[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”.

VerDate Nov 24 2008 11:13 Feb 23, 2017 Jkt 000000 PO 00000 Frm 00001 Fmt 6652 Sfmt 6201 C:\USERS\KLMERY~1\APPDATA\ROAMING\SOFTQUAD\XMLMETAL\7.0\GEN\C\GRAVGA~1
SEC. 2. EXCLUSION FROM PROSECUTION FOR CERTAIN COMPUTER CRIMES FOR THOSE TAKING ACTIVE CYBER DEFENSE MEASURES.

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

“(k) CYBER DEFENSE MEASURES NOT A VIOLATION.—

“(1) GENERALLY.—It is a defense to a prosecution under this section that the conduct constituting the offense was an active cyber defense measure.

“(2) DEFINITIONS.—In this subsection—

“(A) the term ‘victim’ means an entity that is a victim of a persistent unauthorized intrusion of the individual entity’s computer;

“(B) the term ‘active cyber defense measure’—

“(i) means any measure—

“(I) undertaken by, or at the direction of, a victim; and

“(II) consisting of accessing without authorization the computer of the attacker to the victim’s own network to gather information in order to establish attribution of criminal activity to share with law enforcement or to disrupt continued unauthorized ac-
tivity against the victim’s own net-
work; but

“(ii) does not include conduct that—

“(I) destroys the information
stored on a computer of another;

“(II) causes physical injury to
another person; or

“(III) creates a threat to the
public health or safety; and

“(C) the term ‘attacker’ means a person or
an entity that is the source of the persistent un-
authorized intrusion into the victim’s com-
puter.”.