WebMemo
Published by The Heritage Foundation
No. 3166
February 22, 2011

Internet "Kill Switch": Mapping Out Government's Proper Role in Cybersecurity

Paul Rosenzweig

Once again, Congress has begun consideration of a comprehensive cybersecurity bill. Most of the provisions of the bill that eventually emerges from Congress will be uncontroversially good—better education is never wrong.

But one aspect of the bill now making its way through the Senate deserves a great deal more public debate and consideration: the scope and extent of the government's role in defending the Internet from external threats and, in particular, the extent to which the government can order private-sector actors to take action (including disconnecting from the Internet) in times of cyber emergency.

The Dangers of Government Overreach. When similar legislation was first introduced two years ago, the powers that were granted to the President were broad indeed—so broad that some dubbed those powers an "Internet kill switch" because of the effective power to turn off the Internet altogether.

The more recent proposals seem more circumspect. According to reports, the bill introduced last week by Senators Joe Lieberman (ID–CT), Susan Collins (R–ME), and Tom Carper (D–DE) will apply the President's emergency powers only to critical infrastructure. The President would be given the power to "issue a declaration of a national cyberemergency." After such a declaration the Department of Homeland Security (DHS) would be authorized to demand that critical companies "immediately comply with any emergency measure or action" decreed. Most notably, no "notice" would be required "before mandating any emergency measure or actions." Furthermore, a company could be added to the "critical" infrastructure list one moment and ordered by DHS to "immediately comply" with its directives the next.

The Importance of Government Capacity. The problem is indeed a challenging one. Clearly, the federal government needs the ability to protect its own interests, some of which require use of the private-sector portions of the Internet. Likewise, the government is charged with providing "for the common defense," and all Americans would expect it to play a role in defending, say, the West Coast electrical grid against a Chinese assault. The recent report of Chinese infiltration of Canadian government computers is a salient demonstration of the need for some defensive measures. And the reality is that if pre-enforcement judicial review of any governmental order is required, it is possible that the governmental response will be delayed so long that it proves ineffective.

But equally clearly, giving the government power over the private sector and the Internet is fraught with peril to civil liberties. Even though the legislation has explicit language denying presidential power to cut Americans off from the Internet gener-

This paper, in its entirety, can be found at:
http://report.heritage.org/wm3166

Produced by the Center for Legal & Judicial Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

ally (and even though any President of either party should not be presumed to exercise powers granted in a dictatorial way), the recent experiences in Egypt make it clear how relatively easy it is for an autocratically minded leader to take control of private conduct. And even when government acts with good intent, mistakes happen—for example, the recent error in which DHS mistakenly seized a number of innocent domain names that it thought were tied to child pornography but were not. Post-enforcement judicial review is of less value after the order has already been given and implemented.

Balance of Power. So this challenge is not readily susceptible to a rote answer based on ideology. To be sure, conservative principles generally favor private-sector action over governmental control, but they do not answer the narrower question of when the government should, in an emergency, have the power to step in and override the private sector's actions.

In the end, however, the balance should be struck against excessive governmental power, not out of fear of its abuse but rather because the premise of the requested authority lies in a false assumption about the rapidity with which a response will be required. When a cyber attack is perceived to occur at the pace of milliseconds, it may be that the deterrent or defensive response will need to occur with equal rapidity. But this is so fast that governmental action, if it is to be effective at all, may need to proceed without even the time for the presidential declaration and DHS action that is contemplated by the draft legislation. Rather, it is possible (indeed, likely) that some subordinate commanding officer may feel compelled (and authorized) to act without higher authorization if the commander perceives that a cyber attack has begun. And what is true for the military may also be true of private actors who are protecting their own networks—they may feel the need to act instantaneously without the benefit of reflection.

This perception of the need for rapidity reflects a sea-change in concept. The physics of the Internet destroys time and space.[1] Even in the nuclear domain, the imminence of the threat was measured in minutes, allowing the development of processes (like the classic nuclear code "football") that permitted a considered, albeit hurried, human response. The cyber domain is often characterized as one in which a near-instantaneous response is necessary.

That characterization may not, however, be accurate, and its prevalence may actually be pernicious. A counter-response may be essential immediately as a purely defensive measure, but it is likely that a deterrence-based cyber response can be delayed without significant cost. As Martin Libicki pointed out in a recent RAND study, a cyber response is unlikely to be able to disable a cyber attacker completely. As a consequence, for deterrence policy, more important than the speed of the response "is the ability to convince the attacker not to try again. Ironically, for a medium that supposedly conducts its business at warp speed, *the urgency of retaliation is governed by the capacity of the human mind to be convinced, not the need to disable the attacking computer before it strikes again.*"[2]

Be Leery. And if that is the case, if cyber deterrence is less dependent on the quickness of a response than on its certainty, then the argument for strong presidential authority is appreciably diminished. To be sure, this is not an area where one can express a policy judgment with a degree of certainty, but based on what is known today, policymakers should be very leery of any proposal that grants the President plenary authority over the Internet.

*—**Paul Rosenzweig** is Visiting Fellow in the Center for Legal & Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*

1. Paul Rosenzweig, "10 Conservative Principles for Cybersecurity Policy," Heritage Foundation Backgrounder No. 2513, January 31, 2011, at *http://www.heritage.org/Research/Reports/2011/01/10-Conservative-Principles-for-Cybersecurity-Policy.*
2. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), p. 62 (emphasis added).