|  |  |
| --- | --- |
| Theodore Roosevelt IV: | We are extremely lucky to have tonight to professionals who are going to talk about what is happening with foreign intelligence, and how it affects all of us. The challenge that we face is not limited just to our government. It affects all of us, and we need to change our behavior to be cognizant of what’s going on, and so we don’t give our adversaries advantages that they shouldn’t have. I don’t want to sound unduly dramatic by that, but that’s one of the main reasons that I think that we’re lucky enough to have the two professionals here. On my immediate right is Charlie McGonigal who has been named by the FBI director. He takes the post formerly in October. He’s the Special Agent in charge of counterintelligence in the New York field office. The New York field office is probably the most important field office that the FBI has. It is the most important field office I suspect. In some ways, may be more important than Washington itself. |
| Charles McGonigal: | I agree with you. |
| Theodore Roosevelt IV: | He’s joined the FBI in 1996, he worked on flight 800, worked on the terrorist bombings in the US embassies in Tanzania, Kenya. Obviously, worked on the September 11 attacks. To his immediate right is William or Bill Evanina who is the national counterintelligence executive, for NCIX in which role he is the head of counterintelligence for the US government, and the principal of counterintelligence and the security advisor to the director of national intelligence. He is also the director of counterintelligence in security Center, NCSC. The government loves all the acronyms, but that’s another acronym that he has. In that role, he leads and supports counterintelligence security activities of the US intelligence community, US government, and the private sector, which is for us. He also works closely with many of our allies. |
|  | Interestingly enough, he joined his intelligence career by joining the FBI 20 odd years ago. We’re going to start off with each of the panel, so we’ll talk for about 10 minutes. I will then follow up with questions, and then we’ll ask individuals in the audience to ask questions. Please remember two things, one, I’m sure you will have questions that they will not be able to answer. If it’s a question that’s an ongoing investigation, they simply can’t answer that. Please bear that in mind and respect that criteria. The second is, and I want to emphasize this strongly, they don’t want to hear statements from you, they want questions. Questions begin with words like what, how, or why. With that, let me turn it over to our two panelists. |
| Charles McGonigal: | Thank you, Ted, and thank you all for being here this evening. I know you’re committed to hearing a lot about counterintelligence. On a sad note though, my colleague and I share the fact with you that our director, James Comey, was just summarily fired by the president at the Attorney General’s recommendation this evening. James Comey has been officially fired as FBI director. Bill shares in this. I think we both felt that director Comey was probably one of the most loved leaders that we’ve had in the number of years commanding a leadership role in the FBI. I appreciate that. I think many of us who were nominated for leadership positions by him will forever hold him in esteem as we progress through our FBI careers. We wanted to share that with you as we just received the news as we walked in the door. |
|  | No idea who the next FBI director will be, but obviously, Andrew McKay will be probably acting director as we move forward here. Who also has the benefit of being a homegrown New York FBI agent, prior to his ascension to deputy director. Shifting gears a bit. We’re here to talk about counterintelligence, foreign influence. I won’t be able to answer every question as Ted pointed out for you this evening, but what I’d like to do is talk a little bit about the structure of the FBI first in New York. Historically, I would never be in audiences like this made available to the general public, because counterintelligence is generally, we deal with a lot of classified information. We work on projects and operations that generally the general public is not made aware of for a number of reasons. |
|  | However, since the 9/11 terrorist attack, and the 9/11 commission report, which probably many of you are familiar with, the FBI has expanded its public outreach in the counterintelligence realm, and I, for one, have been a steward of working with foreign governments and security services that I would historically probably not work with and share information. I think that has been very, very productive for the FBI and us in the counterintelligence realm, because why? Simply put, we are all facing the same threats. No matter what nation you hail from, or no matter what government you are growing, living under these days. By sharing information, and coordinating globally, we are in a much better position, I think from an information sharing standpoint, then we have been historically. We’ve benefited, not only in the terrorism realm, but also in the counterintelligence realm. A little bit about New York counterintelligence. |
|  | I always say, as the Special Agent in charge of counterintelligence in New York, if you are someone that has an interest in working counterintelligence, or you as a new, and I talked to my new FBI agents that come in out of the Academy daily, if you want to learn and work counterintelligence, New York City is the preeminent field office, as Ted referenced earlier, for working counterintelligence matters in the United States. I would challenge around the world counterintelligence from a sheer presence in the New York metropolitan area is tops. I won’t go into numbers, but I can tell you I have over 150 agents, which is larger than some FBI divisions throughout the country focused on working counterintelligence matters in the New York area. Areas within counterintelligence we focus on. Let’s talk about that for a moment. Espionage, number one. |
