



Written by [Raven Clabough](#) on December 19, 2011

NDAA Would “Quash Dissent” on Internet

A major component of the criticism against the NDAA is that it labels all of the United States as a “battlefield” in the “War on Terror,” thereby treating virtually all American citizens as potential terrorists. But in addition to that, buried deep in the massive paperwork of the bill is a provision that would allow the Pentagon to treat the Internet as a “battlefield” as well, in order to defend our Nation, Allies and interests.



Section 954 of the NDAA, entitled “Military Activities in Cyberspace,” [states](#):

Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct *offensive operations* in cyberspace to defend our Nation, Allies and interests subject to (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution.” [Emphasis added.]

The Pentagon had already voiced an interest in tightening control over the Internet in July, when Deputy Defense Secretary William Lynn [announced](#) that the Pentagon would be treating cyberspace as an operational domain in its Department of Defense Strategy for Operating in Cyberspace:

The United States reserves the right, under the laws of armed conflict, to respond to serious cyber attacks with a proportional and justified military response at the time and place of our choosing. In the 21st Century, bits and bytes can be as threatening as bullets and bombs.

Keystrokes originating in one country can impact the other side of the globe in the blink of an eye. Treating cyberspace as a domain means that the military needs to operate and defend its networks, and to organize, train, and equip its forces to perform cyber missions.

The Department of Defense Strategy for Operating in Cyberspace ([pdf](#)) claims, Hackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks and systems that control critical civilian infrastructure.

That strategy is broken down into several components: treating cyberspace as a domain for the Department of Defense to take advantage of; employing new defense operating concepts to protect Department of Defense networks; partnering with other federal departments as well as private companies such as Google and Facebook to enable the entire strategy; building relationships with American allies to strengthen cybersecurity; and rewarding those who use their technology to capture



Written by [Raven Clabough](#) on December 19, 2011

potential cyber threats.

While no specifics have been outlined, *Wired* writes:

Its likely to include things like unleashing a worm like the Stuxnet worm that damaged Irans nuclear centrifuges, hacking into another countrys power grid to bring it down, disabling websites via denial-of-service attacks, or as the CIA has already done with some collateral damage, hacking into a forum where would-be terrorists meet in order to permanently disable it.

It should come as no surprise that the United States is prepared to defend itself, Lynn declared. Just as our military organizes to defend against hostile acts from land, air and sea, we must also be prepared to respond to hostile acts in cyberspace.

Likewise, Defense Secretary Leon Panetta issued a statement along with the release of the new strategy asserting that it was critical that federal officials strengthen our cyber capabilities to address the cyber threats were facing. He continued, "I view this as an area in which we're going to confront increasing threats in the future and think we have to be better prepared to deal with the growing cyber challenges that will face the nation."

Lynn maintained the same urgent tone when he added, Our assessment is that cyber attacks will be a significant component of any future conflict, whether it involves major nations, rogue states, or terrorist groups.

Wired points out: Despite mainstream news accounts, theres been no documented hacking attacks on U.S. infrastructure designed to cripple it. A recent report from a post-9/11 intelligence fusion center that a water pump in Illinois had been destroyed by Russian hackers turned out to be baseless.

Meanwhile, the U.S. Congress has been busy passing legislation to regulate the Internet. The latest controversial item is the Stop Online Piracy Act (SOPA), which would give the Justice Department authority over websites and copyright infringement through an amendment proposed by Rep. Lamar Smith (R-Texas). Rep. Darrell Issa (R-Calif.), a key critic of SOPA, declared,

The managers amendment retains the fundamental flaws of its predecessor by blocking Americans ability to access websites, imposing costly regulation on web companies and giving Attorney General Eric Holders Department of Justice broad new powers to police the internet.

The *International Business Times* (IBT) [noted](#) that both the NDAA and SOPA bills are aimed at quashing dissent:

The lobbyists who [have spent nearly \\$100 million](#) to push for the Stop Online Piracy Act's passage will do everything within their power to ensure that money does not go to waste. For them, the copyright-holders must be protected at all costs, including at the expense of all Americans' liberties.

The real purpose of the SOPA bill (and its sister bill, PIPA [Protect IP Act], in the Senate) is to target the web-based movements that have fueled revolutionaries both here and abroad.

According to the *IBT*, despite the touted aim of SOPA, its intent is actually not to stop piracy but to shut down Anonymous, Reddit, and even Twitter and YouTube whenever theyre being used by people who want to bring about change.

The *International Business Times* also pointed out the same type of insidious agenda in the NDAA:

Certain provisions of the National Defense Authorization Act have a similar purpose at heart. They



Written by [Raven Clabough](#) on December 19, 2011

are ostensibly aimed at al-Qaeda and other terrorist groups, and will likely lead to some unconstitutional arrests of Muslim terror suspects. But the other purpose of the indefinite detention provisions, and the reason it is before the Congress now, is to allow the government to arrest those who loudly disagree with it.

The *IBT* contended that the Internet provisions in the NDAA seek to destroy whistleblowers in independent news media from exposing corruption in the government, adding,

In other words, the Pentagon is afraid that with the dissemination of the Internet, the spread of information or ideas “not consistent with U.S. government themes and messages” could be too powerful and dangerous to national security.

Fury over the NDAA and SOPA proposals is prompting protesters across the country to demonstrate and to tweet President Obama urging him to veto both bills. The two pieces of legislation have united groups from both ends of the political spectrum over concerns that once these measures become law, there is nothing to stop further infringements upon the civil liberties of American citizens.

One such opposition group, known as Anonymous, has already planned to target specific politicians who have supported the NDAA, including Sen. Robert Portman (R-Ohio), who received \$272,853 from special interest groups to support the NDAA.

“Robert J. Portman, we plan to make an example of you,” declared an Anonymous operative.



Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



Subscribe

What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.