Should the Internet have an 'off' switch?

February 21 2011, By Jon Swartz

A raging debate over new legislation, and its influence on the Internet, has tongues wagging and fingers pointing from Silicon Valley to Washington, D.C.

Just as the Egyptian government recently forced the Internet to go dark, U.S. officials could flip the switch if the Protecting Cyberspace as a National Asset legislation becomes law, say its critics.

Proponents of the bill, which is expected to be reintroduced in the current session of Congress, dismiss the detractors as ill-informed - even naive.

The ominously nicknamed Kill Switch bill is sure to be a flashpoint of discussion at the RSA Conference, the nation's largest gathering of computer-security experts that takes place here this week. The debate is sure to intensify after the Obama administration announced Tuesday a new policy on Internet freedom, designed to make it harder for repressive governments to suppress dissent on the Internet - particularly on Facebook and Twitter.

The bill - crafted by Sens. Joseph Lieberman, I-Conn.; Susan Collins, R-Maine; and Tom Carper, D-Del. - aims to defend the economic infrastructure from a cyberterrorist attack. But it has free-speech advocates and privacy experts howling over the prospect of a government agency quelling the communications of hundreds of millions of people.

"This is all about control, an attempt to control every aspect of our existence," says Christopher Feudo, a cybersecurity expert who is chairman of SecurityFusion Solutions. "I consider it an attack on our personal right of free speech. Look what recently occurred in Egypt."

Its critics immediately dubbed it Kill Switch, suffusing it with Big Brother-tinged foreboding. "Unfortunately, it got this label, which is analogous to death panels (during the health care debates)," says Mark Kagan, director of research at Keane Federal Systems, an information-technology contractor for the government.

The disruption to communications and economic activity "could be catastrophic," says Marc Rotenberg, executive director of the Electronic Privacy Information Center.

Computer-security expert Ira Winkler, a staunch advocate of the legislation, counters, "The fact that people are complaining about this fact is grossly ignorant of the real world. The fact critical infrastructure elements are even accessible to the Internet is the worst part to begin with."

The overheated debate takes place against the backdrop of revolution in the Middle East and a recent breach of Nasdaq's computer system. Both underline the power of the Internet, its vulnerability and the importance of cybersecurity.

It also underscores the delicate balance between protecting the Internet - the largest communications device - and unfettered free speech.

The autocratic government of former Egyptian president Hosni Mubarak ordered the shutdown of four major Internet service providers, effectively shuttering the Internet in Egypt for several days. Could that happen in the U.S. if the bill becomes law?

In the U.S., there are 2,000 to 4,000 Internet providers, many of whom virulently oppose government interference that would put a clamp-down on their businesses.

"When it comes to practicalities, I would be surprised if anything comes to (a kill switch)," says Reputation.com CEO Michael Fertik, a lawyer with expertise in constitutional law and Internet privacy law. "If (the bill and president) stray too far, it would be extremely unpopular."

A national necessity?

Last month, Senate Majority Leader Harry Reid, D-Nev., and other congressional members introduced a placeholder bill and stressed that a cybersecurity measure is a top priority for the 112th Congress.

Carper, Collins and Lieberman have yet to announce plans to reintroduce the bill. But it is likely to be included as part of a larger, more comprehensive bill that includes other bits of legislation, say sources close to Lieberman who are not authorized to speak publicly about the bill.

"There can be no debate over whether our nation needs to improve its cyberdefenses," Lieberman, chairman of the powerful Senate Committee on Homeland Security and Governmental Affairs, said in a statement. "Our legislation is designed to improve these defenses, while protecting the fundamental freedoms that we all cherish."

Lieberman did not comment on whether the bill will be reintroduced.

Proponents of the bill say it is narrowly crafted and does not intend to limit speech but to eliminate the vulnerability of critical systems such as banks, the power grid and telecommunications from attacks by terrorists or agents of hostile countries.

