The War in Cyberspace

Why We Are Losing—and How to Fight Back

RSA Conference 2017, Moscone Center, San Francisco

THE HONORABLE MICHAEL MCCAUL
Chairman, Homeland Security Committee
United States House of Representatives

PROGRAM TIME: 10:05 am – 10:30 am

ABSTRACT: Washington must accept a sobering reality: we are losing on the cyber battlefield and face a bleak threat landscape. From Russian and Chinese hacking to brand-name breaches, our cyber rivals are overtaking our defenses. We are in the fight of our digital lives. But the new Administration has an opportunity to turn the tide and must work with Congress, the private sector, and foreign allies to defend our networks and prevail against attackers.

Good morning. I'd like to thank RSA for welcoming me back.

My wife, Linda, is joining me here today. And because it's February 14th, I'd like to start off by saying, "Honey, Happy Valentine's Day." We have five teenagers at home, so she can tell you that we both have become experts in dealing with domestic terrorism and cybersecurity.

Before we begin, I want to say it's an honor for me to address some of the brightest tech leaders in the world.

You are the motive power of the modern economy. You are advancing human prosperity. And you are on the front lines of protecting our personal privacy and digital security.

This morning some of you are joining us from overseas. And for many others, you began your journey to America years ago.

I am proud that our nation is a beacon of hope to people in all corners of the globe who seek to create, collaborate, and innovate.

But in light of recent events in Washington, I know there is deep concern in this room about whether U.S. policies will continue to welcome international talent.

So let me say this—and we should never forget it: This is a country built by immigrants. This is a nation where the oppressed have long sought and received refuge. And our country is a magnet for creators and entrepreneurs who are willing to take risks and pursue their dreams.

The Unite States <u>must</u> maintain that tradition, not only for our country's credibility but for the survival of liberty itself.

That is why I will fight to ensure that America continues to extend an open hand to peaceful, freedom-loving people…regardless of where they were born…regardless of how they worship…and regardless of the color of their skin.

That is who we are. And that is how we will attract the world's best thinkers to build a stronger country and a more vibrant global economy.

* * *

<u>Today I want to talk to you about the war in cyberspace, why we are falling behind, and what we can do to strike back.</u>

I am going to be brutally honest. We are in the fight of our digital lives. *And we…are…NOT…winning.*

As the Homeland Security Chairman in the House of Representatives, I get briefed on these threats every week.

It's clear to me that our adversaries are turning digital breakthroughs into digital bombs.

And from Russian and Chinese hacking to brand-name breaches, our cyber rivals are overtaking our defenses.

Nation-states are using cyber tools to steal our country's secrets and to copy our intellectual property.

Faceless hackers are snatching our financial data and locking down access to our healthcare information.

And terrorists are abusing encryption and social media to crowd-source the murder of innocent people.

Web-based warfare is becoming incredibly personal. The combatants are everywhere, and the phones in your pockets are the battlespace.

I'd like to ask you to raise your hand if you have ever had an online account hacked. **[pause]** Okay, keep your hands up.

Now raise it if you have been told by a retailer or any online service that your information might have been compromised. **[pause]**

Finally, raise your hand if you are worried your accounts and devices could be compromised in the future. **[pause]**

That's a lot of people…and this is a room of top cybersecurity experts. If you are concerned about getting hacked, ordinary folks should be especially worried.

Former NSA Director Keith Alexander made a powerful point: the magnitude of cyber espionage and theft we are seeing today has led to the "greatest transfer of wealth in history."

This crisis extends from kitchen tables to corporate board rooms.

The voters and companies I meet with feel defenseless, and they are looking to you—the world's top cybersecurity experts—for help in protecting their information.

In Congress, I oversee many of our nation's cybersecurity efforts, and even I have been the victim of cyber theft.

Chinese hackers stole 20 million security clearances—including my own—in a 2015 attack on the U.S. government's Office of Personnel Management.

Would-be intruders are also constantly targeting me with spear-phishing emails.

