OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Public Affairs Office
LEADING INTELLIGENCE INTEGRATION

Remarks as delivered by
The Honorable James R. Clapper
Director of National Intelligence

"National Intelligence, North Korea, and the National Cyber Discussion"

International Conference on Cyber Security
Fordham University
Wednesday, Jan 7, 2015
9:00 a.m.

It's great to be here after fighting the snow traffic in Washington to get to the airport, and then flying here.

I want to thank Father McShane [Fordham University President Joseph M. McShane], for that kind introduction. You have some truly remarkable speakers and panels this week, and I'm humbled that you invited me to speak. Thanks for having me.

Later this morning, in fact right after me – I'm serving as the warm-up act for FBI Director Jim Comey. He really is the senior expert on the investigative side of cybersecurity. And tomorrow, CYBERCOM Commander and NSA Director Admiral Mike Rogers is speaking, and he's the senior expert on how cybersecurity ops actually happen.

You have three-and-a-half days filled with cyber experts, from government, the academic world, and industry. So in the interests of truth in advertising, I'm not an expert on cyber. I guess that's a way of saying I'm going to refer technical questions to the real experts here.

So, I was trying to think through what my contribution to this conference could possibly be. Well, I recently traveled to North Korea (and back, happily). So I thought I'd talk about that. [delayed laughter]

Yes, that's a joke. [laughter] I learned from Father McShane that this crowd needs cuing. [laughter, applause]

I'll talk about that and how it applies to this week's conversation about cyber, given the Sony hack.

The first question I always get about the trip is: "Why you?" As in, "Why on earth would we send the DNI, the director of national intelligence, especially *this* DNI, on a diplomatic mission to get two American citizens who were imprisoned in North Korea?"

Why would they send me? The truth is, the mission had been in the works for quite a while. North Korea wanted an active member of the National Security Council and a cabinet level official to come and to bring a letter from President Obama.

The White House knows I've had a long history of working Korean issues, since I served as chief of intelligence for U.S. Forces in Korea in the mid-'80s. So the White House put my name forward to the DPRK, the Democratic People's Republic of Korea as they call themselves, government in Pyongyang. And I think we were all surprised, to include me, when they agreed. That's how and why I was picked to go.

Actually, I thought the New York Times had a better explanation: Clapper is "Gruff, blunt-speaking and seen by many as a throwback to the Cold War." [laughter]

"An unlikely diplomat, but perfect for the North Koreans." [laughter]

That's the nicest thing the New York Times has ever written about me. [laughter, applause]

So I want to talk about a few experiences from that trip, and how some insight from the trip could play into our discussion about cyber. But first, for those who may not be familiar with the director of national intelligence, I thought I'd spend a couple of minutes on that.

Later this spring, my office will be celebrating our tenth anniversary of our standup in April of 2005. Our establishment came from shortfalls perceived by the 9/11 Commission. The

assertion was that the intelligence agencies weren't sharing information with each other and were incapable of "acting jointly."

So ten years ago, Congress and the President created the position of the DNI, which I now occupy and have for the past four-and-a-half years, and it feels like it's been at least four-and-a-half years.

That was a joke too. [laughter]

Part of my statutory job description designates me as the President's senior, but by no means exclusive, intelligence advisor. We have many, many experts on intelligence.

Another part of the law says I manage the national intelligence budget, which, by the way, has not gotten a pass, as some people seem to think, from the Balanced Budget Act and sequestration.

But I believe the third duty of the DNI is the most critical, which is bridging that "joint action" gap that the 9/11 Commission identified.

And that responsibility goes way, *way* beyond just getting the intelligence agencies to talk to one another. It's about helping them to recognize the cultural strengths and capabilities that each of the 17 Intelligence Community elements brings to the table and then getting them to think as a community. It's about the intelligence culture, bringing our best and most appropriate community resources to bear against our toughest national security problems.

That's what I've referred to as "intelligence integration." It's been my theme, my shtick, my mantra, for the past four-and-a-half years, because I believe that's what the 9/11 Commission had in mind. And that was instantiated in law by the Intelligence Reform and Terrorism Prevention Act of 2004 that created my position – a seriously flawed piece of legislation, as most legislation is.

Intelligence integration is the prerequisite to reaching the 9/11 Commission's goal that we act jointly as an Intelligence Community. That means integration horizontally, across agency lines, with each agency on equal footing and stature. I'm speaking of the Central Intelligence Agency, the National Security Agency, the National Reconnaissance Office, etc.

But I also believe we have to work toward vertical integration from federal to state and local governments, and also to commercial partners, like many here. So that's primarily why I'm here today; to take advantage of a great opportunity to encourage intelligence, law enforcement, homeland security, state and locals, and private industry to work together, to the fullest extent we can, on this difficult cyber problem.

