Active Cyber Defense Certainty Act

Bipartisan Bill Empowers Americans to Develop New Defenses Against Cyber Attacks

What it is:
The Active Cyber Defense Certainty Act (ACDC), H.R. 4036, which was introduced by Reps. Tom Graves (R-GA-14) and Kyrsten Sinema (D-AZ-09) on October 13, is a bipartisan bill that makes targeted changes to the Computer Fraud and Abuse Act (CFAA) to allow use of limited defensive measures that exceed the boundaries of one's network in order to monitor, identify and stop attackers. Specifically, ACDC gives authorized individuals and companies the legal authority to leave their network to:

1) establish attribution of an attack,
2) disrupt cyberattacks without damaging others' computers,
3) retrieve and destroy stolen files,
4) monitor the behavior of an attacker,
5) and utilize beaconing technology.

Allowing defenders to develop and deploy new tools will help deter criminal hacking.

Why it's needed:

- The CFAA, which was enacted in 1986, currently prohibits individuals from taking any defensive actions other than preventative protections, such as ant-virus software. ACDC is likely the most significant update to the CFAA since its enactment.
- Americans who take precautions, such as installing updates, purchasing anti-virus software and using strong passwords, are still falling victim to cyberattacks. Companies continue to suffer major breaches of their often sophisticated cyber defenses.

Questions & Answers

How would most defenders use Active Cyber Defense Techniques?
Most defenders would likely use active-defense techniques to perform "deep reconnaissance" of the hackers who originated the attack. For example, a defender using active-defense techniques could "follow the bread crumbs," back to the source of the attack. They could then attempt to attribute the source, "naming and shaming" the attacker, turn over relevant information to law enforcement, or simply learn the "vector" that the attacker took to execute the original malicious attack and avoid it.

How was the bill drafted?
The bill is the result of a lengthy feedback process, which began on March 3 when Rep. Graves introduced the first ACDC discussion draft. After incorporating feedback from the business community, academia and cybersecurity policy experts, including recommendations he received at his cybersecurity event in Atlanta on May 1, Rep. Graves introduced an updated discussion draft on

May 25. During the intervening period, Rep. Graves again solicited feedback and suggestions, which resulted in the formal introduction of the bill on October 13.

Are Active-Defense Techniques Effective?
Active-defense techniques can absolutely be effective. Even though most of these techniques are not legal under current law, the reality is that skilled defenders are already using them to thwart and deter attacks. ACDC unties the hands of law-abiding defenders to use new techniques to thwart and deter attacks, while also providing legal certainty for industry experts to innovate, which could spur a new generation of tools and methods.

Does the bill protect privacy rights?
Yes, it protects privacy rights by prohibiting vigilantism, forbidding physical damage or destruction of information on anyone else's computer, and prevents collateral damage by constraining the types of actions that would be considered active defense. These safeguards help ensure that active defense is only targeted at the source of the attack, while imposing a strict standard of care on the defender to ensure that innocent bystanders aren't impacted.

How will the bill impact innocent bystanders and avoid collateral damage?
ACDC has a very high standard for cyber defenders. If a defender behaves improperly or recklessly, they will still bear the full penalty of existing law. ACDC does not change the existing penalties for "unauthorized access"; it merely allows a legal defense for such access in cases where self-defense is clearly justified. The bill makes clear that if a person is inadvertently impacted by active-cyber defense, their right to sue for civil damages or injunctive relief is preserved. Defenders would be forced to take a very deliberate, step-by-step process of using active-cyber defense or they would still run the risk of civil and criminal penalties.

Additionally, the bill requires reporting to the FBI-led National Cyber Investigative Joint Task Force before taking active-defense measures, which will help federal law enforcement ensure defenders use these tools responsibly. The bill also includes a voluntary review process through the FBI Joint Taskforce that individuals and companies could utilize before using active-defense techniques, which will assist defenders in conforming to federal law and improving the technical operation of the measure.

Why not just let the FBI and DOJ respond?
The federal government plays a crucial role in investigating and prosecuting cyber-crimes. But it shouldn't stand in the way of victims who are capable of responding to an ongoing attack, nor should it stand in the way of industry innovating and creating new active-defense techniques. The FBI will continue to play the lead role but there is a mutual benefit to empowering individuals and organizations to actively defend themselves online. While DOJ and the FBI do great work, the number of cyberattacks far exceeds the government's ability to respond, identify and prosecute criminals.

Could active-defenders end up tangling with nation-state hackers?
ACDC requires reporting to the FBI-led National Cyber Investigative Joint Task Force before individuals or companies take active-defense measures. This should allow the FBI to de-conflict private actions that may overlap with law enforcement or involve a nation-state.