**James B. Comey**

Director
Federal Bureau of Investigation

Share on Twitter Twitter Share on Facebook Facebook Email Email

International Conference on Cyber Security, Fordham University
New York City, New York

*January 7, 2015*

# Addressing the Cyber Security Threat

*Remarks as delivered.*

Thank you so much, Father, for that kind introduction. Thanks to you and to Fordham for making this possible. This has become one of the most important gatherings of people who care about cyber security from the government perspective, private perspective, and academia that there is and that's thanks to your good work.

I want to start though by saying—I'm glad you mentioned it—my heart is still heavy from Detective Liu's funeral on Sunday and I wanted—I couldn't be here in this great city without noting that.

Echoing in my head are words from Bill Bratton at Detective Ramos' funeral where he urged that we all find ways to see each other better. That law enforcement work to see the communities that we protect better and that the communities work to see law enforcement better. And those are very, very wise words. And especially given the events of the last day or so where two more officers were wounded, I hope that part of that seeing involves an appreciation for just what policing involves. How hard it is. How dangerous it is. But I think there's an important conversation going on in this country right now about race and policing and I hope to have more to say about that in the next couple of weeks.

But I'm here today to talk about cyber. Before I get to that, let me also say that my heart goes out to the people of France and Paris this morning. We're thinking of them. We have, the FBI, a very close relationship with our partners in the French law enforcement and counterterrorism communities. We are working with them. We will do everything we can to help them bring to justice the perpetrators of the atrocity that happened in Paris earlier today. So we're thinking of our friends and partners in Paris this morning.

Let me turn now to the reason that I'm here, which is to talk to you about how we at the FBI are thinking about cyber security and the cyber threat. I want to talk a little bit about some of the recent cases. In particular, I want to give you some new information about the investigation that we're doing into the Sony hack perpetrated by the North Koreans.

Let me start by telling you what you know, which is that everything has changed in ways that are so fundamental that it's difficult to describe what it means when we say the world is changing because of cyber. Now, I find that in all things cyber there's a lot of nodding and I worry there's not a lot of understanding behind the nodding at times. And so I always look for ways to describe just how fundamental the transformation we're standing in the middle of is.

And Cisco provided some stats that I saw recently that I just wanted to mention as I start. In 2003 there were 6.3 billion human beings on the earth and 500 million devices connected to the Internet. In 2010 there were 6.8 billion people on the earth and 12.5 billion devices connected to the Internet. One-point-eight-four per person.

Cisco projects that in 2020, now just five years away, there will be seven billion people on the earth and 50 billion devices connected to the Internet. Six-and-a-half devices on average per person. As a father of five young adults and teenagers, I think we are—in my household we've exceeded the 6.5 number. We're carrying the load for a lot of you who are not keeping up.

But there is no doubt that everything has changed because we've connected our entire lives to the Internet. That is why, because all of life is there, that all of the parts of life that the FBI is responsible for trying to protect—whether it criminal, counterintelligence,

counterterrorism, protecting children, fighting fraud—it all happens there because that's where life is.

What I want to tell you this morning, now afternoon, is how we're thinking about the threat, what our strategy is for the threat, addressing the threat, and why our partners in the private sector matter so much to us being successful in fighting the threats we're responsible for.

Let me start with the threat. I actually try to describe to people in very simple ways what we're talking about today because I don't see cyber as a thing, I see it as a way. As a vector. Because my children play on the Internet. Because that's where I bank. Because that's where my health care is. Because that's—I don't have a social life, but if I had one, that's where I'm sure it would be. That's where our nation's critical infrastructure is, that's where our government's secrets are and that's—because life is there, that's where bad people come who want to hurt children, who want to steal money, who want to take identities, who want to steal secrets, who want to damage dams and critical infrastructure in the United States. It's the way they come at us because that's where life is.

I harken back to what I believe was the great vector change that gave birth to the FBI. And this popped in my head when I was visiting the field office that we have in Indianapolis. A local sheriff gave me a round that had been fired from John Dillinger's Thompson submachine gun. It occurred to me that the great vector change of the 1920's into the 1930's was the confluence of the automobile and asphalt. It gave birth to an entirely new way of doing bad things.