But, I'm also here to promote transparency. That's the big lesson I've learned from the past few years of unauthorized leaks. We've got to preserve and protect our tradecraft, the special skills and capabilities that let us do our work. At the same time, we need to talk to the American public more about other things, the things we can talk about.

So with that long preamble, I want to jump into the things we need to talk about as part of an ongoing cyber conversation. From an intelligence standpoint, that conversation starts with the cyber threat, of course.

Every spring for the past four years, I've made the rounds on Capitol Hill, testifying in open sessions to our various Congressional oversight committees, about our assessments of worldwide threats. Talking to Congress in the open about classified matters and dancing around many issues, in televised sessions, while trying to protect intelligence tradecraft, is one of my favorite things to do. [laughter]

Right up there with getting a root canal or folding fitted sheets. [laughter and applause]

But I'll be doing it again, starting in just a few weeks, because it's important to be open and transparent with the issues we can discuss, even though for me as a career intelligence guy, it's almost genetically antithetical to be transparent.

Each of the past four years, I've told Congress that we're facing the most diverse array of threats I've seen in all my years in the intelligence business. That line has morphed from "my almost 50 years in the intelligence business," to "my 50 years," to "my more than 50 years in the intelligence business," because the threats have grown substantially more diverse every year – so much so that in 2014, I had to go back to the Hill in the late summer to give a mid-year threat update.

At the threat hearings two years ago, we made news when "cyber" bumped "terrorism" off the top of our list of threats. That was the first time since 9/11. But that top-of-the-list cyber threat doesn't mean what a lot of people think it means. Although we must be prepared for a large-scale strike – a "Cyber Pearl Harbor" scenario or "Cyber 9/11," (Big scary things like that get play in the media), our reality is that we've been living with a constant barrage of cyber attacks for some time now.

And those attacks are not monolithic. Different cyber actors have different capabilities and different goals when conducting operations in Cyberspace. Russia for example, has a broad range of highly sophisticated technical and human intelligence capabilities. Moscow's focus goes beyond just taking advantage of common vulnerabilities that can be fixed with a software patch, and in the event of a military conflict or geo-political crisis with Russia, some U.S. critical infrastructure networks will be at risk.

So the Russian cyber threat is much more sophisticated than the others and we've seen that Iran and North Korea are now unpredictable and aggressive cyber actors who aren't afraid to undertake offensive cyber operations against private sector targets. But we hear a lot more public discussion of the Chinese, because they, and now the North Koreans, are much noisier. China has been robbing our industrial base blind, largely with vulnerabilities that are easy to guard against or to simply fix. And that's one of the places where we can talk about a government and industry partnership.

Now, I recognize that banks and retail stores aren't about to turn their systems over to the FBI and Department of Homeland Security to look for cracks in their cyber firewall, but we can definitely help each other carry out our respective roles. So I want to lay out three things that the private sector can do today that will protect them from the vast majority of attacks, from the Chinese and elsewhere.

One: Patch IT software obsessively. Most Chinese cyber intrusions are through well-known vulnerabilities that can be fixed with patches already available.

Two: Segment your data. A single breach shouldn't give attackers access to an entire network infrastructure and a mother lode of proprietary data.

If you've seen James Cameron's movie, Titanic, and I guess statistically, everyone here has seen it six times [laughter], you'll remember the forensic reconstruction of the sinking – how the ship had segmented bulkheads, so that if the hull was breached, the flooding would stay isolated to just one section, and the ship would stay afloat.

But the forensic analysis in the film showed that the bulkheads didn't go high enough, and so the water spilled over the top of each section into the next section until the entire ship was flooded. So we tell the private sector: Don't let that happen to your data. Make sure a single breach won't sink your entire company, your entire enterprise.

And Three: Pay attention to the threat bulletins that DHS and FBI put out. This is the easiest and least intrusive way for industry and government to partner on cyber. We're already warning about the intrusions that are taking place against U.S. businesses and advising the private sector about how to protect itself. So please take necessary measures and encourage your customers, partners, and contacts to pay attention to those bulletins, and let the Bureau know when an intrusion or attack happens, so that the FBI can do its part and help.

So those are the three free pieces of advice our cyber professionals are out proselytizing. I'm sure those are things everyone here already knows, but there's a good reason I'm saying

them again: because bad cyber actors are using precisely those avenues to steal our lunch every day. The Chinese in particular are cleaning us out, because we know we're supposed to do those simple things, and yet we don't do them.

And, if there's a fourth commandment, it's this: Teach folks what spear phishing looks like. So many times, the Chinese and others get access to our systems just by pretending to be someone else and then asking for access, and someone gives it to them.