Indeed, the bill specifically does not grant the president power to act unless a cyberattack threatens to cause more than $25 billion in damages in a year, kill more than 2,500 people or force mass evacuations. The president would have the ability to pinpoint what to clamp down on without causing economic damage to U.S. interests, for anywhere from 30 to 120 days with the approval of Congress, according to the bill.

"This is not Big Brother," says Tom Kellermann, vice president of security awareness at Core Security Technologies, and a former security expert for the World Bank. "It's not about shutting off the Internet, but taking a scalpel to command control to key services to protect them."

Winkler, chief security strategist of TechnoDyne, a systems-integration specialist for financial institutions, pharmaceutical companies and government agencies, agrees. "Nobody is giving Obama the ability to kill Twitter access," Winkler says. "There might possibly be unintended consequences, but people are ignoring imminent harm because there may be theoretical harm if the country devolves into a state of anarchy."

Examples abound, say Kellermann and others, underscoring the threat.

More industries could be at risk, Kagan and others warn. "It's 10 years after 9/11, and some companies still do not do a good job defending their computer systems," Kagan says, pointing to major chemical facilities as prime targets.

"Espionage and crimes have exploded on the Internet," Kellermann says. "There has been anarchy over attempts to leverage assets. This closes the spigot on attempted attacks by hostile forces."

Cyberthreats aside, deep questions persist over what critics claim is the bill's heavy-handed approach, what it means to free speech and whether it can be enforced practically.

The crux of the issue, to computer-law expert Fertik and others, is: If the Internet is a national asset, should it be nationalized?

"Determining where the Internet connects to infrastructure is hard to define and impose," Kagan says.

"In its current form, the legislation offers no clear means to check that power," says Timothy Karr, campaign director for media-policy group Free Press, a non-profit organization.

A 1934 federal law that created the Federal Communications Commission allows the president to "authorize the use or control" of communications outlets during moments of emergency of "public peril or disaster." The Lieberman-led bill would be considered a specific extension of that and would let the nation's chief executive prioritize communications on the Internet, says Fertik.

A provision in the bill would let the president take limited control during an emergency and decide restrictions. "It, essentially, gives the president a loaded gun," Fertik says.

"Say there is a mounted attack from a terrorist group on the Internet," Fertik says. "(The law) could present the president with a kill switch option. But what are the conditions, and how far does (the law) go?"

The debate extends to minutiae in the bill's wording.

It neither expressly calls for the creation of an Internet kill switch nor does it exclude one. It only requires the president to notify Congress before taking action, and it specifically prohibits judicial review of the president's designation of critical infrastructure. The non-profit Center for Democracy and Technology, in a measured letter to Lieberman, Collins and others, wants more specifics on the sweep of "emergency"

measures mentioned in the bill.

"In our constitutional system of checks and balances, that concentrates far too much power in one branch of government," says Karr. "The devil is always in the details, and here the details suggest that this is a dangerous bill that threatens our free-speech rights."

Giving the president broad power to "interfere" with the Internet - even bottling up chunks of it in the name of national security - would require him to go to court to stop communications, says Michelle Richardson, legislative counsel for the American Civil Liberties Union.

What's more, a new law may be next to impossible to administer widely, technology experts say.

"Whether nuclear or the Internet, there is no 'off' button or switch. There is a clear chain of command," Kagan says. "This notion of an all-consuming switch only happens in the movies."

Mubarak was able to temporarily silence the Internet because there are a small number of Internet providers in Egypt. Yet, even with the nationwide digital blockade, activists still communicated effectively, using old-fashioned methods.

Silencing portions of the Internet faces a steeper challenge in the U.S., where there are thousands of Internet providers and where the federal government's previous efforts to clamp down on hostile threats have met with little success, says EPIC's Rotenberg.

He points to a non-Internet example, the struggle to contain the nation's borders. "That was tried with (the Department of Homeland Security) on the border fence, and it was a disaster," Rotenberg says.