the safety of drugs and medical devices imported from China. In that same time span, Congress has ratified just 20 treaties annually.

But presidential power grab it wasn't. Rather, it was Congress that, "because of a combination of institutional myopia and political incentives," more or less unwittingly gave away its power bit by bit. Handing over international lawmaking to the president meant more time to work on the domestic issues that decide elections. The courts, Hathaway writes, "have done nothing to correct the imbalance."

Some have argued that the resulting arrangement is preferable—that Congress is ill suited to making international policy. An effective international negotiator must have the authority to sign an agreement that will not be second-guessed and amended by Congress, they contend. Hathaway is unconvinced. Not only is it "inconsistent with basic democratic principles" for the executive to have unmitigated power in conducting international affairs, but it "can lead to less favorable agreements" that don't have necessary support from Americans who will be affected. And a negotiator who has to answer to Congress often has a stronger position, she argues. With the legislative branch lurking in the background, the president can refuse to give ground on certain provisions, on the pretense that such a deal will never garner approval.

Hathaway proposes comprehensive reform in how the United States makes international law. Congress could continue delegating authority to the president to make international agreements, she suggests, but those delegations should be narrow and include sunset provisions. The president should have to submit more agreements to Congress for review before they go into effect, a requirement that would encourage him to seek the legislative branch's input throughout the process. And legislators should adopt an expedited process for approving agreements. Through such changes, Congress would be brought back into the process. Hathaway stresses that making international law should not be the prerogative of the president.

FOREIGN POLICY & DEFENSE

E-Warfare

THE SOURCE: "The Cyberwar Plan" by Shane Harris, in ***National Journal***, Nov. 14, 2009.

The military of the United States reigns supreme on land, in the air, and at sea. But who will rule cyberspace remains an open question.

Shane Harris, a correspondent for *National Journal*, reports that cyberwarfare—attacks on a nation's power grid, air traffic control system, banks, Web servers, or phones—is now an integral part of U.S. military strategy. The government has made its efforts to keep American computers secure well known, but now evidence that the United States has engaged in an offensive cyber-strategy is piling up. Harris reveals that in May 2007 President George W. Bush authorized an attack on the cell phones and computers of insurgents in Iraq. Unnamed former officials credit such operations with helping to "turn the tide of the war." Some suggest they were even more instrumental than the thousands of additional troops President Bush sent to Iraq as part of the surge in 2007.

With the creation of high-level posts to coordinate U.S. cyber-strategy and the emergence of a younger generation of leaders, the new way of war is getting more attention from the defense establishment. But the United States faces major challenges in keeping pace with Russia and China. An independent study published in July found the nation's cyberwar staff fragmented and inadequate; the study blamed low salaries and a hiring process that can stretch on for months.

Secretary of Defense Robert Gates has said that the military is "desperately short" of cyberwarriors. The Defense Department graduates about 80 students each year from schools devoted to teaching cyberwarfare and hopes to quadruple that number in the next two years. But the government must compete with the private sector for top talent. For example, defense contractor Raytheon Company recently posted a "Cyber Warriors Wanted" advertisement on its Web site and announced 250 open spots.

The United States appears to have proceeded cautiously, in part

out of awareness that the weapons of cyberwarfare are very different from conventional ones, producing systemic effects that can be hard to anticipate. Planners considering an attack on the Iraqi banking system before the 2003 U.S.-led invasion backed off when they realized that the Iraqi networks were tied to ones in France that would also be affected. Moreover, the computer coding used in any assault is at risk of being captured by an adversary, refined, and redeployed. Mike McConnell, a former director of national intelligence, has said that a coordinated cyberattack "could create damage as potentially great as a nuclear weapon over time."

Old-fashioned Cold War–style deterrence theory plays a big role in the new thinking. Harris writes, "Presumably, China has no interest in crippling Wall Street, because it owns much of it. Russia should be reluctant to launch a cyberattack on the United States because, unlike Estonia or Georgia [which Russia is believed to have cyber-attacked in 2007 and 2008, respectively], the United States could fashion a response involving massive conventional force. . . . If nations begin attacking one another's power grids and banks, they will quickly exchange bombs and bullets."

SOCIETY

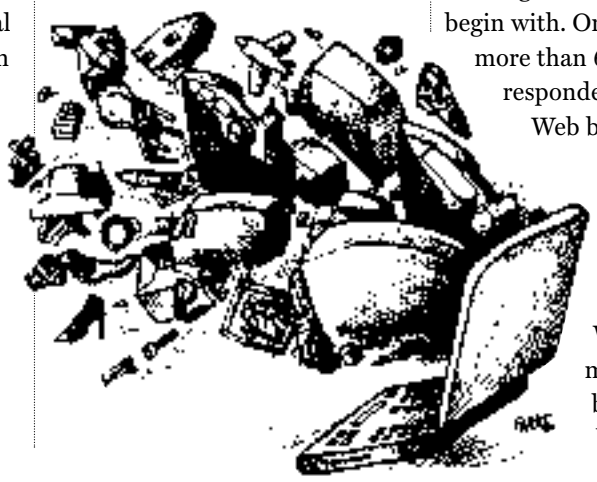
Good Vibrations

THE SOURCE: "Effects of Internet Commerce on Social Trust" by Diana C. Mutz, in ***Public Opinion Quarterly***, Fall 2009.

Hardly a day goes by without some headline declaring a new ill the Internet is visiting upon society. One oft-heard lament: Local shopkeepers are losing business to online retailers, and as a result, small interactions that once strengthened the social fabric of a neighborhood or town are no more. Is the Internet eroding the connections that keep society together?

Not at all, writes Diana C. Mutz, a political scientist at the University of Pennsylvania. Face-to-face interactions may be on the wane, but positive e-commerce experiences (and 80 percent of those who have purchased online characterize their experience positively) tend to boost a generalized sense of faith in other people, particularly strangers.

Earlier studies have established that people who are more trusting are more likely to participate in e-commerce in the first place. And Mutz finds that when they do so and have a positive experience, they become even more trusting. In a carefully crafted experiment, she tested the effects of good and bad online shopping experiences on people who had never bought anything on the Web before. Those whose packages arrived promptly and without hassle answered positively to survey questions about strangers' honesty and helpfulness, and human nature's essential goodness. Those who received broken goods and then poor customer service experienced a sharp drop in warm and fuzzy feelings toward their fellow man.



In general, people are not very trusting of online merchants to begin with. One study found that more than 60 percent of respondents believed that Web businesses were likely to try to cheat them, while only 21 percent said the same of local shops. What's more, many more people believed that online businesses could