Remarks by Vice President Pence at the DHS Cybersecurity Summit

National Security & Defense

Issued on: July 31, 2018

Alexander Hamilton U.S. Custom House
New York City, New York

4:24 P.M. EDT

THE VICE PRESIDENT: Well, thank you, Secretary Nielsen. And thank you for that kind introduction and for your leadership at the Department of Homeland Security. Would you all join me in thanking Secretary Kirstjen Nielsen for her leadership and for bringing together this historic summit today? (Applause.)

To the Secretary and to Secretary Perry, Director Wray, Director Alles, to all the public servants that are gathered here, and to all the leaders of industry and academia who've come from near and far: It is my honor to welcome you all at the close of the events today at the first-ever National Cybersecurity Summit. Thank you all for being here today. (Applause.)

And I bring greetings and gratitude for your participation in this conference from a great champion of American security, President Donald Trump. I'm here today on behalf of the President because cybersecurity is a major focus of this administration.

Over the last year, at the President's direction, we've taken unprecedented action to strengthen our digital infrastructure and defenses because we know that cybersecurity has never been more important to the American people.

America depends on the digital world more with every passing day, as all the industry leaders here know too well. It's opened countless new doors of opportunity, created extraordinary new sources of prosperity, and unleashed a new era of entrepreneurship and innovation that has infused nearly every aspect of our lives and our society.

Yet while this revolution has spurred new opportunities, as you all have discussed here today, it has also spawned new threats.

Criminal terrorists, foreign adversaries constantly prowling this digital domain represent a threat to this nation. And America's digital infrastructure is under constant cyberattack.

The federal government alone experiences hundreds of thousands of digital assaults every day. And across the entire country, the number of attacks on our digital infrastructure is impossible to calculate. Our digital foes are targeting every facet of our society.

They threaten our families' privacy, like the hackers who breached the credit bureau Equifax last year and made off with the Social Security numbers and other personal information of nearly 150 million Americans.

They extort our hard-earned money, as we saw in the North Korean "WannaCry" attack that held more than 200,000 devices in 150 countries hostage, demanding a ransom.

Foreign interests also routinely steal trade secrets from some of our most important industries. As our administration's recent 301 trade investigation found, for many years, China has directed bureaucrats and businesses to find and steal our nation's intellectual property and advanced technologies, especially those pertaining to our national defense.

Our cyber adversaries also seek to infiltrate our critical infrastructure, including our electrical grid, power stations, so that in some future conflict they might have the opportunity to shut down the nerve center of American energy and our national life.

They also target our economy. A single Russian malware attack last year cost a major American shipping company roughly $400 million. And in 2016, cyberattacks, it is estimated, cost our economy as much as $109 billion.

Cyber attackers also go after government at every level, such as in March, when criminal hackers hobbled the city of Atlanta and crippled many basic services for several days.

And as the American people know all too well, our adversaries increasingly use the digital world to manipulate, to divide, to chip away at our most cherished values.

In the face of these threats, the American people demand, and deserve, the strongest possible defense. And we will give it to them. (Applause.)

But sadly, previous administrations have let the American people down when it came to cyber defense. At the outset of this administration, it became clear from early on: In a very real sense, we inherited a cyber crisis. The last administration all but neglected cybersecurity, even though the digital threats were growing more numerous and more dangerous by the day. In 2014, a foreign government actually hacked into the White House network itself, and yet, in the face of constant attacks like that, the last administration too often chose silence and paralysis over strength and action.

But make no mistake about it: Those days are over. At President Trump's direction, our administration has taken decisive action to fortify America's cybersecurity capabilities. We're also forging new partnerships, evidenced by this conference today, all across our society and also with state and local governments and with great corporations so well represented here.

We've secured vital new funding for cybersecurity. In our first year in office, we allocated an additional $1.2 billion for digital defense, and next year, our administration has requested a record $15 billion to secure America's cyber frontiers. And we'll continue to work with Congress to provide the resources we need to defend our nation from the threats we face in the digital domain.

But this critical issue requires more than new funding. America also needs a central hub for cybersecurity. And today we call on the United States Senate to follow the lead of the House of Representatives and, before the end of this year, enact legislation to create a new agency under the authority of DHS. The time has come for the Cybersecurity and Infrastructure Security Agency to commence. Thank you. (Applause.)

This agency will bring together the resources of our national government to focus on cybersecurity. And it's an idea whose time has come.

In addition to funding and reforms, our administration is hardening federal networks as never before. We're taking renewed action to identify and eliminate weaknesses that our adversaries could exploit.

For example, the federal government has long allowed Kaspersky Lab, a Russian anti-virus software, to be installed on federal devices, even though it has a direct relationship with the Russian government

and intelligence services. This threat existed for many years, but our administration ended the threat last year when we banned Kaspersky Lab software from the entire federal government. (Applause.)

We've also dramatically increased information sharing with innovators, developers, and network defenders. America's intelligence and law enforcement agencies have an unparalleled ability to discover weaknesses in digital products and software.

