What pandemics can teach us about protecting the Internet

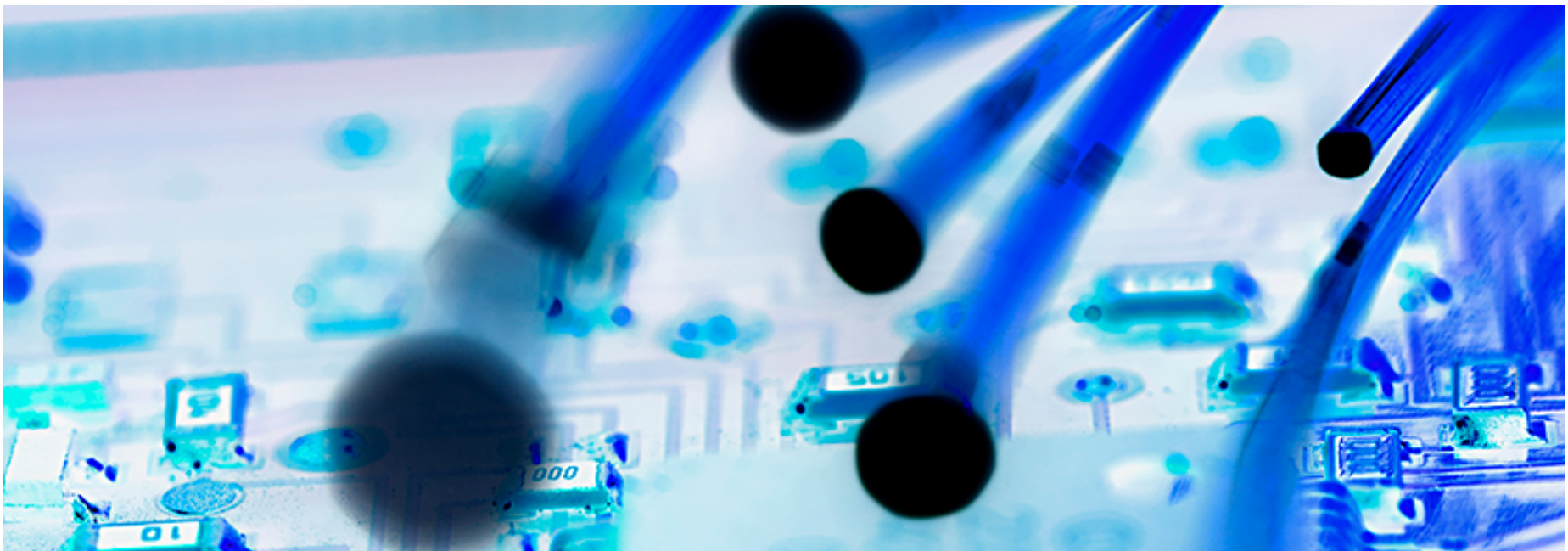
April 26, 2015

How best practices from global health and financial crises can help us develop a global governance framework to protect the Internet from a systemic attack

Roslyn Galbo

Head of International for Commercial Markets Zurich North America

About this expert



In spring 2007, the Internet went dark for much of Estonia. Hackers overwhelmed networks in a wave of distributed denial-of-service attacks that shut down Web sites of the government, banks, universities and news media. Estonia ended the siege by blocking international Internet traffic, cutting the most wired country in Europe off from the World Wide Web.

So far, Internet outages have largely been localized and fixed quickly. But what if the attack went beyond a corporation or a country to affect an entire geographical region, such as North America or Europe?

Despite jokes about popular posts “breaking the Internet,” a real Web shutdown could wreak serious damage. More and more of our world is connected to the Internet. Supervisory control and data acquisition (SCADA) systems, which allow critical infrastructure to be controlled or monitored remotely, pass through communications channels such as the Internet. SCADA systems are used in manufacturing, transportation, energy and other sectors. The Internet of Everything promises to connect even more devices, processes and equipment. The real world depends more than ever on the virtual one, and damage to the virtual world can be very real indeed.

Cyber destruction is real, not virtual

“The risk of a cyber attack on a grand scale, or one that sets off a cascade of failures throughout the system, is an increasingly realistic threat” says Javier Solana, President of ESADEgeo Center for Global Economy and Geopolitics. “An effective governance framework is a necessary pre-condition for society to reap the massive benefits of new technologies. This governance of cyberspace should be global and inclusive in nature, based on a multi-stakeholder approach and flexible enough to adapt to rapidly-evolving challenges ”

Interconnectivity means the damage can spread far. “Increasing interconnectedness raises the potential for systemic and cascading cyber crisis, with real consequences for the economy”, Mr. Solana adds, “and there are no borders.”

In that way, cyber attacks resemble disease and even money, which flow around the world despite governments’ best efforts to stop or control them.

When a disease pandemic breaks out, the World Health Organization steps in. When the financial crisis went global, the Bank for International Settlements helped to limit the damage.

With the Internet, “there are plenty of people you can call, but nobody has a comprehensive overview or mandate,” says Axel Lehmann, Group Chief Risk Officer and Regional Chairman EMEA at Zurich Insurance Company. “I’m not sure whether we need another organization or whether we should better coordinate and leverage [what is currently in place]. The point is how to preserve all the great benefits and opportunities we have through the Internet.”

The Internet already has a number of organizations that govern certain technical aspects. The Internet

Corporation for Assigned Names and Numbers, or ICANN, is a private-sector group that coordinates the Internet's naming system. The International Telecommunication Union, or ITU, is a United Nations agency that ensures information and communication technology systems interconnect seamlessly. The Internet Governance Forum, or IGF, is a means for Internet stakeholders such as governments, the private sector, technical providers and civil society to discuss public policy under the auspices of the U.N. Other organizations address non-technical aspects. For example, Interpol helps investigate cyber crime, which often crosses borders.

Within the private sector, "we have pretty solid technical standards," Mr. Lehmann says. "On a state-to-state level, when it comes to state security and war, there also is some coordination. In the middle field, concerning relations between the public and private, as well as the third sector, there's a lot of gray. Reality shows that when there is a cyber attack, you're not just interested on your own. You have to rely on a network. You need to get some state information. You can compare it to the financial sector before the crisis in 2008."

A few months after the 2008 collapse of Lehman Brothers set off the global financial crisis, the international Financial Stability Forum was enlarged into the Financial Stability Board and empowered to address the sector's vulnerabilities. In addition, the Basel III accord, under the auspices of the BIS and the Group of 20, provided reforms to strengthen the banking sector, including stress tests to uncover weaknesses.

"In the financial sector, we have a kind of global governance, with the FSB, Basel III and the G-20," Mr. Lehmann says. Resulting best practices could provide an example for the cyber world. "Stress tests, especially at the intersection of the Internet world and the real world, could be a win-win," he adds.

Another model is the World Health Organization. "You have an authority that is sharing information and it's voluntary how you apply it," he says. "The topic of cyber risk is so big that you can't have one authority for taking action. But you can have a central point for sharing information and adding value so companies can use it on a voluntary basis."

Some corners of cyber space have successfully forged public-private partnerships. For example, U.S. companies report cyber incidents to the Federal Bureau of Investigation and to the U.S. Computer Emergency Readiness Team, or US-CERT, which can then alert other companies to any systems vulnerabilities.

New territory, new rules

Another goal may be to lay down some rules of the game. There are globally accepted rules for trade, land, the sea and outer space. "We don't have [these types] of habits or codes in the Internet," Mr. Solana says. "They will have to include elements of private property, public property, etc. That will be very difficult to do."

Part of the point is to make cyber space safe from geopolitics. "What we have to do is construct a governance that is not overly technical, but can isolate or prevent global geopolitical problems that come to complicate the life of the Internet. The Internet is more than the national security of countries. It's economic security of companies," Mr. Solana says.

Choking off the Internet in a form of cyber protectionism "could be 'beneficial' to a country that doesn't want people complaining about human rights, but at the same time it would clash with the economic need to export and import and also the need to have open channels of communication with the rest of the world," he says. "For companies to be safe and states to be prosperous, they have to see how they

can isolate cyber space from being taken over by geopolitics."

A robust governance organization will have to engender trust from all stakeholders, especially in light of exposed and suspected cyber espionage and attacks by national governments. A global cyber public-private governance body could reflect the anti-hierarchical nature of the Internet itself, in the way that the G-20 has no boss or secretariat. Everyone will have to weigh trust versus suspicion, and risks versus benefits, but the reality is that failure to act is no longer an option as our dependence on the Internet is increasing while cyber attacks are mounting in number and cost.

"Is there a future tipping point where the risks get greater than the benefit?" Mr. Lehmann of Zurich Insurance Group asks. "How would that affect trust? What would that do to the economy?"

Mr. Solana hopes to keep us from a situation where we have to ask that question. "The wish is to help organize, step by step, some governance that would allow cyber space to be more stable. Even if we cannot solve 100% of the problems, then 60% is better than none."

Download the reports here

(1.85 MB/PDF)

(316.7 KB/PDF)

Related articles

April 26, 2015
Cyber governance: a holistic and global approach

April 26, 2015
The $445 Billion cyber risk gap

April 26, 2015
Global cyber governance preparing for new business risks

Related Topics

› **Cyber risk**