

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927

Minority (202) 225-3641

October 31, 2016

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Tim Murphy
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Upton and Chairman Murphy:

We are writing to ask that you hold hearings on the recent cyberattack that reportedly caused outages on many popular websites, including Twitter and Netflix. This incident raises new questions about the vulnerability of the internet and the ability of the United States to prevent such attacks in the future.

On Friday, October 21, 2016, Dynamic Network Services, Inc., known as Dyn, was hit by a distributed denial-of service (DDoS) attack directed at its server infrastructure.¹ Dyn offers domain-name-system (DNS) services to some of the most trafficked sites on the internet.² Attackers used a malicious software code, or malware, known as Mirai to organize a network of Internet of Things (IoT) devices to overwhelm Dyn's servers with 1.2 trillion bits of data every second.³ This volume of junk data left many popular websites inaccessible to legitimate users.⁴

¹ Dyn, *Dyn Statement on 10/21/2016 DDoS Attack* (Oct. 22, 2016) (online at dyn.com/blog/dyn-statement-on-10212016-ddos-attack/).

² *How an attack on a company you've never heard of crushed the internet*, Mashable (Oct. 21, 2016).

³ *Attacks on the Internet Keep Getting Bigger and Nastier*, Associated Press (Oct. 22, 2016).

⁴ *Cyberattack Knocks Out Access to Websites*, Wall Street Journal (Oct. 24, 2016).

The attack began at 7 a.m. and occurred in three waves, spreading westward across the United States throughout the day.⁵

A group known as New World Hackers claimed responsibility for the attack.⁶ They have claimed that this attack was simply a dry run for a much bigger target. The group's claims have not yet been verified.

DDoS attacks have become increasingly common in recent months. In September, a similar attack used hundreds of thousands of connected cameras and other IoT devices to attack security researcher and blogger Brian Krebs.⁷ At the time, security experts alleged that the Krebs attack was the largest attack DDoS ever recorded.⁸ Cybersecurity experts have found that the same type of malware was used in the attacks against Krebs and Dyn.⁹

This Committee is uniquely positioned to investigate this attack. As Chairman Upton indicated in a public statement, this is an area of serious concern for businesses and consumers.¹⁰ The expansion of technology and increasing connectivity of devices make it imperative that we understand what happened in this recent cyberattack and assess what can be learned from it. This could have wide-sweeping effects not only on telecommunications and Internet regulation, but also on many other areas under the Committee's jurisdiction. We urge you to hold hearings as soon as possible.

Sincerely,



Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce



Anna G. Eshoo
Ranking Member
Subcommittee on Communications
and Technology

⁵ *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, New York Times (Oct. 21, 2016).

⁶ *Attacks on the Internet Keep Getting Bigger and Nastier*, Associated Press (Oct. 22, 2016).

⁷ *Cyberattack Knocks Out Access to Websites*, Wall Street Journal (Oct. 24, 2016).

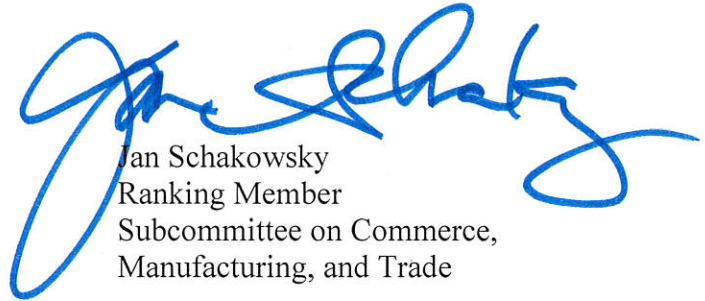
⁸ *Id.*

⁹ *Attacks on the Internet Keep Getting Bigger and Nastier*, Associated Press (Oct. 22, 2016).

¹⁰ Committee on Energy and Commerce, *Upton on Cyberattacks Against DNS Networks* (Oct. 21, 2016) (Press Release).



Diana DeGette
Ranking Member
Subcommittee on Oversight and
Investigations



Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade



Jerry McNerney
Member of Congress