Suddenly criminals could move at breathtaking speeds, right? Forty miles an hour. Fifty downhill. Right? They could go from Ohio to Indiana to Illinois in the same day and do bank robberies in each of those locations. They were blowing away traditional notions of county line and state line. Right? It was straining the framework that law enforcement used and so a national force was needed and there was—I'm the seventh director—there was the first director of the FBI, J. Edgar Hoover. And a national force was born to respond to that entirely new way of crimes being committed. A new vector that required a new approach.

This is that times a million. Dillinger or Bonnie and Clyde could not do a thousand robberies in all 50 states in the same day from their pajamas from Belarus. That's the challenge we face today. The traditional notions of space and time and venue and border and my jurisdiction and your jurisdiction are blown away by a threat that moves not at 40 miles an hour or 50 downhill, but at 186,000 miles per second. The speed of light.

Traditional notions, frameworks, are destroyed by that kind of threat. That requires every part of the FBI, those who are spending their days protecting kids, fighting fraud, fighting spies, fighting terrorism, protecting intellectual property, all of those things; it requires those people to be digitally literate. It requires me to have the right kind of people, the right kind of equipment and deploy them in a way that deals with a vector change that is mind boggling compared to the Dillinger era.

So what to do? Let me turn to our strategy. The first thing to do though is adopt an attitude of humility. I think we stand in the single greatest transformation in human history and anybody who stands here and says, "I know what five years from now looks like, I know what 10 years from now looks like, and therefore the FBI should be deployed and equipped in the following way," is arrogant and, in my view, foolish.

I have to approach this with a sense that we have never seen this before. So I have to be humble enough to say, I'll take things that seem reasonable, I'll get feedback, and I'll iterate. So we approach it, I hope, with humility.

And then we devise a five-point strategy. We're going to try to focus ourselves, we're going to try to shrink the world, we're going to try to impose real costs on bad actors, we're going to try to improve our relationships with state local law enforcement and most importantly of all, we're going to try to improve our relationship, our battle rhythm, our working relationship with private sector partners.

Let me say a word about what I mean by each of those.

Focus. Because this affects everything that we might be inclined to deal with, we can't do it all. And so what we're trying to do in the FBI is figure out so where should our

resources be deployed. And we think it makes sense to go against the biggest. The worst. The baddest. And think about what to go after given what's unique about the FBI. We have international reach and we have significant resources. So given that, what should we focus on? And there's a lot to choose from as you know.

I have been teased repeatedly, but I'm not giving up describing the threat we face as an evil layer cake with nation states at the top…terrorists, organized criminal actors, sophisticated worldwide botherders and botnets, hacktivists, weirdoes, bullies, pedophiles, creeps…all kinds of people at the lower levels of the layer cake.

We're going to try to focus on the top layers of that cake and focus ourselves on the nation state actors and the biggest, the most extensive, the most dangerous criminal syndicates and international operations. Where can we make the biggest impact for the investment of resources?

We're also, as we focus those resources, going to try to deploy them in a different way. As I said, this vector change blows away traditional notions of, well, this is my area of responsibility, this is your area of responsibility. This is my judicial district, that's your judicial district. Blown away by a threat that's moving as a photon.

And so we're going to assign this work not based on some notion of physical fixed jurisdiction or venue. We're going to assign it where the talent is. So what we're doing is looking across the FBI and saying, "Where is the talent to deal with this particular threat?" And we will assign that threat to that field office. It could be at one corner of the country or the other corner of the country. It's where the talent is. And then we'll allow up to four other offices to support that effort, to help the primary assigned office. We call this the cyber threat team model. Seems to make good sense to me. I don't know. We've never done it before. We're trying it and we're getting feedback from people to see whether it works and whether we need to iterate and change in some fashion.

Second, shrink the world. What do I mean by that? The bad guys have shrunk the world on us. They're sitting in their pajamas half way around the world. They're in a military uniform half way around the world moving at the speed of light. Blowing away the traditional notions. Shrinking the globe to the point of the pin. We have to do the same.

So we're trying to do a couple different things to respond to that. We're going to forward-deploy more and more cyber special agents of the FBI and intelligence analysts of the FBI in our foreign partners' offices around the world to make sure that our battle rhythm tries to keep up with the threat that's moving that fast. To forward deploy so we have no gap between when the threat is seen and when someone acts on it.