|  | Number one threat in counterintelligence is espionage. Those who have access to classified information that are either abusing that privilege by sharing that information with a foreign government, or someone that should not have access to it, or a need to know. We work espionage cases routinely in the FBI and across the board. Now, the only advantage our Washington field office has on the FBI New York is the level of cleared personnel. Those with security clearances in and around the Washington DC Northern Virginia area because of all the federal government agencies that are there and have the number of cleared personnel, predominant number of espionage cases are worked out of our Washington field office. However, in New York, we do have clear identities, we do have those who have access to information, and if that information is compromised, or those individuals are compromised, the FBI has sole jurisdiction on espionage related matters. That is one big portfolio for us in New York. |
|  | Another area we focus on is counter proliferation. Many of you are probably familiar with that term. For those of you that are not, when we have foreign adversaries, and I’ll name them for you here today, Russia, China, Iran, North Korea. Those are the preeminent country threats we are focused on when it comes to counter proliferation. Counter proliferation is simply a foreign adversary trying to obtain, procure, steal dual use technology. Technology here in the United States that is export controlled, and by obtaining that material, it can be used for a number of things. Our greatest concerns are that is used for military application, nuclear application, weapons of mass destruction, creation, facilitation. We have a number of investigations focused on adversaries trying to get their hands on that dual use technology. |
|  | Another area we’re working on right now, economic espionage. As we talk about espionage in classified material, we talk about economic espionage. I’m doing a record level of outreach in the private sector related to assisting companies, corporations, and organizations that have intellectual property that is being absconded by adversaries every day. It’s more of an economic threat, and we have a number of economic espionage investigations ongoing as we speak related to the outright theft of intellectual property. We’re not just talking about small companies or organization. Major corporations. |
|  | Now, how are the adversaries getting that information is probably a question that’s arising right now. Two ways, one through cyber intrusions, two through the cultivation of employees, and the ability of an employee, whether it be going to a competitor, or being cultivated by a foreign adversary whereby that material is then obtained through that relationship. It’s the FBI's responsibility, with some of the partners in Department of Commerce, homeland security whereby we partner up to prevent that theft, and to protect the economic sovereignty of many of these organizations that have this sensitive intellectual property throughout the United States, specifically in New York City. |
|  | It is the city of commerce, it’s also the city that is a target and will remain a target based on the level of intellectual property in the economic innovation that goes on in New York City and the surrounding area. We take that very seriously, we are doing a lot of outreach to educate the private sector and those organizations that have intellectual property on what the adversary is after, how they are targeting those organizations, and then more importantly, how they work with the FBI to prevent that theft? Why do I say that? Because when I show up at the door, I’m sure all of you can imagine that every CEO, COO, CFO, and every other acronym you have in an organization to include the security officer is ready, willing, and able to announce that the FBI is here, they’re here to help, only my IP has been stolen by a foreign adversary, and I don’t want it in the New York Times tomorrow morning. |
|  | Because frankly, their shareholders are not going to be very pleased with the fact that their IP just left the country, and now the FBI is there to try to get it back and investigate the theft. We spent an enormous amount of time working with the private sector and corporations to protect their intellectual property. Because in the end, we don’t want anybody out there to be a victim, and more importantly, I always say, “Look, the economic basis everything in New York City. If we don’t have that cutting edge technology, that innovation, people don’t have jobs, because the solvency of those organizations becomes at risk. That’s very, very important to us as an organization and protecting intellectual property. Again, historically, we would not do as much outreach as we’re doing now, but the level of threats related to cyber intrusions and the outright theft of that intellectual property is, I mean, it’s astronomical right now. It continues to happen every day. |
|  | The problem I’m trying to face is how do I get more companies to come forward and work with us on that? Because many of them will not risk the reputational damage in bringing that forward in lieu of just accepting the loss and moving on. The problem is, the adversary receives that message just as much as you do from keeping that quiet, and nine times out of 10, you’re going to be a victim again if you’ve been a victim once. I encourage anybody that is experiencing any type of intellectual property theft to contact the FBI. Contact me in support of working with you. Two things to remember on that which I think are very important. One, we don’t always have to prosecute. That’s one thing I want to make everybody aware of. |
