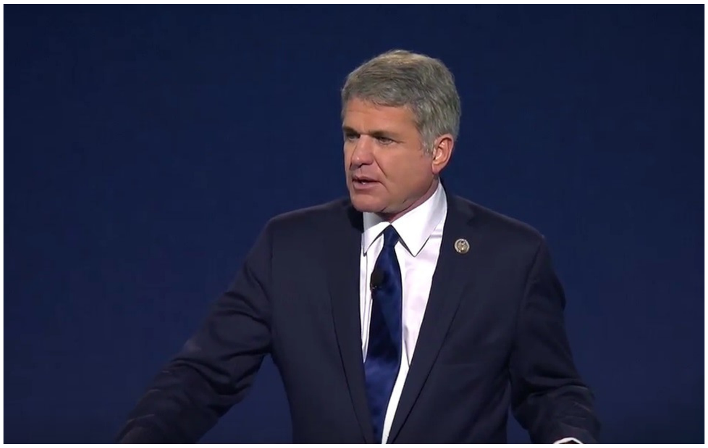
AmericanRhetoric.com

Michael McCaul

RSA Conference Keynote Address

delivered 14 February 2017, Moscone Center, San Francisco, California



AUTHENTICITY CERTIFIED: Text version below transcribed directly from audio

Good morning. I'd like to thank RSA for bringing me back here today. I also want to acknowledge my wife Linda this Valentines Day. Happy Valentines Day, honey. We have five teenagers at home, so when it comes to homeland security, issues I have a lot of personal experience on the home front, we call it domestic terrorism at my house.

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 mode of power of the modern economy. You are advancing human prosperity. And you're 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'm proud that our nation is a beacon of hope to people in all corners of the globe who seek to create, collaborate, and innovate. (Thank you.)

But in light of recent events in Washington I know there's deep concern in this room about whether U.S. policies will continue to welcome that international talent. So let me say this -- and we should never forget: This is a country built by immigrants. This is a nation where the oppressed have long sought refuge. And our country is a magnet for creators and entrepreneurs who are willing to take risks and pursue their dreams. The United States must 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 -- because 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.

Today I want to you about the war in cyberspace, why I believe we are falling behind, and what we can do to strike back. I'm going to be brutally honest: We are in the fight of our digital lives, and we are not winning.

As a chairman of the Homeland Security Committee in the House, 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 [inaudible at: 3:08] headaches, 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 cyber data and locking down access to our healthcare information. And terrorists are abusing encryption and social media to crowdsource 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 first for you to raise your hand if you've ever had an online account hacked. Now raise it if you've been told by a retailer or any online service that your information may have been compromised. And I'm going to raise mine as well. (Or compromised by a teenager.) Finally, raise your hand if you're worried that your accounts and devices could be compromised in the future. I would think that's everybody in this room.

And you're a room of top cybersecurity experts. If you're concerned about getting hacked, then ordinary people should be especially worried.

Former NSA Director Keith Alexander made a powerful point: The magnitude of cyber espionage and theft we're seeing today has led to "the greatest transfer of wealth" in human history.[1] The crisis extends from kitchen tables to corporate boardrooms.

In Congress, I oversaw many of our nation's cybersecurity efforts. And I've 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.

But the threat is worse than just espionage. Our democracy itself is at risk. Last year, there is no doubt in my mind that the Russian government tried to undermine and influence our elections. They broke into political institutions, invaded the privacy of private citizens, spread false propaganda, and created discord in the lead up to an historic vote. I was briefed on the situation starting in the springtime, and frankly, it didn't matter to me whether it was Democrats or Republicans being targeted. These were Americans first, in the crosshairs of the Kremlin. And to me, that was unacceptable.

I pushed both the Obama Administration and then candidate Trump to take public and forceful stands on the issue. But I was disappointed in their response. The crisis was the biggest wakeup call yet that cyber intrusions have the potential to jeopardize the very fabric of our Republic.

So why aren't we 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 digital age.

Second, the high speed of high tech gives cybercriminals an advantage. History shows us that offensive weapons always outpace our 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've never seen a weapon used against us so regularly, so aggressively, and a weapon that can adapt while we are trying to defend against it.

And it’s expensive to keep up with it. Today, in some cases, the United States Government is fighting 21st century threats with 20th century technology and a 19th century bureaucracy.

Third, we have serious information-sharing challenges. I compare this to the period before 9/11. We all had the information we needed to keep terrorists from attacking on the fateful day. But we did not connect the dots. The walls were 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 of these intrusions. Yet the sharing is still far too weak. 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 former federal prosecutor and as a father of five teenagers that if there are no consequences for bad behavior, that bad behavior will continue. In the cyber realm, we have to show that there will be consequences, and that intruders will be brought to justice. Unfortunately, we still do not have clear proportionate 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. 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 and force their propaganda on a global Internet scale. And partly as a result, we are seeing an unprecedented spike in terror plotting against the West. We had the brutal attacks in Paris and Brussels as tragic examples and reminders of how terrorists stay under-the-radar by using end-to-end encryption on their phones to cover their tracks.