In national defense, few things turn heads like seeing your aviation system flying over the skies of a foreign nation with a different flag on its tail, or finding out that an adversary is already working to counter your expensive, cutting-edge capabilities that haven't been released yet. And in the private sector there are few things more dispiriting to corporate health and morale and corporate wealth than seeing proprietary products show up on a foreign market a month before product-launch at a tenth of the price.

That's China's primary motivation: to catch up to and then surpass Western industrial and defense capabilities and to eventually pass by the U.S. economy.

The Chinese are focused on those goals; whereas the recent cyber attack from North Korea, which by the way is the most serious cyber attack ever made against U.S. interests with potentially hundreds-of-millions of dollars and counting in damages, was driven by an entirely different philosophy.

So, back to the weekend trip I took, which was exactly two months ago today. We flew into Pyongyang, the capital city, on Friday evening, the seventh of November. And the first thing that struck me was just how dark the city and airport were, just completely dark. We damaged a tire on the plane while taxiing in the dark, because of the poor construction of the taxiways and runways at Sunan airport.

Then, when I saw the city on Saturday, I was expecting to see drab clothes and lack of modern tools, people walking to get around, people sweeping and doing similar, mundane, labor-

intensive jobs. And those expectations were met, from what I saw of Pyongyang. But I was also struck by how impassive everyone was. They didn't show any emotion. They didn't stop to greet each other, didn't nod hello, and we didn't see anyone conversing or laughing. They were just going about their business, going wherever they were going. It was almost automaton like. It was eerie.

And the plight of the citizens of Pyongyang stood in solemn contrast to the dinner I had the previous night, Friday the seventh, an elaborate 12-course Korean meal. Having spent time in Korea, I consider myself somewhat a connoisseur of Korean food, and that was one of the best Korean meals I've ever had. Unfortunately, the company was not pleasurable.

My dinner host was General Kim, the four-star general in charge of the Reconnaissance General Bureau, the RGB, the organization later responsible for overseeing the attack against Sony. The RGB is an amalgam of special operations and intelligence resources. They do overseas collection, reconnaissance, and importantly, cyber operations.

General Kim claimed to me that he was my North Korean counterpart. He was just a couple years younger than I, and we had to communicate through a translator, a North Korean who spoke flawless English but with a British accent that was pretty strange. [laughter]

General Kim spent most of the meal berating me about American aggression and what terrible people we were. He said that North Korea was under siege by its closest neighbors, who were supported, aided, and abetted by the United States. He got louder and louder, and he kept leaning toward me, pointing his finger at my chest and saying that U.S. and South Korean exercises were a provocation to war.

And not being a diplomat, my reaction was to lean back across the table, point my finger at his chest, [laughter] and respond that shelling South Korean islands wasn't the most diplomatic course of action they could have taken either. [laughter] This kind of connoted the entire evening's conversation. [laughter and applause]

But of course, my purpose was to secure the release of our two citizens. So at one point, my executive assistant suggested I take a head break to let things cool off, which I did.

I guess I have to give the New York Times credit, "Gruff and blunt-speaking" aren't too far off. [laughter] I'm not sure I was "perfect for the North Koreans," though.

At the end of the evening, I presented General Kim with a letter from President Obama. The letter didn't say much, except to designate me as his envoy, and that releasing our two citizens would be viewed as a positive gesture.

Saturday, the next day, was nerve wracking. We weren't sure, (I wasn't at least), whether we were going to get our two citizens back or not. So we stayed around the state guesthouse all morning.

About 11:00 in the morning, Saturday, an emissary from the minister of state security showed up to announce that the DPRK government had demoted me. They no longer considered me the President's envoy, and accordingly, they couldn't guarantee my safety and security in the city of Pyongyang. He said the citizens of Pyongyang were aware and my purpose was to secure the release of our two "criminals."

Thanks. [laughter]

So we waited around and waited around. It's not like you can hail a cab and go ride around. We were under their control.

About 3:00 that afternoon, this same emissary from the minister of state security came back and said: You've got 20 minutes to hustle together your luggage and check out of this place. We're leaving.

We went in the vehicles to downtown Pyongyang, and we were ushered into a conference room there, and sat through an interesting "amnesty-granting ceremony," I guess I'd call it, in

which the minister of state security read a proclamation from Kim Jong Un, the Supreme Leader .

That was the first time I'd seen our two citizens, who were still in their prison garb. They were turned over to us. We got them a change of clothes, out to the vehicles, and back to the airport. I can't recall a time when an aircraft with "United States of America" emblazoned across it ever looked as good. [laughter]

The next day, really our second Saturday after we crossed the date line, we landed at McChord Air Force Base, near Seattle. I went up to the cockpit and watched the two family reunions, which were very gratifying and very emotional, and at that moment, it was all worth it to me.

