

[DISCUSSION DRAFT]

FEBRUARY 23, 2017

115TH CONGRESS
1ST SESSION

H. R. _____

To amend title 18, United States Code, to provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. GRAVES of Georgia introduced the following bill; which was referred to the Committee on _____

A BILL

To amend title 18, United States Code, to provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Active Cyber Defense
5 Certainty Act”.

1 **SEC. 2. EXCLUSION FROM PROSECUTION FOR CERTAIN**
2 **COMPUTER CRIMES FOR THOSE TAKING AC-**
3 **TIVE CYBER DEFENSE MEASURES.**

4 Section 1030 of title 18, United States Code, is
5 amended by adding at the end the following:

6 “(k) CYBER DEFENSE MEASURES NOT A VIOLA-
7 TION.—

8 “(1) GENERALLY.—It is a defense to a prosecu-
9 tion under this section that the conduct constituting
10 the offense was an active cyber defense measure.

11 “(2) DEFINITIONS.—In this subsection—

12 “(A) the term ‘victim’ means an entity
13 that is a victim of a persistent unauthorized in-
14 trusion of the individual entity’s computer;

15 “(B) the term ‘active cyber defense meas-
16 ure’—

17 “(i) means any measure—

18 “(I) undertaken by, or at the di-
19 rection of, a victim; and

20 “(II) consisting of accessing
21 without authorization the computer of
22 the attacker to the victim’ own net-
23 work to gather information in order to
24 establish attribution of criminal activ-
25 ity to share with law enforcement or
26 to disrupt continued unauthorized ac-

1 tivity against the victim’s own net-
2 work; but
3 “(ii) does not include conduct that—
4 “(I) destroys the information
5 stored on a computers of another;
6 “(II) causes physical injury to
7 another person; or
8 “(III) creates a threat to the
9 public health or safety; and
10 “(C) the term ‘attacker’ means a person or
11 an entity that is the source of the persistent un-
12 authorized intrusion into the victim’s com-
13 puter.”.