

Sun Journal

State

Kill-switch critics cool to Collins' new cyber security bill

By [Steve Mistler, Staff Writer](#)

Published Feb 23, 2011 12:00 am | Last updated Feb 23, 2011 12:00 am

Republican U.S. Sen. Susan Collins' latest proposal to beef up the country's cyber security has a new name and language explicitly denying the president the so-called "kill switch" power to unilaterally shut down the Internet.

But so far the legislation's makeover has failed to win over the technology community, libertarians and civil rights advocates, who worry the bill still gives the president and the government too much power to disrupt Internet communications.

Collins and her co-sponsors last week submitted the Cyber Security and Internet Freedom Act of 2011, a sequel to a proposal that stalled last session when lawmakers couldn't decide which federal agency should be granted oversight.

Earlier this year, Collins and Sen. Joseph Lieberman, I-Conn., [said they planned to reintroduce](#) the cyber security bill. Those plans were quickly assailed by critics of last year's bill who cited events in Egypt, where former President Hosni Mubarak attempted to quell anti-government protests by shutting down that country's Internet access.

Collins and Lieberman called comparisons between their bill and Mubarak's actions "specious." They said their legislation targeted only critical infrastructure sites, such as the energy grid, water supply or financial networks.

The new proposal adds language that prohibits the president or any other officer or employee of the federal government from shutting down the Internet.

But Bruce Schneier, a national [security expert](#), isn't convinced that the new proposal will do anything to help secure the country's cyber infrastructure.

"Help? The ability to kill the Internet is what the bad guys want," Schneier said. "Deliberately engineering it into the Internet would harm Internet security, not help it."

Collins said the Communications Act of 1934 already gives the president kill-switch power, and that her legislation would remove ambiguity in the law and replace it with specific protocols defined by a "national or regional catastrophe," such as an attack resulting in mass casualties, economic losses and mass, prolonged evacuations.

But Schneier said targeting specific cyber infrastructure for shutdown could have unforeseen consequences. Last summer [he wrote that](#) if the government decided to shut down the Web access of financial institutions, it had no way of knowing the impacts on ATM machines or stock exchanges.

Additionally, Schneier said, engineering a selective shutdown switch for specific infrastructure such as the power grid could make the country more vulnerable to attack.

"We would make the job of any would-be terrorist intent on bringing down the Internet much easier," Schneier wrote. "And given how unlikely the risk is, any actual shutdown would be far more likely to be a result of an unfortunate error or a malicious hacker than of a presidential order."

Libertarian groups, such as the Cato Institute, are also skeptical of the proposal. After the new legislation was unveiled last week, Jim Harper, an analyst for Cato, [wrote that the](#) Fifth Amendment to the U.S. Constitution prohibits the federal government from seizing private assets.

Harper added that it didn't matter if the kill switch targeted specific infrastructure.

"The Internet kill-switch debate is not about the precision or care with which such a policy might be designed or implemented," he wrote. "It's about the galling claim on the part of senators Lieberman, Collins and Carper that the U.S. government can seize private assets at will or whim."

The reworked proposal has also yet to win support from the American Civil Liberties Union.

The ACLU's legislative counsel Michelle Richardson said Tuesday that the bill has "substantial problems" that could infringe upon First Amendment rights. She said the ACLU hoped the bill's sponsors would consider creating a court system to review any presidential order to shut down specific areas of the Internet.

Collins defended the legislation during a lengthy Feb. 17 speech from the Senate floor. She said current laws were "outmoded" and that the Communications Act already gave the president broad powers that her bill seeks to limit.

The measure would prohibit a targeted shutdown for a total of 120 days. A shutdown exceeding that threshold would require congressional action and oversight.

She said the bill also forbids the critical infrastructure definition from including Internet systems protected by the First Amendment. The proposal also gives the owner of a so-called critical infrastructure system the ability to challenge the designation in court.

"I would like to stress that the need for Congress to pass a comprehensive cyber security bill is more urgent than ever," Collins said.

She said the Senate's sergeant at arms reported last year that computer systems of Congress and the White House were under cyber attack an average of 1.8 billion times per month.

"We cannot afford to wait for a 'cyber 9/11' before our government finally realizes the importance of protecting our digital resources, limiting our vulnerabilities and mitigating the consequences of penetrations to our networks," she said.