James B. Comey

Director
Federal Bureau of Investigation

Sixth Annual Financial Crimes and Cyber Security Symposium, Federal Reserve Bank

New York City, New York

November 18, 2015

Confronting the Cyber Threat

Remarks as delivered.

Thank you so much. And you're stuck with me for another seven years and 10 months—not that I'm counting. But thank you for the citation, and back at you, Cy. Thank you for your leadership on so many issues, but especially on all things cyber and especially the encryption challenge that we face, which I'll say a few words about.

Let me begin, though, by saying that my heart, as I'm sure is true of everybody in this auditorium, remains heavy, after the tremendous loss suffered by the people of France and the people of the world on Friday night. We have long had a very close counterterrorism relationship with our French colleagues. It remains strong, it will be strong, we will lean on it very hard in the days ahead. As you know, we, together with our partners—and I'm in a city that is the best example in this nation of the partnerships at the federal, state, and local levels on counterterrorism—we are working around the clock to make sure that such things do not happen here in the United States, and I'm very grateful for the partnerships.

We're here, though, today to talk about cyber, and I want to share some thoughts with you about how the FBI is thinking about it, some of the challenges that we face. And I want to touch briefly on why we are talking so much about encryption these days—why both the district attorney and I believe this is such an important topic for all of us to care about.

Let me start with how I think about the threat. And I think everyone in this room gets this, so I won't spend a lot of time on this. But sometimes, people who don't do our work, we have to frame it for them in a way that I hope resonates.

I believe that we stand in the middle of the greatest transformation in human relations in human history. And this is a change that affects all of the FBI's work, because cyber is not a thing, it's a way—it's a vector. Because we have connected all of our lives to the Internet; because it's where we bank; because it's where we have social lives— if I had one, I'm sure it would be on the Internet. It's where our children play, it's where our health care is, it's where our financial information is, it's where our critical infrastructure is. It's where life is. And that will become more and more true as the "Internet of things" becomes a feature of all of our lives, and our sneakers talk to our refrigerator and our car talks to our heating system. All of our lives are there, and so those who would do us harm—who would steal our money, hurt our kids, damage our infrastructure, look to attack our nation—that's where they come. It is a vector change unlike any we've ever seen before.

The modern FBI was born, a little less than a hundred years ago in practical terms, in response to the great vector change of the early 20th century—when the confluence of asphalt and the automobile introduced a kind of crime that no one had ever seen before. You always had robberies, but now they were coming in a vector that was unimagined in its scope and in its speed. John Dillinger could do robberies in two states in the same day, moving at 55 miles an hour downhill. All of a sudden, county lines were very meaningful and state lines were meaningful, and this vector change thwarted law enforcement. And so what was needed was a national force to span those boundaries and respond to that threat—and the modern FBI was born. I'm the seventh Director, the first FBI Director was there, and the modern FBI in a real sense was a response to that vector change.

This vector changes dwarfs that in ways that are even hard to describe, because Dillinger could not do a thousand robberies in all 50 states all in the same day in his pajamas halfway around the world, moving at the speed of light. That is what we face today. So now, county lines—not really meaningful against this threat. State lines, international lines are not meaningful against this threat. This threat, moving at 186,000

miles per second—which I think is the speed of light—shrinks the world to the size of a dot, and poses enormous challenges for us.

So we in the FBI have a strategy, which I want to explain to you very briefly, to try to respond to that. But at the core of it is humility. We have never seen a transformation in human history like this vector change, so it would be arrogant in the extreme to stand in the middle of it and say, “I can see the future. I know how we should be deployed, equipped, and trained against this threat, against this vector change that the world has never experienced.”

Instead, we have to approach it with humility and say, we’re going to do things that seem reasonable, we’re going to get feedback, and we’re going to iterate, to make sure we’re responding to something no one has ever seen before.

The Bureau’s strategy is pretty straightforward, and it has five parts that I’ll explain to you very quickly.