And the enemy is adapting. Now they send clever, socially-engineered messages that look like they're from the people we know and the companies we trust.

Yet it's about more than just the security of our inboxes. Our democracy itself is at risk.

Last year, the Russian government tried to undermine our elections.

They broke into political institutions, invaded the privacy of private citizens, spread false propaganda, and created discord in the lead up to a historic vote.

I was briefed on the situation starting in the spring, and frankly, it didn't matter to me whether it was Democrats or Republicans being targeted.

These were *Americans* in the crosshairs of the Kremlin, and to me, that was unacceptable. There needs to be consequences for such actions.

I pushed both the Obama Administration and then-Candidate Donald Trump to take public and forceful stands on the issue. But I was disappointed in the response.

This crisis was the biggest wake-up call yet that our cyber prophecies are coming true, and such attacks have the potential to jeopardize the very fabric of our republic.

But why are we not winning? How can cyber criminals conduct virtual robberies right under our noses?

Let me suggest five reasons.

First, there's the issue of volume.

I've said before that the digital frontier is a lot like the Wild West: there are more cyber outlaws than cyber sheriffs to round them up.

A lot of hackers out there should be behind bars, but law enforcement agencies at all levels are struggling to keep up with the volume and complexity of network intrusions.

Also, our laws have not kept up with this new age.

Second, the high speed of high tech gives cybercriminals an advantage.

History shows us that offensive weapons always outpace defenses.

We faced this challenge with every man-made weapon since the Stone Age. The spear led to the shield, the bullet to the bulletproof vest, and so on.

Yet we have never seen a weapon used against us so regularly, so aggressively, and so adaptably while we are trying to defend against it. And it's expensive to keep up.

Today, in some cases, the U.S. government is fighting 21st century threats with 20th century technology and a 19th century bureaucracy.

And we've made it far too easy for hackers by leaving the windows to our networks unlocked and the house keys under the doormat.

Third, we've got serious information-sharing challenges.

I compare this to the period before 9/11.

We had all the information we needed to keep terrorists from infiltrating our country, hijacking airplanes, and conducting the deadliest terrorist attack on American soil.

But we didn't connect the dots. We had the walls up, and we didn't share the information.

We are in the same place with cyber.

Between your companies, government agencies, and U.S. allies, we have the threat data to stop many intrusions.

Yet the sharing is still too weak, often because companies are afraid they might damage their reputations, expose intellectual property, or violate privacy.

As a result, the vast majority of cyber attacks go unreported, leaving others vulnerable to the same intrusions.

Fourth, deterrence is difficult.

I know as a father of five teenagers that if there are no consequences for bad behavior, then bad behavior will continue.

I also knew this from my days as a federal prosecutor. If you let the bad guys get away for too long, they'll convince more bad guys to join them.

In the cyber realm, we've got to show there will be consequences—and that intruders will be brought to justice.

Unfortunately, we still do not have clear "proportional response" policies for striking back against nation states, cyber criminals, and others who invade our systems.

And we certainly don't have the manpower, appropriate legal structures, and global cooperation to take down suspects as fast as we need to.

Fifth, we face a real paradox between national security and digital security.

Nowhere is this more obvious than with the terror threat.

We are seeing the highest spike in homegrown terror plots in the United States since 9/11, and Europe is in a worse position.

Gone are the days of Osama bin Laden, when extremists plotted using caves and couriers.

Now we have a new generation of terrorists who are recruiting over the internet, and using "virtual safe havens" to escape detection.

The brutal attacks in Paris and Brussels are tragic examples of how terrorists stayed under-the-radar by using tech savvy and end-to-end encryption to cover their tracks.

Unfortunately, we can't stop what we can't see.

At the same time, we must resist the temptation to go after encryption. Creating a backdoor into secure platforms is a fool's errand.

Encrypted technologies are everywhere, and weakening them would put our personal data at risk and leave our companies vulnerable to intrusion.