|  | If there is a major theft within your organization, the goal is not always prosecution. It’s neutralization. Big term in counterintelligence. Because we learn how the adversary was able to get at your intellectual property, and sometimes that becomes more important than sending a message of a deterrent which would be prosecution. Be mindful of that out there as you are experiencing any type of theft, or are a victim of such activity. Finally I’ll close, and I’ll let Bill jump in here. The FBI in New York, it’s a 24 seven day a week job. I wish I could tell you, “Hey, I have doubled the agent pool that I do.” But we try to prioritize by country threats. What do I mean by that? We constantly are analyzing the level of activity. The threat. We apply our resources accordingly to those threats based on the level of activity. |
|  | One thing, and I’ll close with this, that we’re going through within the FBI, which has been a bit of a challenge for us, is we have a cyber division, and we have a counterintelligence division. Both looking at the same threat streams. The problem is once in a while, we never cross paths to share information, because they’re after hackers, and I’m after those who are carrying out intelligence related collection operations in New York City. However, as I said, the threat remains the same. While I was in my prior job, my job at FBI headquarters was to integrate cyber with counterintelligence. |
|  | Now, many of you that have done mergers, acquisitions, or brought two major entities together under the same roof, I’m sure that was a seamless exercise, and you had no bureaucracy associated with that. Well, let me tell you, in the federal government and the FBI, when you’re trying to merge two major divisions, there are some significant challenges to that. In the end, you just know that we are a lot better than we were post-9/11 in not only sharing information, but combating the threat, both from a cyber perspective, and from a counterintelligence perspective. If you have questions, and I’ll add a few notes as we go along here about specific cases that are in the public to give you better visibility on what we are doing from a counterintelligence mission here at the FBI in New York. Truly a pleasure to be with you today, and I look forward to your questions and your comments. Thank you. |
| William Evanina: | Good evening. Thank you, sir. It’s truly an honor to be here from Washington DC and spend some time with you tonight. I’m not hopeful, I’m sure we’re going to have a robust discussion and dialogue, and we are not going to hear your commentary. Because he’s got a magic button over there that can delete you. I think we’ll do that. Before I get into my role in what the government provides in terms of where my organization sits, and what the ODNI is, I just want to do two things real quick. Number one is, you’ve heard the old adage or proverb, it depends on where you sit. It depends on what seat you're in is your optic, your view. You’ve all heard that? And also you’ve heard of fake news. Well, I’m about to explain some fake news right now. You just heard my good friend and colleague, Charlie, talk about how great the New York office of the FBI is. That would be classified under fake news 101. My two perspectives on that, turn that mic off. Turn that mic off. |
| Charles McGonigal: | Go back to DC. |
| William Evanina: | I grew up as an FBI agent across the river in New Jersey. My working the real cases and the real subjects. All the targets were surely in New York City, but the bad actors lived in New Jersey. We had to do all the work, and they had all the credit. That’s one part of it. The other part of it is, I got the opportunity and pleasure to work alongside Charlie for many years in Washington DC where Charlie not only was the lead investigator, supervisor, and manager of some of the FBI’s biggest investigations in the last 15 years in the Washington field office and at headquarters. The Washington field office, and at headquarters. Charlie talks about he’s a good advocate and marketing member of the New York offices of the FBI, but if you’re a counterintelligence want to be and you want to work on intelligence, you have all the embassies in Washington DC. That’s where all the spies are. Why would you not want to work, as Charlie says, the number one mission is espionage, and that’s where the spies are. |
| Charles McGonigal: | Fake news. |
| William Evanina: | We’ll move on to be reality. Charlie brought a lot of good perspectives in terms of the FBI’s, I will say, very challenging mission, almost an impossible mission to help protect and defend, not only the United States, the government, the private sector, and what we do for a living. I’m also an FBI agent, so I am the fourth appointed national counterintelligence executive. My boss is the director of national intelligence, currently Dan Coats, former Senator, Dan Coats. Previously was director Klapper who works for the president. Part of this job, I’ve been in this job three years, I was head of the counterespionage group at the CIA. Then prior to that, I worked for Charlie in the Washington field office. Just to give you an assembly line from the FBI, to the CIA, to now, the national level, what we do in the national level, and my center is called the national counterintelligence security Center. |
|  | Our optic is to drive strategy, policy, guidance for counterintelligence security across the US government and the private sector. What does that mean? Every year, my shop authors the strategy, counterintelligence strategy in the United States of America. Signed by me, and it gets signed by the president of United States. That drives the strategy. The five pillars of what we’re going to do as a intelligence community to protect our nation. We tell people what we’re going to do. Then the FBI, CIA, NSA, and GA, they get that document and they determine how they’re going to do it. They are the implementator’s of that particular venue. How the FBI does it, CIA does overseas, and as it collects that process. We drive policy. Policy and how we do things in the government, with respect to clandestine operations. |