The first thing we’re trying to do in the FBI is focus ourselves. I think of the threats coming at us through that vector as a stack. At the top are nation-state actors coming at us through cyber intrusions, looking to steal, obviously, government secrets, steal innovation. There are near-state actors working in league with them. There are huge international syndicates bent on stealing information, stealing money, stealing identities to facilitate other crimes. There are individual criminals, there are hacktivists, there are creeps and weirdos of all kinds, there are bullies, there are people sending people e-mails saying that I need you to wire money to me in Nigeria or someplace—those are all part of the stack, but towards the lower end of the stack. (And don’t ever wire me money anywhere, please—I don’t need it and I’m not in Nigeria.)

What we’re trying to do is focus ourselves on the work that makes the most sense given the FBI’s footprint, which is global, and our resources. We’re trying to focus ourselves on the top of that stack—on the nation-state intrusions; on the sophisticated international criminal syndicates; the enormous botnets—the biggest, most international aspects of all things cyber. So doing that, we think that if we can focus ourselves, we’ll be better than if we try to do everything.

And our focus takes a form of assigning the work differently than we have before in the FBI. Normally, physical location is an important element of where work is assigned in the FBI, for obvious reasons. If a bank robbery happens in Chicago, we're going to assign it to the Chicago office. But physical location is actually not all that meaningful when you're talking about threats that are moving at the speed of light from halfway around the world. So we're actually pushing physical location down a little bit in deciding where we assign work.

We've come up with something we call a cyber threat team model, where we assign work not based on where the physical manifestation of an intrusion is—what company got hit, what bank got hit, and where they're headquartered—but instead where the talent is. So the FBI assigns threats based on where we think the best talent against that threat is. That may be in Little Rock, Arkansas, that may be in New York, that may be in Tampa, that may be Seattle—even where victim companies are not located in those jurisdictions. But, to take account of the fact that physical manifestations matter, we assign that one office as the owner of the threat, and we allow up to four other offices to assist, to make sure that we're conducting effective liaison with chief security officers, chief information security officers in the physical locations of those companies. So that's the first thing that we're trying to do—is assign work in a way that respects the change in this vector, and then we'll iterate if it doesn't make sense. But it seems to be working pretty well so far.

So the first part of our strategy is focus. The second part is, we think, because the bad guys moving at the speed of light have shrunk the world to the size of a pin, we have to shrink it back. And that has two elements in our strategy, two elements of our "shrink" strategy.

First is, we're going to deploy more of our people around the world. We're going to push our analysts, and our cyber agents, our experts, to more and more places around the world—because even though this is an infrastructure-, a fiber-optic-based threat, those physical relationships, especially with our foreign partners where the keyboards may sit in their jurisdictions, matter tremendously. So you're going to see more and more FBI people pushed out around the world to try and shrink it back.

The second way we're trying to shrink the world is shrink the world inside the federal government. When I left government last in 2005, the federal government's response to the cyber threat reminded me of 4-year-old soccer. And I have five kids, so I've watched a lot of 4-year-old soccer—and those of you who've seen it, it's a big clump of kids moving together chasing the ball, because the ball's the thing. It's the cool thing, it's the important thing, so everybody on the field should go get the ball.

Returning to government, the good news is, when I came back in 2013, we had gotten to a place where everybody understood we have to spread out and we have to pass to each other. We had gotten to a place that I would say, probably college-level soccer. The challenge we face is that the bad guys are playing World Cup-level soccer. We have to continue to work the way we pass the ball, the way we assign positions, and the way we see the field and visualize the field.

At the core of that for the federal government is something called the NCIJTF—the National Cyber Investigative Joint Task Force. It's a mouthful to say, but it's actually the beating heart of avoiding the 4-year-old soccer problem, because that NCIJTF is made up of 20 federal agencies from the law enforcement world and the intelligence world, that sit together in a facility in the D.C. area, visualize the threat, and share information and coordinate their work. "You have a good left foot, you ought to take this shot; I've got a good right foot, I'll take that shot. You tell me how it goes, we'll talk to each other so we accomplish the goal of winning the game." We have very cool facilities there—which I'm not going to describe—that allow us to visualize what's going on, on a worldwide basis, with the cyber threat, and chop up the work and pass it to each other. We even have close foreign partners now sitting in the same space, to help us shrink the world back.