This is common sense to many of you. But it's not conventional wisdom in Washington, DC. When politicians on Capitol Hill see a problem, we come up with 535 bad solutions.

But I have worked hard to make sure we approach this challenge more thoughtfully so we can keep our country safe while also keeping our data safe. But we're still not there yet.

<u>So what does it take to prevail against our cyber adversaries?</u>

It starts with the right mindset.

In 1940, British Prime Minister Winston Churchill responded to the Nazi invasion of Europe with a rousing speech in the House of Commons.

He vowed that the British would "fight on the seas and oceans…fight on the beaches…fight on the landing grounds…fight in the fields and in the streets…fight in the hills…[and] never surrender."

Now, I don't think we need a bunker mentality just yet. But we need to acknowledge that we are under siege on the cyber battlefield and respond with a sense of urgency and resolve.

First, we must redouble our efforts to defend private sector networks and the public.

When I say "we," I'm not talking about just the government.

President Reagan used to say that the most terrifying words in the English language were: "I'm from the government. And I'm here to help."

Today it might be: "I'm from the government. And I can help secure your iPhone."

Bigger federal agencies are not necessarily the answer when it comes to cybersecurity. The answer is right here in this room. It's the bleeding-edge work being done in the private sector.

We need your innovation—and your initiative—to stay a step ahead of cyber criminals.

However, government plays a critical coordinating role.

In the wake of the Snowden leaks, it is more important than ever that we reassure the public that federal cybersecurity here at home is led by a civilian department. Not by the military. And not by intelligence agencies.

Just as we do not allow soldiers to police our city streets, we should not have organizations like the military patrolling our networks.

Cyber is a team sport. Everyone on the field can't chase the ball at the same time. If we do, we will lose. Instead, we need strong offense AND strong defense.

So I am pushing to make the lanes of responsibility more clear. And I have proposed the creation of a single, stronger cybersecurity agency at the Department of Homeland Security, building on important laws we have passed in recent years.

This is a key step in standing up to cyber attackers.

Our next priority should be fixing the information sharing weaknesses I outlined earlier.

Your chances of winning on any battlefield are lower if you don't know where the enemy is coming from and what weapons they're using.

In 2015, Congress passed The Cybersecurity Act, a landmark bill I drafted to increase information sharing about cyber threats.

The law's liability protections and privacy safeguards make it easier for companies to swap threat data and to share it with federal agencies to stop attacks.

But more companies need to step up to the plate and start sharing with each other.

Next, we need a talented cyber workforce on the frontlines.

I'll stop short of calling for a "digital draft," but we need far more young people to enlist in the struggle.

We are losing top cyber talent because morale is bad on the inside and the money is better on the outside.

I'm trying hard to change that. I worked with my colleagues in Congress to pass legislation to expedite hiring authority at DHS for new recruits, but the Department needs to act more quickly to use this authority.

We also passed bipartisan legislation creating a "scholarships for service" program to help students pay for college if they commit to working on cybersecurity at the Federal, State, or local level.

Thousands of students have now gone through the program, allowing us not only to *recruit* top people but to *retain* them.

Many of your organizations face the same challenges. And you want the flexibility to bring in specialists from around the world.

I believe America's doors must stay open to high-skilled workers who will contribute to our society and join us in building an innovation economy.

That's why I'm supporting efforts in Congress to streamline our H-1B visa process to make sure tech companies can get the right people, from the right places, at the right time.

Great ideas can come from anywhere in the world, and our nation is better off if we welcome the people who have them—young or old, rich or poor.

Then there is the "going dark" challenge. Here, there are no easy answers.

As I noted, we cannot undermine encryption, which is the bedrock of internet security.

But at the same time, we cannot stand on the sidelines and allow groups like ISIS to remote-control terrorist attacks using the darkness of the web.

So this year I will again partner with Senator Mark Warner to call for a commission of the nation's top experts—from academia, privacy, tech, law enforcement, and beyond—to find real solutions that balance digital security with national security.