And the second thing we're going to do is, within the government, try to continue to improve at getting our act together at dividing up our resources between organizations in the government.

As I've said before, when I left government in 2005, I described our response to the cyber threat as a bit like 4-year-old soccer. I have five children as I think I said, and I watched a lot of 4-year-old soccer and it is clumps of children chasing the ball. Because the ball is the cool thing so you want to be near the ball at all times so in big clumps they chase the ball. Cyber was very cool. All of us in government knew we had to do something about cyber, so there was a big clump of us running around chasing it.

Now that I've come back—I've been back a year and four months now. I saw when I came back we've made significant progress. We're probably high school, college-level soccer. We spread out. We know we have to pass. We know it's important to know where you are on the field. Everybody shouldn't be following the ball. But we're facing a World Cup-level adversary. We have to get better at feeding each other the ball when we need it and doing it at machine speed.

We have built as a government something called the National Cyber Joint Investigative Task Force, NCIJTF, where 19 federal agencies sit together and divide up the work. See the threat, see the challenge, divide it up and share information. That's great. That's one significant down payment on moving toward World Cup-level soccer, but we have more to do.

I said we need to impose costs. What do I mean by that? I worry sometimes that whether the actor is a nation state or a criminal or a creep down the block, there's a sense that it's a freebie. That if I'm at a keyboard somehow it's free that I can break in and steal the lifeblood of an American business or steal the identity of an American

citizen when it is in reality no different than kicking in your front door and walking out with your television, right? Or dragging something you love dearly out of your life.

We have to treat it that way. We have to impose real costs on people who think they're alone…think they're far enough away that it's a freebie. And the first way we need to do that is, as often as possible, lay hands on people and lock them up. Often when I say that people say, "Well, these people are far away and they're in foreign countries." I'm not saying it's easy, but we are dogged people. Never say never.

As the world shrinks and people travel, we have more and more opportunities to lay hands on people who think they perpetrated a freebie in an effort to make it a real cost. So we're going to try to lay hands on people or get our partners to lay hands on people as often as possible.

The other thing we're going to do is when we can't lay hands on people, as often as possible, we're going to call out the conduct. And as often as we possibly can we're going to say here's what happened and who did it. It's why I thought it was so important that the indictment was returned out of the Western District of Pennsylvania indicting the five People's Liberation Army actors for a naked theft of the lifeblood of American companies. I thought it was very, very important to have that be a public indictment and explain the conduct.

For the same reason, I thought it was very, very important that we as a government, we as an FBI, said we know who hacked Sony. It was the North Koreans who hacked Sony. And call out that conduct and explain it. That is why we have, as much as we can, tried to offer our attribution and the whys behind our attribution.

The destructive nature of that attack proves that everyone has to take cyber security seriously. It could happen to anybody in this room. The Treasury Department's recent sanctions against North Korea, I think, are an important signal of how seriously the government takes these events. Alright? That there will be consequences for those who use malicious cyber activity to harm Americans or harm American businesses.

As you know, we at the FBI and the entire intelligence community have previously attributed these attacks to North Korea and we continue to believe that is the case. There is not much in this life that I have high confidence about. I have very high confidence about this attribution, as does the entire intelligence community.

So how do we know that? Why do I have such high confidence in this attribution to North Korea? Well, here's the tricky part. I want to show you as much as I can, the American people, about the why and I want to show the bad guys as little as possible about the how. Okay? How we see and what we see. Because it will happen again and we have to preserve our methods and our sources.

There are a couple of ways we've already said, right? You know that the technical analysis of the data deletion malware from the attack shows clear links to other malware that we know the North Koreans previously developed. The tools in the Sony attacks bore striking similarities to a cyber attack that the North Koreans conducted in March of last year against South Korean banks and media outlets.

We've done a—I have, as you may know from watching "Silence of the Lambs," people who sit at Quantico…very dark jobs. Their job is trying to understand the minds of bad actors. That's our behavioral analysis unit. We put them to work studying the statements, the writings, the diction of the people who claim to be the so-called Guardians of Peace in this attack. We compared it to other attacks that we know the North Koreans have done and they say, "Easy for us. It's the same actors."

We brought in a red team from all across the intelligence community and said, "Let's hack at this. What else could be explaining this? What other explanations might there be? What might we be missing? What competing hypothesis might there be? Evaluate possible alternatives. What might we be missing?" And we end up in the same place.