So that is the second element of our strategy: we're going to focus ourselves, and then we're going to try and shrink the world. And the reason we're going to try to do those things is we need to, as the third part of our strategy, impose costs.

All of us who do this work have a sense that people around the world, bad guys around the world, think it's a freebie—that if I'm in my pajamas at a keyboard halfway around the world, I can steal anything from—I'm responsible for the United States, I'll talk about

the United States—anything from Americans, and it's a freebie. It's not like I kicked in their door and walked out with their valuables, or walked out with the things that matter most to them. It's not like I harmed their children directly.

We understand in law enforcement—and we have to make sure the criminals understand—that it is the same. Even though you're in your pajamas, you are still terrorizing children, you are still stealing that which matters most to us. And we have to get to a place where, even if someone is at the keyboard in their basement somewhere on the other side of the earth, they feel us behind them—they can feel our breath on their neck. And we have to impose costs to make that happen. We have to lock people up, so they understand this is not a freebie.

Critical to that locking up, that being able to impose costs, is shrinking the world—because so often the takedowns that we're involved in require international cooperation. Everybody in this room understands the threat well. It was illustrated vividly recently with the announcement, here in the Southern District of New York, of the indictments of the hackers who were running, as the U.S. Attorney said, a sophisticated enterprise that, at its core, was hacking—to steal personal information, to steal press information, to manipulate stock prices, to run basically a multinational criminal enterprise that relied upon their ability to hack. Key to taking that down was cooperation. In that case we had great cooperation with our friends in Israel, to be able to impose costs by putting handcuffs on people around the world all at the same time.

We have to do more and more of that. Wherever possible, we have to lay hands on people, to make sure they understand these are as serious a crime as if you kicked in a door in someone's apartment here in Manhattan.

If we can't lay hands on people, we have to call out the conduct. You saw us doing this, I hope, over the last year, calling out the conduct of Chinese actors in stealing American innovation, in calling out the action of the North Korean government in attacking Sony. We hope that by calling it out, naming the conduct, talking about the conduct, we can change behavior. And we can lock people up, we can call it out, and third, we have to make sure people understand that we have many flaws, because we're human, but we are dogged people—and we do not forget. Even Russian hackers like to go on vacation.

Even Russian hackers like to go on a honeymoon to somewhere in the Mediterranean. We will be there, and we will impose costs in order to change behavior.

So: focus ourselves; shrink the world, so that we can impose costs.

The fourth part of our strategy is, we simply must help our state and local partners be more effective at investigating in the digital world. In the good old days, you could do a search warrant—in a drug case, or an organized crime case—and hit a location responding with a judge's order and find paper. In the good old days, you would find black composition notebooks in which the morons would have written who got how much—Shorty got this, Joe got that, and changes and names.

The good old days are gone. Because in any case you work, when you hit that location pursuant to a search warrant, you're going to find thumb drives, PDAs, laptops—devices that require digital literacy. Every single investigator in this nation, to be effective, has to be a digital investigator. We in the federal government have to do a better job of equipping them, especially with the training that they need to be effective.

There's great progress being made here as part of our strategy. We and the Secret Service are working together to push out training, to make it available to people, so they can become certified cyber investigators. Those of you in law enforcement know the LEEP portal—that is available on the LEEP portal—people can do most of that training from their desks in their police offices around the country. We have to do more and more of that to equip our state and local partners.

I also think that to work more effectively, it does not make sense, at least to my mind, that the FBI and the Secret Service each have cyber task forces in cities around the country. It makes too much sense to me to combine them. And so we're actually trying a pilot in Atlanta and Boston where we're going to combine our task forces and see how it goes. I think it'll go fine. I think they have great talent, we have great talent. "Turf" makes no sense at all when you're talking about the volume of threat we face when it comes to cyber. So I hope the model you see down the road is us doing that work together, and then equipping our state and local partners to do the work—especially in

the smaller jurisdictions, which don't have the sophistication and the resources of NYPD or the Manhattan D.A.'s office. We have to help them.

