



COMMITTEE ON
ENERGY & COMMERCE
DEMOCRATS
RANKING MEMBER FRANK PALLONE, JR.

FOR IMMEDIATE RELEASE

November 16, 2016

CONTACT

[Matt Schumacher](#) — (202) 225-5735

Pallone Opening Statement at Hearing on Recent Cyberattack

Energy and Commerce Ranking Member Frank Pallone, Jr. (D-NJ) submitted the following opening remarks for the record at a joint Subcommittee on Communications and Technology and Subcommittee on Commerce, Manufacturing, and Trade hearing titled “Understanding the Role of Connected Devices in Recent Cyber Attacks:”

There is truth to the saying — you don’t know what you have until it’s gone. Three weeks ago, a cyberattack on a single company — Dyn — left millions of Americans without access to some of the most popular websites on the internet.

This was a disruptive attack coming at a critical time. Citizens couldn’t get access to major news and weather sites. Commerce slowed. Online payment services went down.

And even though no one knew exactly what was happening, many guessed that the internet itself was under attack. We didn’t know how much bigger the outage could get or who was attacking us.

Fortunately, we now know that this particular attack was not as bad as it could have been. Looking ahead, we still don’t know if the last attack was a dry run or a road map for a larger, more crippling attack. But we do know now just how vulnerable our systems can be. As some of the witnesses testifying before us today have noted, future attacks could target our health care systems or critical infrastructure. Everything from the stock market to the energy grid is connected in some way.

That’s why I, along with ranking members Eshoo, DeGette, and Schakowsky, as well as Congressman McNerney, asked for this hearing. I was gratified that our Republican colleagues agreed that our committee needs to better understand these vulnerabilities.

So, what exactly happened? It appears a few hackers attacked a particularly crucial part of the internet’s infrastructure—the domain name service provider, Dyn. This one company helped keep a number of major websites online. So by attacking just one company, these cyber criminals were able to knock out a number of others.

But the way that these attackers went after Dyn is just as important as the effect of the attack. The hackers were able to turn our devices against us. They hijacked hundreds of thousands of seemingly innocent devices that so many consumers have in their homes—simple gadgets like digital video recorders and webcams.

The attackers were able to take over these connected devices because they could easily find the default passwords used by the device manufacturers. Some of these passwords were hardwired into the devices so that consumers couldn't change these weak passwords even if they wanted to.

That's why manufacturers of these devices need to take steps to address this problem. Better security is obvious. Hardwired default passwords are not acceptable.

And consumers may also have a role to play when it comes to device security. Using strong, unique passwords is critical. But the recent attack on Dyn makes it clear that consumers can't, and shouldn't be expected to fix this problem.

In fact, most people probably don't even know that their devices were used and those devices owners were not the ones affected by the attack. Instead, it was millions of internet users across the country who couldn't access many popular websites who were affected. Because of this dynamic, I am concerned that although device owners and manufacturers may be in the best place to fix the problems, they have the least incentive to do so. That's why, if we are going to really fix this, the government may need to take additional steps to keep us safe.

But before we reach that conclusion, we need to answer some tough questions. For instance, will regulations be effective, and what tradeoffs are we making if we regulate? What industry, if any, should be regulated? And what agency should be charged with this responsibility? I am hopeful that today's hearing will bring us closer to these important answers—and it's not a moment too soon because the next attack can come at any time.

With that, I'd like to thank all of our witnesses for being here today, and I'd like to yield the remaining balance of my time to Congressman McNerney.

###

democrats-energycommerce.house.gov | [Twitter](#) | [Facebook](#) | [Instagram](#) | [YouTube](#) | [Flickr](#)