At the same time, we must resist the temptation to go after encryption with simple knee-jerk responses. I believe that creating backdoors into secure platforms would be a huge mistake. It would put our personal data at risk and leave our companies vulnerable to intrusion. Instead, we need to find a way to keep our country safe, while also keeping our data safe and secure. But we're still not there yet.

So what does it take to prevail against our cyber -- cyber adversaries? 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, you know, on this. But we need to acknowledge that we are under siege in the cyber space, the cyber battlefield, and respond with 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.

In fact, President Reagan once said the most terrifying words in the English language were: "I'm from the government and I'm here to help" you. It still holds true today. Today it might be: "I'm from the government and I can help you secure your iPhone." But federal agencies are not necessarily the answer when it comes to cybersecurity. I believe that the answer is right here in this room. It's the bleeding-edge work being done in the private sector. And we need your innovation -- we need your initiative, to stay a step ahead of cyber criminals.

Government does play a role, a critical role in coordination. In the wake of [the] Snowden leaks, it is important, now more than ever, that we reassure the public that federal cybersecurity here at home is being led by a civilian department -- a civilian department, not by the military and not by intelligence agencies. Just as we do not allow soldiers to protect our city streets -- we allow the police -- we should not have organizations like the military patrolling our networks.

Cyber is a team sport. We need strong offense and strong defense. So I'm pushing to make the lanes of responsibility more clear. I propose the creation of a stronger, consolidated cybersecurity agency at the Department of Homeland Security, building on important laws we have passed in recent years. This is an important step in standing up to cyber attackers.

Our next priority should be fixing the information sharing weaknesses I outlined earlier. In 2015, Congress passed my bill, The Cybersecurity Act, a landmark bill to increase information sharing about cyber threats.

The law's liability protections and privacy safeguards make it easier for companies to stop attacks, and if they chose, to share it with the federal government. But more companies need to step up to the plate and start sharing with each -- each other. Once again, that is a goal -- we are counting on you to help us achieve.

Next, we need a talented cyber workforce on the frontlines. We are losing top cyber talent because morale is bad on the inside as -- and money is better on the outside. I'm trying to change that. I've 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 need bipartisan legislation -- and we passed it -- 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 this program, allowing us not only to recruit them -- and recruit top people -- but also 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. And that is why I'm supporting efforts in the 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.

And then there is a "going dark" challenge. There's no easy answer to this one. As I said before, we cannot undermine encryption -- and we heard from talented encryption experts in the previous panel. It's bedrock of internet security. But at the same time, we cannot -- can't allow groups like ISIS to remote-control terrorist attacks using the darkness of the web. So this year I -- I will work again with Senator Mark Warner to call for a commission of the nation's top experts -- from academia, privacy, tech, and law enforcement, and beyond -- to find real solutions that balance digital security with national security. And I hope many of you will support this Digital Security Commission. The eyes of the world are upon us, and I believe America should lead the way on this very important issue.

Second, to prevail against online adversaries we must defend our government institutions, our critical infrastructures, 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.

At the end of last year, the Department announced the “Einstein 3A” to advance intrusion detection. It 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 the digital space.

So, once again: We need industry to help us.

In Congress, I'll be working on bills to break down bureaucratic barriers so that we can collaborate more closely with your companies to secure federal networks. We also know that our adversaries are targeting our infrastructure, 85 percent of which is in the hands of the private sector. They are deploying cyber implants that could be used to threaten 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. I just met with Admiral Mike Rogers for breakfast, the head of the NSA. And he warned Congress that the -- that the bad guys are leaving “cyber fingerprints” on our critical infrastructure. They are sending a message: “Watch what you say and do, America, because we can hit you from within.”

It's 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 up chain-link fences around their headquarters rather than putting digital fences around their networks. I plan to work with the new Administration to address the critical infrastructure vulnerabilities more seriously, and I applaud them for undertaking a major review of these threats.

More broadly, I've 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 just won’t cut it. The United States Government needs better response options. 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 will require 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, anymore, foreign adversaries to use cyber intrusions to meddle into our domestic affairs, and especially into our democratic process. This is 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, I am certain that they will do it again. We've got to say enough is enough.

Finally, America should be engaging with our overseas partners to win the war in cyberspace -- our NATO allies. 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 the 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 infrastructures in place for joint action.

Lastly, we should make sure we are prepared for what lies ahead. For instance, we need to be ready for the era of quantum computing. The "digital atomic bomb" is on the not-too-distant horizon. And the first hostile country to gain such 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 on 2016, it was a watershed year in cyberspace -- and for a lot of the wrong reasons. But I think it made us all more realistic about the danger we face and more clear-eyed about what needs to be done. And 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. And to those of you who make cybersecurity your day job, I want to thank you for what you've done, for what you are doing, and what you will do to defend us into the future.

Thank you so much for having me.