And that leads me to the fifth part of our strategy: we simply must get better at working with the private sector. This is an enormous challenge. It's essential to us, because nearly all the information we need to be effective sits on the private sector's infrastructure—which is a great thing; it's a wonderful thing that the Internet is in private hands in the United States. The expertise resides within the private sector, so if we're going to be good at what we do we have to cooperate better.

In the absence of effective cooperation, we are left, in law enforcement, like police officers patrolling the street with 50-foot-high walls on either side. We can tell you with high confidence, "The street is safe." But if we can't find a way to offer assistance and to have vision into the neighborhoods through those walls, we're not going to be able to help the people who live there.

This faces a bunch of different challenges—legal, technical, and cultural. But it's not a moon landing. This is something, given the stakes, we should be able to accomplish.

Start with legal. We need clear rules of the road for companies to have them understand, if I share information with the government, here's what happens to it; here's how it can be used; here are the risks associated with that; and here's how those risks are mitigated. There's good work being done on that—I'm optimistic we're going to solve those problems.

Second, technical. There are all kinds of good relationships going on to push information—a lot of them analog, writing things on a piece of paper. We have to get to a place where we share information at machine speed. We have to get to a place where we push information to each other in a way that moves at the speed of the threat.

There's good work being done here. I hope you know the FBI has worked very, very hard in the last two years to get better at pushing information very, very quickly to our partners. We've pushed out dozens and dozens and dozens of our FLASH alerts, of our

Private Industry Notifications, our PINs. We've put on hundreds of briefings of CISOs and trusted partners to make sure they understand the threat. But we have to do more.

One example of doing more is the Malware Investigator, which I hope you've heard of. This is a tool that we are making available to the private sector that I think represents the future. The FBI has long had our own database of malware. And any FBI agent working a case takes a sample of malware and queries our internal database, and then gets a hit if we've seen that malware before and knows it connects to something in San Diego or in Houston. We're making that tool available to our private sector partners. So a private sector partner can sit at the same screen and query our database with their malware sample to see what it connects to.

What's in it for the private sector is obvious—you get very, very quick responses; know what to do, who to go talk to. What's in it for us is we'll get more samples of malware, to allow our "fingerprint" database in the digital world to get better and more complete and more useful to the private sector. We have to do more of that kind of stuff.

So, legal, technical; maybe the hardest of all over the last two years has been cultural. In the so-called post-Snowden world, a wind has blown that has chilled cooperation sometimes across the divide between the government and the private sector. We have to resist that, by pushing what might have been cynicism back to skepticism.

People should be skeptical of government power—they should want to know what our authorities are, how we use them, how we're overseen. That's very, very important. I like to explain to people, you should not trust people simply because they seem like good people. You should want to know: how are they overseen? What are their authorities? What are the checks and balances? I think I'm a good person—don't trust me; ask. What are the details? There's an angel in those details.

So we need to continue to have those conversations, to push cynicism to healthy skepticism. But also I think events in the world have helped push it back.

There is no better example of the importance to our entire nation of cooperation than the Sony attack. The Sony attack was a vicious, hugely damaging attack to that

company. But we were able to respond quickly to it, and effectively to it, because Sony knew us. All of America's companies spend lots of time making sure the fire department knows your company, so that if there's a disaster, they know where to go. If it's in the dark, they know how to rescue people. If it's smoky, they know where to go. They have a sense of what's needed to do to protect people.

Fortunately, with a company like Sony, they knew us well enough that we could respond quickly like that. Companies need to do that. If you're running a private enterprise in America today, you better know us, in a good way, so if something happens, we can help you. I see more and more of that happening and it's helping to calm some of the cultural winds that we face—but there's a lot more work to do there.

So we are going to: focus ourselves; try to shrink the world; try to impose costs; try to work better with our private sector partners; and try to help our state and local partners be more effective. We have a long way to go.

Sometimes an obstacle to private sector cooperation is what I call "weenie general counsels." Now here's the thing: I was a weenie general counsel, at two different companies. And that's the job of a general counsel—to ask questions like this: "What?" Or to say, "What's the government going to do with that?" or "How might we get hurt by this?" and "What if it leaked, or what if it gets used against us in a competition?" or, "What a minute—what if people claim we defamed them? Whose information is this?"