But while the last administrations almost always held on to this ~~administration~~ [information], in this White House I'm proud to report that we've significantly improved how much we share with the private sector and the speed with which we share it. Today, nearly a third of the threat indicators we share with businesses aren't available from any other source, and will continue on that track.

And finally, our administration is putting the finishing touches on our National Cyber Strategy. This strategy will make clear that the United States will bring every element of our national power to bear to protect the integrity and security of the American digital domain. (Applause.)

Our actions have already made our adversaries' actions more costly. And as we continue to reinforce our cyber defenses, we will deter them as never before. But as you well know, we can't prevent every assault or attack in the digital sphere. The sheer size and magnitude of the danger, combined with the rapid evolution, means that some attempts will simply slip through the cracks.

Be assured, our government will continue to ensure the resilience of our digital infrastructure so that when these breaches may occur, we can get back on our feet fast, chart a path forward, learn from our vulnerability, and prevent the next attack.

But when it comes to stopping our cyber adversaries, resilience, though, isn't enough. We also must be prepared to respond. And in this White House, I'm proud to report, we are.

Our administration has taken action to elevate the United States Cyber Command to a "combatant command," putting it on the same level as the commands that oversee our military operations around the world. Gone are the days when America allows our adversaries to cyberattack us with impunity. Our goal remains: American security will be as dominant in the digital world as we are in the physical world. (Applause.)

But for all that we've done, and for all that we're doing, there's still much more work ahead. And what bring us all here today is the recognition that we cannot do it alone. Strengthening American cybersecurity does not belong solely to our national government in Washington, D.C. The greatest progress happens from the bottom up, not from the top down. And so beyond our government-wide approach, we need you. We need you to continue to partner with us for a nationwide approach, for together we can protect America's digital domain. (Applause.)

You know, it's been said "cybersecurity is a team sport." It requires seamless collaboration between the federal government, state and local leaders, but also innovators, entrepreneurs, academic experts. In a word, it requires all of you in this room and all of those that you represent all across the nation.

We've already taken important steps, I'm pleased to report, to improve our partnerships at every level. And, in addition to this conference today, where you've heard much about those efforts, I'm particularly excited with the new initiative that Secretary Nielsen announced this morning: the National Risk Management Center.

This new center will be the gateway for American companies who want to work with the federal government more closely to strengthen our shared cybersecurity. And let me take this moment to thank all of you who have already expressed your intention to join this critical initiative.

Just a few weeks ago, in the Situation Room, I personally met with the President's National Security

Telecommunications Advisory Committee, also known as NSTAC, which brings together key industry leaders to develop recommendations on cyber policy.

I learned then, and will learn more in just a few short weeks, that NSTAC will soon launch a cybersecurity "moonshot" initiative to focus our national energies and skills on digital dominance. Those leaders that day informed me that America won the race to the moon. And, under this administration, in partnership with all of you, America will lead the way to cybersecurity and strength. (Applause.)

Now, the examples that I mentioned today are all essential to the security and prosperity of the American people. But as we gather today, the American people also deserve to know that our democracy is secure as well. So before I close, let me speak to our administration's unprecedented action to safeguard the integrity of our elections.

While other nations certainly possess the capability, the fact is Russia meddled in our 2016 elections. That is the unambiguous judgment of our intelligence community, and, as the President said, we accept the intelligence community's conclusion.

Russia's goal was to sow discord and division and to weaken the American people's faith in our democracy. And while no actual votes were changed, any attempt to interfere in our elections is an affront to our democracy, and it will not be allowed. (Applause.)

The United States of America will not tolerate any foreign interference in our elections from any nation state — not from Russia, China, Iran, North Korea, or anyone else. As President Trump said, "We're not going to have it."

To that end, over the past year, President Trump has directed our administration to create, as well, a whole-of-government approach to strengthen election security. As recently as last week, the President convened a National Security Council meeting for updates on the progress that we've made.

As the President has said, we've taken a "firm stance," and we've backed it up with "strong action."

The FBI has formed the Foreign Influence Task Force to identify secret foreign attempts to infiltrate our society and undermine our democracy.

The Department of Homeland Security has launched the Election Information Sharing Analysis Center. This project, which all 50 states and more than 900 counties have already joined, will help prevent attacks before they happen, identify them when they're underway, and stop them before they can do any lasting damage.

Working with the Congress, we've also made $380 million available to states to help them ensure the security of their election systems, including upgrading voting machines and the most up-to-date and secure technology.

We're deploying new sensors to monitor election networks and identify potential intrusions at the state and local level. Thirty-seven states have opted into this program, but before this November, we intend to expand a further twenty-two states and counties, as they request.

Our administration has also launched a "National Cyber Situational Awareness Room" that offers states a virtual connection between DHS and election offices on Election Day itself. In my home state of Indiana, as well as Ohio, North Carolina, and West Virginia, this system was used in the May 8th primary, and we're working hard to expand this project for other states so that it's ready before the midterm elections in November.

