

This really has been a tremendous effort, and so important for our country. This particular issue, obviously, is certainly a bipartisan issue.

I say that, Mr. Chairman, because our Constitution makes the first and foremost responsibility of the Federal Government to provide for the common defense. That is actually in the preamble of our Constitution.

In our modern world, those who are seeking harm to our Nation, to our citizens, to our companies, can use many different means, including attacks over the Internet to attack our Nation.

Recent cyber attacks on U.S. companies like Sony, Target, and Home Depot not only harm these companies, Mr. Chairman, but they harm the American citizens who do business with them, putting their most personal private information at risk.

These threats, as are well known, are coming from nation-states like North Korea, Russia, Iran, China, as well as cyber criminals seeking to steal not only personal information but also intellectual property and sensitive government information.

In today's digital world, we have a duty to defend ourselves against cyber espionage, and the best way to combat these threats is to first recognize the threat and combine private and government resources and intelligence. Mr. Chairman, that is exactly what this bill does.

Mr. Chairman, I think this bill will help to facilitate greater cooperation and efforts to protect our Nation's digital infrastructure, including power grids and other utilities and other services that everyday Americans rely on each and every day.

By removing barriers, which will allow private companies to voluntarily share their cybersecurity threat information with the Department of Homeland Security and/or other companies, I think we will in a very large way improve earlier detection and mitigation of potential threats.

Additionally, this legislation that we are debating on the floor today ensures that personal identification information is removed prior to sharing information related to cyber threats and that very strong safeguards are in place to protect personal privacy and civil liberties.

Mr. Chairman, I point that out because that was something that was discussed a lot by practically every member of the Homeland Security Committee. We were all very, very united on that issue. And I think that is an important critical component, a point to make, and it is reflected in this legislation.

As Mr. RATCLIFFE mentioned just earlier, 85 percent of America's critical infrastructure is owned and operated by the private sector—think about that, 85 percent—which means that cyber threats pose as much of an economic threat to the United States as they do to our security, and we have a

constitutional responsibility, as I pointed out in the beginning, to protect ourselves, to protect our Nation, to protect our American citizens from this ever-evolving threat.

So, Mr. Chairman, I would urge that all of my colleagues join me, join all of us on our committee, in voting in favor of this important legislation that will provide an additional line, and a very important line, of defense against cyber attacks.

The CHAIR. The Committee will rise informally.

The Speaker pro tempore (Mr. LOUDERMILK) assumed the chair.

MESSAGE FROM THE SENATE

A message from the Senate by Ms. Curtis, one of its clerks, announced that the Senate has passed a bill of the following title in which the concurrence of the House is requested:

S. 178. An act to provide justice for the victims of trafficking.

The SPEAKER pro tempore. The Committee will resume its sitting.

NATIONAL CYBERSECURITY PROTECTION ADVANCEMENT ACT OF 2015

The Committee resumed its sitting.

Mr. THOMPSON of Mississippi. Mr. Chairman, I yield 2 minutes to the gentleman from Virginia (Mr. CONNOLLY).

Mr. CONNOLLY. I thank my dear friend from Mississippi (Mr. THOMPSON), and I commend him and the distinguished chairman of the committee, Mr. McCAUL, for their wonderful work on this bill.

Mr. Chairman, we cannot wait. America cannot wait for a cyber Pearl Harbor. This issue—cybersecurity—may be the most complex and difficult challenge we confront long term as a nation.

In the wired 21st century, the line between our physical world and cyberspace continues to blur with every aspect of our lives, from social interaction to commerce. Yet the remarkable gains that have accompanied an increasingly digital and connected society also have opened up new, unprecedented vulnerabilities that threaten to undermine this progress and cause great harm to our country's national security, critical infrastructure, and economy.

□ 0945

It is long overdue for Congress to modernize our cyber laws to address those vulnerabilities present in both public and private networks. The bills before us this week are a step in the right direction, and I am glad to support them, but they are a first step.

Information sharing alone does not inoculate or even defend us from cyber attacks. Indeed, in the critical three P's of enhancing cybersecurity—people, policies, and practices—the measures before us make improvements primarily to policy.

I commend the two committees for working in a bipartisan fashion to improve privacy and transparency protections. More is still needed to safeguard the civil liberties of our constituents.

Further, I hope that the broad liability protections provided by these bills will, in fact, be narrowed upon further consultation with the Senate. Cybersecurity must be a shared public-private responsibility, and that includes the expectation and requirement that our partners will, in fact, take reasonable actions.

Moving forward, I hope Congress will build on this effort to address the security of critical infrastructure, the vast majority of which, as has been already pointed out, is owned and operated by the private sector.

The CHAIR. The time of the gentleman has expired.

Mr. THOMPSON of Mississippi. I yield the gentleman an additional 30 seconds.

Mr. CONNOLLY. We also need to strengthen our Nation's cyber workforce, devise effective data breach notification policies, and bring about a wholesale cultural revolution so that society fully understands the critical importance of good cyber hygiene.

The bottom line is that our vulnerability in cyberspace demands that we take decisive action and take it now, but much like the tactics used in effective cybersecurity, we must recognize that enhancing our cyber defenses is an iterative process that requires continuous effort.

I congratulate the staffs and the leadership of the committee.

Mr. McCAUL. Mr. Chairman, I yield 5 minutes to the gentleman from Georgia (Mr. LOUDERMILK), a member of the Committee on Homeland Security.

Mr. LOUDERMILK. Mr. Chairman, over the past 40 years, we have experienced advancements in information technology that literally have transformed business, education, government; it has even transformed our culture.

Information research that only a couple of decades ago would take days, months, maybe even years to accomplish is available, quite literally, at our fingertips and instantaneously.

Other aspects of our lives have also been shaped by this immediate access to information. Shopping, you can go shopping without ever going to a store. You can conduct financial transactions without ever going to a bank. You can even have access to entertainment without ever going to a theater.

These advancements in technology have not only transformed the way we access and store information, but it has also transformed the way we communicate.

No longer is instantaneous voice-to-voice communication only available through a phone call, but people around the world instantly connect with one another with a variety of methods, from email, instant text messaging, even video conferencing, and