doing a good enough job in this area. An anonymous former NSA analyst verifies that the agency used a secret database that archived foreign and domestic emails and enabled analysts to read large volumes of messages to and from US citizens, provided they fell within certain parameters and the citizens were not explicitly targeted in the queries. Officials

acknowledge that the massive over-collection of US citizens' communications can lead to a substantial number of privacy infringements, which has raised alarms in both the Foreign Intelligence Surveillance Court and Congress.

Navy Wants Proposals on Cyber Research
Federal Computer Week (06/15/09), B. Bain

The US Navy has posted an announcement online seeking new models of computation and system architectures for cooperative cyberdefense, as well as research on controlling systems to produce trustworthy results. The Office of Naval Research (ONR) also is interested in research from industry and academia on metrics for comparing computation in networked environments; automated ways to define architectures for embedded real-time systems; and critical principles for new host architectures, focused on information assurance, manageability, and agility. The Navy plans to use the research for a large-scale and always-on information infrastructure that would be highly mobile and dynamic, and operate across many networks. ONR also is interested in research on "cyberphysical interaction spaces" caused by advances in networking and software-enabled devices. "ONR believes that significant fundamental advances can be achieved through research at the intersection of computer science, the natural sciences, and social sciences," according to the announcement. "There are many research opportunities and challenges we anticipate in this area." Researchers have until Aug. 27, 2009, to submit full proposals for approximately $14.5 million in awards.

China Intent on Requiring Internet Censor Software
New York Times (06/19/09) P. A8; E. Wong; A. Vance

US computer manufacturers say the Chinese government is standing firm on its requirement that all new computers sold in China beginning in July come with pre-installed censorship software, contrary to previous reports. In addition to the censorship software, an employee in Beijing's Spiritual Civilization Office says the Chinese government plans to recruit 10,000 volunteers to monitor online content by the end of the summer. The online-monitoring effort is part of a plan to "purify social civilization," the employee says. The Chinese government also is extending its control over the Internet by directly warning some online services. For example, the China Internet Illegal Information Reporting Center, a government-support Internet watchdog group, recently criticized Google's Chinese-language Web site for linking to "pornographic and vulgar" sites, and said that Google must eliminate the offending links. China's efforts so far to block content that is either pornographic or potentially damaging to the Communist Party has largely been circumvented by savvy computer users, leading to China's new requirement. Many people say the censorship software, called Green Dam-Youth Escort, will be used to block Web sites with unfavorable political content, though officials insist the software will be used primarily to block pornographic content. Computer experts also have discovered major security vulnerabilities that would enable hackers to easily hijack the computers.