Now, I know because I've read it in the newspaper and I've seen it on the news, that some serious folks have suggested that we have it wrong. I would suggest—I'm not suggesting. I'm saying. They don't have the facts that I have, don't see what I see, but there are a couple things that I have urged the intelligence community to declassify that I want to tell you right now.

The Guardians of Peace would send e-mails threatening Sony employees and would post online various statements explaining their work. In nearly every case they used proxy servers to disguise where they were coming from in sending those e-mails and in posting those statements.

But several times they got sloppy. Several times, either because they forgot or because they had a technical problem, they connected directly and we could see them. And we could see that the IP addresses that were being used to post and to send the e-mails were coming IPs that were exclusively used by the North Koreans.

It was a mistake by them that we haven't told you about before that was a very clear indication who was doing this. They would shut it off very quickly once they realized the mistake, but not before we saw them and knew where it was coming from.

As I said, we have a range of other sources and methods that I'm going to continue to protect because we think they're critical to our ability—the entire intelligence community's ability—to see future attacks and to understand this attack better. We have brought them all to bear in this situation and I remain where I started—not with just high confidence, but very high confidence that the North Koreans perpetrated this attack.

We're still looking to identify the vector. How did they get into Sony? We see so far spear phishing coming at Sony in September—as late as September of this year. We're still working that and when we figure that out we'll do our best to give you the details on that, but that seems the likely vector for the entry into Sony.

Overall we think this investigation is a prime example as well of the importance of public-private partnerships which I'm going to talk about in a second. Sony did the right thing here. The moment they knew they had this problem they reached out to the FBI and have been a great partner ever since in trying to unwind it, understand the nature and scope of the attack, and identify the perpetrators.

So there is no doubt that imposing costs, both laying hands on people and calling out bad conduct, has to be part of the FBI strategy, and it will be.

Fourth. We need to get better at helping our state and local partners deal with the threat because all manner of crimes that we don't have the resources and time to get to are appearing for the county sheriffs, the local police departments, the local DAs.

Their citizens are saying, "I was ripped off. Somebody sent me an e-mail saying the FBI director needs me to wire this money to Nigeria and I wired it. And so I need help."

I don't want anyone within the sound of my voice—I never want you to wire money to me anywhere on the earth.

We need to equip our state and local partners to be able to be digitally literate and to conduct their investigations in responding to the same threats coming through the vector that is cyber. And so one of the things we're trying to do is work with the Secret Service to offer training to the 17,000 state and local law enforcement organizations in this country to equip their people to be digitally literate. A ton of work going on there. Lots more needs to be done.

And then last, the fifth part of the strategy is the importance of increasing our cooperation and improving our cooperation with our private partners. Let me say why this matters so much. I think you get this. All of it is in your world, private sector partners. Invariably, that's where the victims are. That's where the information is that we need in order to be able to respond to actions by nation states, by terrorists, by hacktivists, by all—the entire layer cake manifests itself on your networks and on your systems. If we can't find a way to effectively share that information to those of us with the enforcement powers, we're sunk.

You also see things. You have tremendous brains in the private sector. You see things. You think of things that could be tremendously useful to us. We have to find ways, productive ways, to get the content of your brain into the government.

Without effective sharing, I'm a bit like a police officer patrolling a street with 50-foot high walls. Solid walls on either side of the street. I can tell you the street looks fine. The little piece of the world that I can see clearly, it looks clean to me. If I can't see through that 50-foot wall into that neighborhood, I have no ability to help make it safe or to even

tell you what's going on there. We have to find a way to make those walls in some fashion at least semi-permeable so we can share information.

This is not easy. I know some of the frustration on the private sector side. As I have said, I was the general counsel of two companies before coming back to government, and I've been in lots of conversation that went like this. "Why doesn't the government tell us something?" Right? "What are they going to do with what we tell them? What if it leaks? What if it gets used against us in a competition? What if we get accused of lying to somebody? What if we get sued? What are our shareholders going to think? What's the board going to think? Why can't the government tell us things that we can actually do something about?"

I understand some of the challenges that lay there right now. I think we need clearer rules for the private sector…to offer clear rules of the road for what will happen to what you share and what we need you to share. Right? We need better technology. Be able to share information both ways more effectively and more quickly. You need protection. You need guidance. I need information.