Okay, I want to bring this story back to cyber. I think it's important to note that the general I had dinner with that first night, General Kim, is the director of the RGB. He's the guy who ultimately would have to okay the cyber attack against Sony, and he really is illustrative of the people we're dealing with in the cyber realm in North Korea.

All of that vitriol he spewed in my direction over dinner was real. They really do believe that they're constantly under siege from all directions. Painting us as an enemy that's about to invade their country any day now is one of the chief propaganda elements that's held North Korea together for the past 60 years. And they are deadly serious about affronts to the Supreme Leader, whom they consider to be a deity.

I watched *The Interview* over the weekend, and it's obvious to me that the North Koreans don't have a sense of humor. [laughter and applause]

The DPRK is a family-owned country. It's been that way ever since it was founded in the '40s. And there's no room for dissent, not when the favorite management technique of their leader is public executions. It's "super effective" as a management tool. [laughter]

Behind all of this, North Korea wants to be recognized as a world power. They see nuclear weapons as their insurance policy and ticket to survival, and the rest of their society, including their conventional military forces, suffers for it. But cyber is a powerful new realm for them, where they believe they can exert maximum influence at minimum cost, and this recent episode with Sony has shown that they can get recognition for their cyber capabilities.

That's why we have to push back. If they get global recognition at a low cost with no consequence, they'll do it again, and keep doing it again until we push back. And of course others will follow suit.

So, here in the United States, the role of the Intelligence Community is to put all of those factors in context, to give our national leaders the intelligence they need, everything that figures into their calculus to make good decisions about how to respond, and we have to do that without oversimplifying the situation and while acknowledging the things we don't know.

Despite what some people think, the Intelligence Community doesn't have the eyes and ears of God. We're not omniscient. A closed society like North Korea is a really hard target for intelligence, and they're just one small piece of the cyber-threat puzzle, which includes actors that aren't nation-states. We see indications that some terrorist organizations are very interested in developing offensive cyber capabilities, and that cybercriminals are using a growing black market to sell cyber tools with little regard for whose hands they fall into.

Taken all together, cyber poses an incredibly complex set of threats, because criminals, and "hacktivist" collectives like Anonymous, are all thrown in together with aggressors like North Korea and Iran, and with the Russians and Chinese, who could do real damage if they are so inclined. Each of those actors has different capabilities and different objectives when they engage in Cyberspace, and all them of operate on the same Internet.

It makes me long for the halcyon days of the Cold War, when the world essentially had two large, mutually exclusive communications networks. One belonged to the United States, dominated by the United States and our Allies, and the other was dominated by the Soviets and

theirs. So we could be reasonably sure that if we were listening to someone on the Soviet network, that person was not a U.S. citizen.

Today, the internet and telecommunications networks are all interconnected and global, and much of the technology the infrastructure relies on comes from the U.S. Our task, as an Intelligence Community, is to find the bad actors and to distinguish a terrorist sending directions on how to build a bomb or how to defeat TSA procedures, from someone sending their granddaughter a recipe for apple pie.

So we're not just looking for a needle in a haystack. We're looking for thousands of needles scattered over acres and acres of haystacks.

It's our job to provide insight into the nature of cyber intrusions and give warnings where we can, and that job is extremely difficult in the absence of international norms and standards. We're, to borrow a legal phrase, developing "a body of case law" to define what constitutes a cyberwar, or act of cyber terrorism, or cyber vandalism, or cybercrime. And we're learning as we go, just as everyone else is.

And through it all, the IC holds civil liberties and privacy as a top priority. We're going to make mistakes, (and some of those have been exposed), a small percentage of the time. We're going to accidentally intercept someone's grandma's apple pie recipe. But we've shown that when we do, as soon as we realize our mistake, we get rid of that information, and we report ourselves to the bodies that conduct oversight, in all three branches of the government. That's important to me, personally, because, by the way, I'm an American citizen, and I care about my civil liberties and privacy too.

Beyond that, when we can do so without compromising our tradecraft, we've been transparent with the public about our mistakes. So we've published about 5,000 pages of previously classified documents on our Tumblr website: "IC on the Record," many of which are pretty critical of our mistakes, including classified court documents that show the FISA court,

(the Foreign Intelligence Surveillance Act court that oversees sensitive surveillance programs), is not a so-called "rubber stamp.

Two years ago, I didn't know what a "Tumblr" was. Two weeks ago, Tumblr featured our site, the IC's site, as one of a select few "Big in 2014" sites for their end of year review. We were right up there with "L'il Bub." [laughter]

Another joke. [laughter] Sorry, I said I'll try to give you warning. [laughter]

I'm here to tell you, sharing the stage with a famous cat – *on the internet* – that's how you know you've arrived. [laughter and applause]

That, and traveling to North Korea.

So let me end with that point, and I think we have some time for some questions. Thanks.

###