Those are all important questions. We in the government have to engage to make sure those folks get good answers to that. But what's been interesting in the post-Sony world is, I think CEOs and boards understand, in a way they might not have before, that it is a business imperative to cooperate with the government—in a lawful, appropriate way—but to make sure you are in a position to take advantage of our resources, and to make sure that we're in a position appropriate to help you when you are threatened. I think it has engaged the general counsels' clients in a way that it didn't before, and I think that's a very healthy thing.

So thank you for your engagement on this. We will get better as a result. And we will approach it with humility and take feedback to iterate.

I want to explain, though, before I say goodbye to you, why this encryption issue that the district attorney and I have talked about so much, and Commissioner Bratton has talked about so much, matters.

We are drifting to a place in America where lawful court orders—judicial search warrants, judicial wire intercept orders that are the lifeblood of our criminal work to protect children, to fight gangs, to solve kidnappings—all the work that we do requires that judicial orders be complied with, to have us get the information to stop bad things from happening, and to catch and punish those people who have done bad things—we're drifting to a place where increasingly those orders are ineffective, because a device is protected by full encryption, or data-in-motion is fully encrypted.

And the challenge we face is illustrated this way. It's not a "cryptowar." I hate the "war" metaphor, because wars are fought by people who don't share values. This conversation involves people who all share the same values, whether you work for the FBI or you work for a tech company.

All of us care about two things. All of us care about safety and security on the Internet. I am a huge fan of strong encryption. If the government used it better in some circumstances, people wouldn't be reading my security clearance documents in other parts of the world. I am a big fan of strong encryption—it helps us protect our innovation, it helps us protect our banking information, it helps us protect that which matters so much. And it makes my life easier to try to respond to cyber intrusions.

And all of us care about public safety. All of us care about protecting people, protecting children, protecting cities, protecting all the things we're sworn to protect.

In the form of strong encryption, we now see a collision between those two values. And it's illustrated no better than through the threat posed to us by the group that we call ISIL, the so-called Islamic State—which in the United States, to talk about what they've been doing here, has been recruiting through social media. And if they find a live one, they move them to Twitter direct messaging—which we can get access to with judicial process. But if they find somebody they think might kill on their behalf, or might come and kill in the caliphate, they move them to a mobile messaging app that's end-to-end

encrypted. And at that moment, the needle we've been searching the entire nation to find, and have found, goes invisible to us.

That is the Going Dark problem. That is the collision between two values we all care about. That is the collision between safety and security on the Internet, which is a great thing, and public safety, which is a great thing.

There is not an easy answer to the resolution of that collision between values. But democracies should not drift. Democracies should talk about hard things and figure out, how might we deal with this? Because the stakes are too high to drift to a place where someday, people look at me or look at the district attorney and say, "Wait a minute, what? What do you mean the tools that we rely on you to use aren't effective?" Our jobs are to send up a flare to tell people: those tools you need us to use and you thought we were using—there is a big problem with those.

The FBI is not an alien force imposed on America from Mars. The FBI belongs to the American people. We only have the authorities granted to us by the United States Congress on behalf of the American people. My job is to tell the American people when the tools that you have given us through Congress are being several impaired by a collision of two values we all care about. Very, very hard problem—but the stakes require us to engage on it and talk about it.

The good news—thanks to the work that Cy Vance has done, that Bill Bratton has done, that we at the FBI have tried to do—is, I think the temperature has come down. I think people realize we are not maniacs. We're maniacs in some ways, we're not maniacs in this way. We see a problem, and serious people who stare at it see the same problem. What's next is: what do we, as smart people, do to try and solve that problem? I'm very grateful for Cy's leadership on this. We have to keep talking about this, because it really matters.

So thank you for engaging on all things cyber. Those of you in the private sector, thank you for fighting through cultural headwinds, through practical headwinds, through legal headwinds, to find a sustainable, healthy, appropriate, lawful basis for cooperating

across that divide, so that the street and the neighborhoods are both able to be patrolled in a safe way, and all of us are safer and better as a result.

And I thank you for your time.