We have made significant progress in a lot of the different parts of the American economy in sharing, but there are a bunch of impediments that remain. Mechanical, I mentioned. Legal, I mentioned. And then there's one that's harder to describe, but feels very real to me, and that is cultural.

In the wake of Mr. Snowden's so-called revelations, there's a wind blowing that I worry has blown what is a healthy skepticism of government power—I think everybody should be skeptical of government—to a cynicism so that people don't want to be with us anymore. Meet us out behind the 7-Eleven late at night and I'll talk to you as long as nobody sees me. Or wear a bag over my head to a meeting with the government. Because there is this wind blowing that there's something bad if you're touching the United States Government. We have to build even though there's that wind. We've got to do our best to speak into that wind to try to explain how we're using our authorities in the government. But we simply cannot fight this threat without talking to each other. Without building effective bridges despite the wind that's blowing.

So that's our strategy. Focus ourselves, shrink the world, impose real costs, get better at cooperating with our state and local partners and maybe most of all, get better at cooperating with our private sector partners.

Before I leave you though I want to mention something that I know Cy Vance mentioned today because he's been a leader on this—the problem of what we call Going Dark.

This is very, very important to us in law enforcement. Especially in law enforcement. We are drifting to a place in this country without serious public discussion that I don't think a democracy should drift to without discussion.

When I left government in 2005, there was a significant Going Dark problem with data in motion. We were increasingly finding ourselves in a place where we went to a judge, we got a court order, we showed probable cause, we had permission to intercept data in motion and we couldn't.

That problem was kind of blinking off to my periphery in 2005. When I came back in 2013, it's blinking directly in front of me because of the proliferation of communication modes, right? The hundreds and hundreds of apps through which people communicate. We're making it increasingly difficult for us with lawful authority, especially in our criminal work, to be able to intercept the communications of drug dealers, organized criminals, of bad people of all sorts with court approval.

But there's another dimension to it that made it blink even more brightly—directly in front of me. Not just the data motion. Increasingly what we're finding ourselves up against is data at rest that is sitting in a place or in a device that, even with a search warrant, we can't get access to. And this is everywhere in law enforcement.

There used to be a day in the good old days of law enforcement, you get a search warrant, you enter a drug location and the knuckleheads would have written down in one of those black composition books who got what and how many kilos there were and you take the book and you would photocopy it and give it to the prosecutor and you would be good to go. Now we encounter a thumb drive, a PDA, a laptop, a tablet…and increasingly we're encountering devices that we cannot get access to even with lawful

authority. To me, this is not about the government wanting to whack people's privacy. I'm a big fan of privacy. I don't want the government, without lawful authority, going through anything of mine.

This, though, is about us drifting to a place where there will be zones beyond the reach of the law in the United States. The Fourth Amendment is one of the most important parts of this entire democracy because the government may not search and seize the people's papers and effects without a warrant. But now we're drifting to a place that, even with a warrant, there will be papers and effects, even with court authority, that are beyond the reach of the law. Maybe we want to go there. Maybe that's where we want to end up as a democracy. Maybe people decide that privacy is that important. But I don't think we're talking about it enough. I don't think we're thinking about, "So what are the trade-offs involved there?"

My job, I don't believe, is to tell people what to do. I mean, in a democracy, the people should decide what to do. My job, I think, is simply to say there are significant public safety implications here and let's talk about it before we get to the place that Cy Vance talks about. Where people look at us with tears in their eyes and say, "What do you mean you can't? What do you mean you can't? This little girl has disappeared. What do you mean you can't tell me who she was texting with before she disappeared? You've got the phone. You've got a court order." Before we get to "what do you mean you can't," I think we've got to talk about it as a people.

So, in conclusion, thank you for being here. Just that you're attending this conference is a sign that you get the significance and the challenge we face that cyber has truly changed everything we're responsible for. Thank you especially to those of you in the private sector for making us smarter, for pushing us, for asking hard questions. I meant it when I said people should be skeptical of government. Ask hard questions. We will learn from your questions.

Thank you for helping us catch the bad guys that are trying to do so much harm to you. And most of all, thank you for the work that I think we will do together in a lawful, appropriate way to protect the American people. Thanks for listening.