We've also been working to help state and local governments rapidly respond to cyberattacks. Less than two weeks ago, Finney County, Kansas, reached out to DHS for help after a malware attack forced

them to shut down not just their election network, but the entire county's network. Federal officials worked earnestly, hand-in-hand, with county officials to identify and ultimately eliminate this dangerous intrusion. This action was a model of the collaboration that we need to ensure the security of our elections, and we commend the state, and local, and federal officials that made it happen. (Applause.)

Now, make no mistake about it: Our administration recognizes that elections are administered and conducted at the state and local level. This administration has already been a champion of federalism and respected the purview and the authority of our state and local officials. Yet it concerns us that many states still don't have concrete plans to upgrade their voting systems, and 14 states are struggling to replace outdated voting machines that lack paper trails before the next presidential election.

And so today, not just as Vice President, but as a former governor, I want to urge, with great respect, every state to take renewed action. Take advantage of the assistance offered by our administration. Do everything in your power to strengthen and protect your election systems. You owe your constituents that, and the American people expect nothing less. (Applause.)

This is a time for vigilance and resolve, and I can assure you our administration will continue to take strong action. We have already done more than any administration in American history to preserve the integrity of the ballot box, and we've just begun.

We will continue to work tirelessly to prevent foreign nations and malign actors from hacking into our election infrastructure with the potential of changing votes or election outcomes. As the President has said, we will "repel…any efforts to interfere in our elections."

When anyone violates our laws, we will bring them to justice and utilize every element of our national power to respond, because our democracy demands and deserves the most vigorous defense we can give it. (Applause.)

And I want to assure you, we will do this in a manner that respects the God-given liberties enshrined in our Constitution, including the freedom of speech and the freedom of the press.

We will never stifle voices in a free society, but we can expose malign and fraudulent voices when they seek to undermine confidence in our democracy, and this we will do. Our administration will always make efforts to shed light on foreign attempts to interfere or sow malign influence in our elections in our society.

Our 16th President, Abraham Lincoln, probably said it best when he said, "Give the people the facts, and the Republic will be saved." When the American people have the facts, they always uphold our most cherished institutions and values. And this is just as true today as it has ever been in our nation's long and storied history.

So thank you again for being here and being a part of this important and historic gathering. You do the nation a great credit by participating in today's discussion, and more important, by following through on the discussion with a greater partnership and collaboration in cybersecurity.

The truth is, cybersecurity is unlike any challenge we've ever faced. It is a work that's never done. It is a process that is continuous. And so must our collaboration be.

Technologies are shifting by the minute, from the Internet of Things to 5G to artificial intelligence to quantum computing, and each advance is accompanied not only by new opportunities, but new challenges. And just as the threats are evolving, our defenses, too, must evolve. The only way to be strong and secure is if we stand strong and secure together on behalf of the American people. (Applause.)

Cybersecurity, then, is a shared responsibility. And I believe that cybersecurity is a civic duty. You've already distinguished yourselves as leaders and patriots in this cause long before this conference today by your efforts on behalf of the American people. And the President and I need you to continue to be advocates in your industry and among your peers for greater cybersecurity collaboration. The American people deserve nothing less.

Keep talking with your peers about how they need to enlist in this fight. Tell them that they have an obligation to identify the weaknesses in their own networks and platforms, because the weakest link creates the greatest vulnerability.

Tell them we need them to buy American when it comes to digital products and services, not just to support American jobs and innovation, but to support American security. Tell them they need to share their insights, ideas, and innovations that will strengthen our collective security.

And above all else, tell them what you've heard here today at this conference. Tell them we need to work together on an increasing basis, not just with our national government, but with state and local governments, to ensure the continued security and prosperity of our nation.

The American people are counting on all of us. They deserve to know that their homes are free from prying eyes, their personal information is safe and secure, that their bank accounts can't be robbed, that the lights will turn on when they flip the switch in the morning, and the American people deserve to know that our democracy cannot be corrupted, and that our nation is stronger and more secure, even in the midst of a technological revolution than it's ever been before. This, we can do together.

So thank you for the opportunity to address you today, to wrap up what I trust has been a meaningful and productive dialogue. But I hope you will not feel that you've come here today and done your part by this attendance. I hope you leave here today with a burden on your heart to do more.

The truth is, as the Old Book says, we should "not grow weary in doing good, for in due season we will reap a harvest if we do not give up." So don't grow weary. Don't grow weary in standing up for the security of the American people in the cyber domain.

With the trust of the American people, with the patriotism and collaboration of all of you gathered here who work together with us on this vital issue, with the leadership of President Donald Trump, and, I know, with the support and the prayers of the American people, we will defend our nation. We will defend our nation on this cyber frontier. And I know, as Americans have always done, we will do it together.

Thank you very much. God bless you. And God bless the United States of America. (Applause.)

END
4:50 P.M. EDT