The Coming *Cyber Crisis*

By Kenneth Rogoff

The striking parallels between the Great Financial Crisis and the threat of cyber attack.

When the financial crisis of 2008 hit, many shocked critics asked why markets, regulators, and financial experts failed to see it coming. Today, one might ask the same question about the global economy's vulnerability to cyber attack. Indeed, the parallels between financial crises and the threat of cyber meltdowns are striking.

Although the greatest cyber threat comes from rogue states with the capacity to develop extremely sophisticated computer viruses, risks can also come from anarchistic hackers and terrorists, or even from computer glitches compounded by natural catastrophe.

A few security experts have voiced great alarm, including, most recently, Jonathan Evans, the head of the British Security Service (MI5). By and large, however, few leaders are willing to compromise growth in the tech sector or the internet in any significant way in the name of a threat that is so amorphous. Instead, they prefer to establish relatively innocuous working groups and task forces.

It is difficult to overstate the dependence of modern economies on large-scale computer systems. But imagine if one day a host of key communications satellites were incapacitated, or the databases of major financial systems were erased.

Experts have long identified the electricity grid as the most acute vulnerability, since any modern economy would collapse without power. True, many skeptics argue that with reasonable low-cost prophylactic measures, large-scale cyber-meltdowns are highly implausible, and that doom-mongers overstate the worst-case scenarios. They say that the ability of cyber-terrorists and blackmailers to take the global economy to the brink, as in the 2007 Bruce Willis movie *Die Hard 4,* is utterly fictional.

It is difficult to judge who is right, and important experts are found on both sides of the debate. But there do seem to be an uncomfortable number of similarities between the political economy of cyberspace regulation and of financial regulation.

First, both cybersecurity and financial stability are extremely complex topics with which government regulators can hardly keep up. Industry remu-

Kenneth Rogoff is Professor of Economics and Public Policy at Harvard University, and former chief economist at the International Monetary Fund.

THE INTERNATIONAL ECONOMY
THE MAGAZINE OF
INTERNATIONAL ECONOMIC POLICY
220 I Street, N.E.
Suite 200
Washington, D.C. 20002
Phone: 202-861-0791
Fax: 202-861-0790
www.international-economy.com
editor@international-economy.com

The U.S. House of Representatives Cybersecurity Task Force, led by **Rep. Mac Thornberry (R-TX)** *[center], releases its recommendations on October 5, 2011. Also pictured, left to right,* **Reps. Dan Lungren (R-CA), Lee Terry (R-NE), Steve Stivers (R-OH),** *and* **Jason Chaffetz (R-UT).** Nota bene: *Not a computer science degree among the lot.*

neration for experts is far in excess of any public sector salary, and the best minds are continually bid away. As a result, some argue that the only solution is reliance on self-regulation by the software industry. One hears this argument for many modern industries, from big food to big pharma to big finance.

Second, like the financial sector, the tech industry is enormously influential politically through contributions and lobbying. In the United States, all presidential candidates must make pilgrimages to Silicon Valley and other tech centers to raise money. Excessive financial sector influence was, of course, a root cause of the 2008 meltdown and remains deeply implicated in today's continuing eurozone mess.

Third, with slowing growth in advanced economies, information technology seems to hold the moral high ground, just as finance did until five years ago. And crude attempts by governments to enforce regulation are likely to prove ineffective in protecting against catastrophe, while all too effective in strangling growth.

In both cases—financial stability and cyber security—the risk of contagion creates a situation in which a wedge can form between private incentives and social risks. Admittedly, progress in the technology sector overall often produces huge social welfare gains, which arguably outstrip those produced by all other sectors in recent decades. But, just as with nuclear power plants, progress can go awry in the absence of good regulation.

We are told not to worry about large-scale cyber meltdowns, because none has occurred, and governments are being vigilant.

Finally, the greatest risks come from arrogance and ignorance, two human characteristics at the heart of most financial crises. Recent revelations about the super-viruses "Stuxnet" and "Flame" are particularly disconcerting. These viruses, apparently developed by the United States and Israel to disrupt Iran's nuclear program, embody a level of sophistication far beyond anything previously seen. Both are deeply encrypted and difficult to detect once inside a computer. The Flame virus has the capacity to take over a computer's peripherals, record Skype conversations, take pictures through a computer's camera, and transmit information via Bluetooth to any nearby device.

If the world's most sophisticated governments are developing computer viruses, what guarantee is there that something won't go wrong? How can we be sure that they won't "escape" and infect a much broader class of systems, or be adopted for other uses, or that future rogue states or terrorists won't find a way to turn them on their creators? No economy is more vulnerable than that of the United States, and it is arrogance to believe that U.S. cyber superiority (to all except perhaps China) provides it with impenetrable security from attack.

Unfortunately the solution is not so simple as just building better anti-virus programs. Virus protection and virus development constitute an uneven arms race. A virus can be just a couple hundred lines of computer code, compared to hundreds of thousands of lines for anti-virus programs, which must be designed to detect wide classes of enemies.

We are told not to worry about large-scale cyber meltdowns, because none has occurred, and governments are being vigilant. Unfortunately, another lesson of the financial crisis is that most politicians are congenitally incapable of making difficult choices until risks actually materialize. Let us hope that we are lucky for a while longer. ◆