[DISCUSSION DRAFT]
ACTIVE CYBER DEFENSE CERTAINTY ACT – 2.0

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Active Cyber Defense Certainty Act''.

SEC. 2. EXCEPTION FOR THE USE OF ATTRIBUTIONAL TECHNOLOGY

Section 1030 of title 18, United States Code, is amended by adding at the end the following: "(k) EXCEPTION FOR THE USE OF ATTRIBUTIONAL TECHNOLOGY. ---

"(1) The provisions of this section shall not apply with respect to the use of attributional technology in regard to a defender who uses a program, code, or command for attributional purposes that beacons or returns locational or attributional data in response to a cyber intrusion in order to identify the source of an intrusion; if

"(A) the program, code, or command originated on the computer of the defender but is removed by an unauthorized user; and

"(B) the program, code or command does not result in the destruction of data or result in an impairment of the functionality of the attacker's computer system, or create a backdoor enabling intrusive access into the attacker's computer system."

SEC. 3. 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: ''(l) ACTIVE 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' own network to gather information in order to:

1) establish attribution of criminal activity to share with law enforcement and other United States Government agencies responsible for cybersecurity;

2) disrupt continued unauthorized activity against the victim's own network; or

3) monitor the behavior of an attacker to assist in developing future intrusion prevention or cyber defense techniques, but;

''(ii) does not include conduct that—

''(I) destroys or renders inoperable information that does not belong to the victim that is stored on a computers of another;

''(II) causes physical or financial injury to another person;

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

''(IV) exceeds the level of activity required to perform reconnaissance on an intermediary computer to allow for attribution of the origin of the persistent cyber intrusion;

''(C) the term 'attacker' means a person or an entity that is the source of the persistent unauthorized intrusion into the victim's computer; and

''(D) the term 'intermediary computer' means a person or entity's computer that is not under the ownership or control of the attacker but has been used to launch or obscure the origin of the persistent cyber-attack.''.

SEC. 4. NOTIFICATION REQUIREMENT FOR THE USE OF ACTIVE CYBER DEFENSE MEASURES

Section 1030 of title 18, Unites State Code, is amended by adding the following:
"(m) NOTIFICATION REQUIREMENT FOR THE USE OF ACTIVE CYBER DEFENSE MEASURES -

"(1) GENERALLY. - A victim who uses an active cyber defense measure under this section must notify the FBI National Cyber Investigative Joint Task Force prior to using the measure.

"(2) REQUIRED INFORMATION. - Notification must include the type of cyber breach that the person or entity was a victim of, the intended target of the active cyber defense measure, the steps taken to preserve evidence of the attacker's criminal cyber intrusion, as well as steps taken to prevent damage to intermediary computers not under the ownership of the attacker."

SEC. 5. SUNSET.

The exclusion from prosecution created by this Act shall expire 2 years after the date of enactment of this Act.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu