https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech

Secretary Kirstjen M. Nielsen's National Cybersecurity Summit Keynote Speech

Release Date:
July 31, 2018

Introduction

Thank you Chris for that kind introduction, and for giving us a beautiful roadmap for everything we look to accomplish today.

It is my great honor and pleasure to welcome you here today, it's so wonderful when an idea with such passion actually comes to fruition, so it's very much a pleasure of mine to see you all here today.

We have a lot of serious threats to discuss today. Americans are worried about what our digital enemies might do…whether it is taking down the power grid…holding healthcare systems hostage…or the nightmare scenario: blocking access to the web the day a new TV show drops on Netflix. I often hear about this from folks that that keeps them up at night.

But I'd like to thank Secretary Perry, Director Wray, and General Nakasone, who will join me on stage in just a little bit, for bringing their expertise and leadership to this discussion as well. What you will see before you today is a true effort from the United States government, to work with the private sector, and academia to combat these threats.

I'd also like to Director Alles of the United States Secret Service who is here bringing his level of expertise, of course Under Secretary Krebs, and those of you in the audience, and who are watching from home so-to-speak, to the men and women from DHS, for everything you do to protect our country, thank you. And whether you represent government, industry, or academia, we are glad to have you on our team, and I want to thank you for your continued collaboration and for the time you're giving us today, and your future efforts to work with us as we look at these threats.

This afternoon, we will also have the pleasure of hearing from Vice President Pence. He will lay out how this Administration is strengthening cybersecurity across the board—and why we will be *relentless* against our cyber adversaries.

This event is the first of its kind. Today we are coming together—government leaders, CEOs, academics, and cyber experts—to send a message to these online threat actors: *Game. Over*. Our team is formed, our team is ready and we are ready to combat you wherever you might manifest your threat.

We are not waiting for the next intrusion before we act. We are taking a clear-eyed look at the threat and taking action—and notably, as Under Secretary Krebs mentioned—*collective* action to combat them.

And, that's truly the only way we'll win this struggle.

Today is a watershed moment, a chance for us to cement partnerships in order to protect our networks and repel digital invaders together.

Roadmap

This morning I'm going to give you a stark overview of the threat landscape. I won't sugar-coat it.

But I will also tell you how DHS and this Administration are fighting back.

And I'd like announce bold new efforts—starting *today*—that will make the digital infrastructure of our country more resilient.

The Threat

So let me give you the bottom line up front: we are facing an urgent, evolving crisis in cyberspace. Our adversaries' capabilities online are outpacing our stove-piped defenses.

In fact, I believe that cyber threats collectively now exceed the danger of physical attacks against us. This is a major sea change for my Department and for our country's security.

Indeed, most Americans go about their daily lives without fear of personal injury or harm from our adversaries. But our *digital* lives are now in danger every single day.
And these virtual threats can have very real-world consequences. When the bad guys can remotely turn off the lights, steal money from your bank account, and shut down emergency services, the impacts go far beyond our smartphone screens.

But don't get me wrong. Terrorists and criminals still pose a serious threat to our lives, we take this mission at DHS very seriously, and they are plotting against Americans daily; however, the "attack surface" in cyberspace is now broader and under more frequent assault.

This has forced us to rethink homeland security.

DHS was founded fifteen years ago to prevent another 9/11, but today I believe the next major attack is more likely to reach us online than on an airplane.

DNI Intelligence Dan Coats recently said that "the warning lights are blinking red" in cyberspace. I agree. Intruders are in our systems, they are seeking to compromise more of them every day, and they represent a very active threat to our digital security as a nation.

Every*one* and every*thing* is a target: individuals …industries …infrastructure …institutions …and our international interests. And the scope of the problem keeps getting wider.
The cyber-threat landscape is different today because cyberspace is not only a target. Cyber can also be used as a weapon, an attack vector, or a means for which nefarious activity can be conducted.

Today, our innovations can be stolen and used to diminish our prosperity…our infrastructure can be hijacked and used to hold us hostage…and our institutions can be compromised and used to undermine our democratic process.

Our smartphones and computers can be turned into bad-guy force multipliers without us even realizing it. Your compromised computer can become part of the bot army. Or your CPU power can be commandeered to steal Bitcoin to finance a rogue regime.

I wish I could tell you that we've rounded a corner. But last year was the worst-ever in terms of cyberattack volume. The headlines seemed never-ending, and not to be the Debby Downer but I think continue to see them this year.

Nearly half of all Americans had sensitive personal information exposed online in 2017. But that wasn't the *total* for 2017. That resulted from a *single breach,* when cybercriminals hacked a major credit bureau.
We witnessed North Korea's WannaCry ransomware spread to more than 150 countries, which held healthcare systems hostage and brought factories to a halt.

And we saw Russia probing our energy grid, compromising thousands of routers around the world, and unleashing NotPetya malware, which wreaked havoc and ended up being one of the costliest cyber incidents in history.

These incidents, though, are only the beginning. Rogue regimes and hostile groups are probing critical systems worldwide every moment as we speak. And without aggressive action to secure our networks, it is only a matter of time before we get hit hard in the homeland.

It's not just risks to our prosperity, privacy, and infrastructure we have to worry about.

Our democracy itself is in the crosshairs. Let me take just a moment to touch on these because I think it's important to do so.

Two years ago, as we all know, a foreign power launched a brazen, multi-faceted influence campaign to undermine public faith in our democratic process and to distort our presidential election.

That campaign was multifaceted and involved cyber espionage, leaks of stolen data, cyber intrusions into voter registration systems, online propaganda, and more.

Let me be clear: Our intelligence community had it right. It was the Russians. We know that, they know that. It was directed from the highest levels. And we *cannot* and *will not* allow it to happen again.
Although NO actual votes were changed in 2016, let me be clear in this, ANY attempt to interfere in our elections is a direct attack on our democracy, it is unacceptable, and it will not be tolerated.

Mark my words: America will not tolerate this meddling.

Key Challenges

So it's clear that we are in a tough fight right now. The cybersecurity headwinds are against us. I could talk about this all day but let me give you a few examples.

First, increased connectivity has led to increased systemic risk.

There's no getting around it. The wider and deeper the web gets, the more vulnerable we become.

The "internet of things"—which is really now the "internet of *everything*"—has compounded the problem by giving cyber criminals a direct route onto our doorsteps and into our homes. Wherever and whenever you are connected to the internet, you are unlocking doors and windows you may not even be aware of to let the bad guys in.

What's more, our growing digital dependence means that vulnerabilities can have widespread, unpredictable, and cascading consequences when they are exploited.

Whether it's common tools such as GPS or payment systems, everything is closely intertwined.

An attack on a single tech company, for instance, can rapidly spiral into a crisis affecting the financial sector, the energy grid, water systems, or the healthcare industry.

Secondly, our cyber rivals are getting more sophisticated.

Several years ago, a cyber-intrusion by a foreign adversary might be similar to a sloppy home break-in. The window would be broken, furniture would be overturned, and missing jewelry would be a dead giveaway that someone had been in your house— that you had been hit.

But they are getting savvier. Now when you get home, the door is still locked, and your house appears exactly as you left it. But no, in reality, the intruder has been inside for hours, perhaps days and weeks, and will remain in hiding, waiting for the right moment to strike.

That's what we're up against.

So, to prevent cyber intrusions today, we don't just need an alarm system. Or a neighborhood watch. Or security cameras. Or armed guards constantly roaming the hallways. We need it *all.*
Third, similar to the pre-9/11 days, and this is where we'll focus today, we still have trouble "connecting the dots."

Between all of us—government, the private sector, and individuals—we *do* have the data to disrupt and prevent cyberattacks.
But we aren't sharing fast enough or collaborating deeply enough to make it happen.

This is partly because we are operating in a legal and operational paradigm designed for a different era—long before brand-name breaches could threaten to cripple entire industries.

We still have the walls up and we still have stovepipes, and we still have sidewalks.

How We Are Responding

So what are we doing about it?

First and foremost, let me say this: *we are replacing complacency with consequences*. To deter bad behavior, you have to punish it. And we cannot wait for "the big one" to do just that. Our adversaries have the capability to destroy. So we cannot afford to bide time as they prep the battlefield and identify our hidden digital evacuation routes or try to outmaneuver us. We must act now.

That starts with calling out the offenders. Whether it is the North Koreans or the Russians, we are identifying countries that have compromised our systems or have unleashed destructive malware.

And we are imposing costs—whole of government costs, diplomatically, financially, legally, and through other means.

The United States possesses a wide range of response options—some of them seen, and some unseen—and we will no longer hesitate to use them to hold foreign adversaries accountable and to deter cyber hostility.

Let me also again take this opportunity today to issue a warning, as I have in other speeches, to any foreign power that would consider meddling in our networks or in the affairs of our democracy: *The United States will no longer tolerate your interference. You will be exposed. And, you will pay a high price.*

Second, we are changing our posture and setting course to confront systemic risk head on.

Traditionally, DHS, and our sector specific agencies, has focused primarily on protecting individual "assets," companies, individual systems or "sectors." But now we are looking more across government, across sectors, across government-private, at those nationally critical "functions." What are they? These are the lifeblood of our economy, of our national security, and of our day-to-day lives.

We must identify single points of failure, concentrated dependencies and interdependencies that can create those ripple effects across sectors.

To do this, we are launching voluntary supply-chain risk management programs. Under Secretary Krebs will talk about that later. And we are partnering with companies to hunt down unseen security weaknesses and to limit our attack surface.

I urge you to join us and lend your expertise to these efforts.

Third, we are reorganizing ourselves for a new fight.

I am working with Congress to pass legislation to establish the Cybersecurity and Infrastructure Security Agency within DHS.

This would recast what is now NPPD, or the National Protection and Programs Directorate—our cybersecurity arm—into an ambitious operational agency capable of better confronting digital threats.

But we all know that waiting for Congress to act is like waiting for a new Game of Thrones book to come out. You really, really want it—but you don't hold your breath.

So in the meantime we are taking other steps—including one that I will announce today—to make sure we keep up and stay ahead of our online adversaries.

This also includes dramatically ramping up efforts to protect our election systems, including through a new Elections Task Force and deploying a *vast*array of services, programs, and partnerships nationwide to help our partners secure our election infrastructure.
Finally, we are embracing a "collective defense" posture.

As I've said many times before, in a hyper-connected world, and as Chris mentioned in his introduction, *your* risk is now *my* risk and *my* risk is *your* risk. Each of us is on the frontlines of the digital battlefield, so we must work together to protect ourselves.
Any of us could be the weak link that not only allows adversaries to infect our systems but allows them to use our systems to spread further into others.

The adversary's approach is like a flood. It will find every crack, crevice, and seam. Even if I place sandbags around my house to prepare for the flood, if my neighbors don't do it too, my house will be underwater.

Collective defense calls for *all of us* to use sandbags, if you will—to optimally configure our systems, to employ patch management, to share, receive, and act on threat indicators.
To that end, DHS is improving and expanding our information-sharing programs, including those focused on sharing threat indicators.

And we are developing novel ways for government and industry to collaborate to identify threats before they hit our networks and to respond more quickly and effectively to incidents, which we will discuss throughout the day.

Taking the Next Step & Call to Action

We've made a lot of progress. But it's simply not enough.

We must move beyond routine information sharing. And we must do better at teaming up with the private sector to combat our common enemies in cyberspace—to understand their goals, to understand their actions, to understand the operational effects and implications of their intrusions, manipulations, and disruptions.

As we all here know, the majority of U.S. infrastructure is owned and operated by the private sector—not the government.

So we must be working to enable those in this room—across industries—to better defend your systems and our critical functions.

For far, far too long we have lacked a single focal point to bring government agencies and industry together to assess the digital dangers we face—and to counter them…a place where analysts and network defenders can address these risks *together* through the full myriad of mission sets when we address cyber.
I am pleased to announce that we are going to change that.

This week the Department of Homeland Security is launching the National Risk Management Center—an initiative driven by industry needs and focused on fostering a cross-cutting approach to defend our nation's critical infrastructure.

It will employ a more strategic approach to risk management borne out of the re-emergence of nation-state threats, our hyperconnected environment, and our survival and its need to effectively and continually collaborate with the private sector.

So what does that actually mean in practice?

Housed at DHS, the Center will bring together government experts with willing industry partners so that they can influence how we support them. Our goal is to simplify the process—to provide a single point of access to the full range of government activities to defend against cyber threats.

I occasionally still hear of companies and locals that call 9-1-1 when they believe they've been under a cyberattack, the best thing to do would be to call this center. This will provide that focal point, we will work with our partners in government who will be on stage today, and others, to provide you what you need to help repel, to help mitigate, to root out the adversary from your systems.

We will be able to take a piece of intelligence, and with the help of the private sector, ask ourselves "so what," and determine what we're going to do about it—together.

These days, cyber threat data is like a puzzle piece, for those of you when you started to begin a puzzle with your children and they pick up a puzzle piece, the first question is, "what puzzle does that puzzle piece belong to?" Having the private sector with us will help us to determine what puzzle it belongs to, and then determine how it fits into the puzzle so we can see the trend, we can see the thread, and we can see the purpose, perhaps, of the attack, but certainly the implications and effects. So this is where the expertise of the private sector comes in, to help us contextualize the threat both in the planning phase as well as in the response and recovery. The private sector also knows its operational environment better than we will ever know in the government, so we will look to their expertise to help us understand how the pieces fit together.

So, we will welcome industry experts, side-by-side with ours, to break down the silos and engage daily to develop actionable solutions to defend our critical infrastructure.

We will begin with a tri-sector model focusing on financial services, telecommunications, and energy sectors.

We will push this effort forward in 90-day "sprints" starting immediately to identify key priorities and to conduct joint risk assessments. And we will have a major cross-sector exercise this fall.

We will look to you to influence how we can support you best…to help us tailor our assessments, plans, and playbooks that you can then action.

As I often say from a Department with myriad missions – let's do what we do best and partner with you to do the rest.

But time is not on our side. So we are moving quickly. I ask all of you to consider working with us to develop the Center and deepen engagement so that we can fortify our defenses.

I would also ask that everyone here—whether you are from a federal agency, a Fortune 500 company, a think tank, or a university—identify at least one new actionable, operational way you can contribute to our nation's collective cyber defense.

That's why we are here today. Think about it now. Think about it throughout the day. Commit to it this afternoon. And follow through on it when you leave.

We don't put together summits to keep admiring all the problems. We do it to solve them.

Our adversaries are crowdsourcing attacks, and today I am pleased to say we will crowdsource our response.

Closing

I am sure I speak for my colleagues when I say we do not take your presence here lightly. We appreciate your time, your efforts, your commitment, your leadership, and we thank you for being here. And we hope to enlist your continued efforts in this fight if you're not already in it with us.

Our digital enemies are taking advantage of all of us. They are exploiting our open society to steal, to manipulate, to intimidate, to coerce, to disrupt, and to undermine. They are using our interconnectedness to attack us—but let's use the fact that we are all connected *to our advantage.* As I noted at the beginning, we are in crisis mode—the "Cat 5" hurricane has been forecast. And now we must prepare.

That leaves us with a choice: admit defeat and assume that our devices and networks will always be compromised—OR respond decisively and dramatically in order to restore security and resiliency to the web. If we prepare individually, we will surely fail collectively.

You're here today because you believe in working together with clear-eyed urgency. And together, I have no doubt we will turn the tide. So thank your attendance today, thank you for your participation, we look forward to many conversations to come, and we look at the end of the day to announce some very tangible actions that we will agree to throughout the day. So thank you very much and again thank you for joining us at this summit.