I hope many of you will support this Digital Security Commission because the eyes of the world are upon us, and America should lead the way.

Second, to prevail against online adversaries we must defend our government institutions, our critical infrastructure, and our democracy—and we must respond to attacks decisively.

As far as federal networks are concerned, DHS is responsible for securing the so-called "dot gov" domain and for incident response.

At the end of last year, the Department announced that "Einstein 3A"—its advanced intrusion detection system—was providing coverage to a total of 93 percent of U.S. civilian agencies.

However, we will never be able to build virtual walls high enough to completely stop hackers from getting inside.

So once again, my message is that we need YOU to help us.

In Congress, I will be working on bills to break down bureaucratic barriers so that we can work more closely with companies to help us anticipate the next moves of the hackers.

We also know that our adversaries are targeting our critical infrastructure, 85 percent of which is in the hands of the private sector.

They are deploying cyber implants that could be used to hold us hostage or attack us.

A major cyber attack on gas pipelines or the power grid, for instance, could damage the economy and weaken our ability to defend the United States.

Admiral Mike Rogers, the head of the NSA, has warned Congress that the bad guys are leaving "cyber fingerprints" on critical infrastructure. They are sending a message: "Watch what you say and do, America, because we can hit you from within."

It is only a matter of time before such an attack happens, which is why critical infrastructure should be built with cybersecurity in mind.

Unfortunately, too often companies are focused on putting chain-link fences around their headquarters rather than putting digital fences around their networks.

I plan to work with the new Administration to address critical infrastructure vulnerabilities more seriously, and I applaud them for undertaking a major review of the threats.

More broadly, I have been urging the Administration to develop a new national cybersecurity strategy as soon as possible.

We are feeling tectonic shifts on the virtual ground beneath us. And our current cyber plans won't cut it.

The U.S. government needs better response options, and it needs to be conducting regular "cyber exercises" to make sure we're prepared—including with foreign partners.

Additionally, our ability to win the war in cyberspace depends on our ability to deliver consequences…by striking back when appropriate.

This requires strong leadership from the top, a willingness to track down rogue hackers, and a determination to hold hostile countries accountable for bad behavior.

We cannot allow foreign adversaries to use cyber intrusions to meddle in our domestic affairs, especially our democratic process. That's a redline we should not allow anyone to cross.

And our strategy should go beyond just "returning fire" online. It should include the threat of sanctions and other real-world penalties.

Russia is the perfect example. We must continue to call out Moscow for election interference. And if we don't hold the line on sanctions and deliver meaningful consequences, they will do it again. And they will do it to our allies.

We've got to say *enough is enough*.

Finally, America should be working with close allies to win the war in cyberspace.

Our nations have different laws and privacy expectations. But we've got to figure out how to respect those differences while working together quickly—because attackers won't give us the benefit of time.

We must develop clear "rules of the road," especially when it comes to cyber warfare.

In times of crisis, uncertainty and lack of coordination can cause situations to spiral out of control.

So we should confer with our partners on major incidents, work together to build mutual defenses, and put the structures in place for joint action.

Lastly, we should make sure we are prepared for the future.

For instance, quantum computing is an area where we need to be planning urgently.

Trust me, the "digital atomic bomb" is on the not-too-distant horizon. And the first hostile country to gain such a capability will pose a serious threat to the rest of the world.

The United States should lead a coalition of like-minded nations to prepare for the quantum future and ensure we have the right cyber defenses in place when it comes.

* * *

Looking back, 2016 was a watershed year in cyberspace.

There were a lot of "firsts"—and many of them were not the kind we celebrate.

But I think it made us all more realistic about the danger we face and more clear-eyed about what we need to do.

While the cyber landscape is bleak, we cannot let the threat of the “unknown” and “unseen” outweigh what we already do know and already can see*:* ***that we have the world’s greatest minds working to defend our networks.***

To those of you who make cybersecurity your day job—thank you for what you’ve done, for what you are doing, and for what you *will do* to defend us into the future.

I appreciate you having me here today.