|  | I also want security, how do we do background investigations? How do we protect and defend our people, our buildings, and our data overseas in consults and embassies. It’s a pretty vast mission, but it’s at the strategy policy level. I spend a lot of my time with the White House and Congress just informing, educating, threat and warning to our policymakers and congressmen so they can go ahead and drive new legislation, or write new national level policies. It’s a unique position, and it was a challenged for me going from operations in the tactical, to the very strategic governmentwide mindset. It was a challenge. I’m not even there yet, but it’s been interesting dilemma for me to be moved beyond the tactical mindset, and be more strategic. |
|  | Also, some cool parts of my job, and also the [inaudible 00:21:10] the counterintelligence team for NATO. I spent a lot of time with our NATO brother and around the world quarterly, on [inaudible 00:21:18], we have conferences to drive some type of semblance of collective nests and oneness with our NATO partners. I’ll get into that in a second. As well as what we call the flyby partners. The US, Canada, Great Britain, New Zealand, and Australia. I chair what's called the counterintelligence and security panel across those five countries, and we meet once a month on [inaudible 00:21:40], or every other month in person, and we look at things, ideas, issues, problems, or threats that are [inaudible 00:21:47] to all of us, and how we work in them individually. What we end up doing is learning and showing best practices. |
|  | For instance, at the FBI has a really cool method or methodology on how they’re going to look at big data. Well, that can be shared across lines. The same thing of our New Zealand friends, find something that’s interesting. We have to share those venues. That’s pretty interesting. Now today, on the influence idea, I’m just going to give you a personal view of [inaudible 00:22:15] how it really impacted me. For years, when I was at the CIA, my first two years at my current job, I would be over NATO. |
|  | Whether it be in Brussels, or we would go in different countries, and I would always hear countries talking about the propaganda influence of the Russians. Whether it be the Polish, Lithuanians, the Latvians. Lithuanians, even sometimes the French, the Italians. I’d be glassy eyed, I’d be falling asleep, and I’m like, “If I hear propaganda one more time.” I had propaganda fatigue, because I had no optic or empathy for these countries who were bordering the country of Russia. Obviously, the last seven months, that's changed. That has come home. That is here. |
|  | Now, the last few times I was over there, I was wide awake, and everything made sense to me. I could tell you right now, when you look at our situation which we are dealing with right now with the propaganda influence campaign of the country Russia, what I could tell you is, the European partners, the folks who have been dealing with this for decades, decades, and there are countries out there who truly believe they’re on the verge of an invasion. Whether that’s true or not, it doesn’t matter. They believe it to be true. No different than our electoral process that just happened. Whether or not the Russians actually interfered in our election doesn’t matter, raise your hand if you think they did not. Even if they didn’t, it doesn’t matter. Because the narrative is created. We know for a fact that they did. |
|  | I have to explain this to my dad in Pennsylvania how this really works. What propaganda really means. It doesn’t make a difference. The reality is sometimes is what we believe and how we feel, and what we think. We’re all part of that as a country, as a media, organization, as government officials, as private citizens, as people that make our country go every day. What we do every day is try and find a way to not only combat the reality of propaganda and influence, but educate as well. I think tonight we are going to do our best to be able to provide an optic for you through your questions, and our answers, and our dialogue, and discussions about what we all can do collectively, where could we learn some skill sets? Where could we get some resources? |
|  | How to understand it better. What this really means. Because there’s a couple things in our lexicon that are confusing. Supply chain. Critical infrastructure. Hack. What is that actually happening. Propaganda influence. They’re all words that mean different things to different people. We’re going to try and get to the bottom of the little that today, talk about what it really means for you, and for your families, and for your coworkers where you work, and how that impacts it. Charlie talked little bit about Sieber, I just wanted to give you some numbers real quick. We [inaudible 00:25:10] last five years, looked at all of the theft of personally identifiable information. PII. Majority of it by one country, China. We looked at numbers. |
|  | Right now, over half of American adults have been victimized by theft of PII. Over half. That’s this whole half of the room right here. You, you just don’t know yet, it’ll happen soon. All of that theft of PII, for the [inaudible 00:25:36], to Anthem, to US airways, to American airways, to United airport restorations, to hotel reservations, we can go on, and on, and on. You’re [inaudible 00:25:47] under hacking. Hacking. I could tell you right now, it wasn’t by any sophisticated hacking mechanism by the Chinese government. 90 percent of all that theft, 90 percent occurred from one thing. You want to guess what it is? Spearfishing. |
|  | Our inability as humans to not click a link is incredible. Our adversaries know that. They can send us email, a hyperlink to a twitter account, or an email, and we will click that link. Then they’re in and they become a systems admin, and they can cipher off all that data. Some of the damage is self-inflicted, but until we do some of the controlling of the controllable’s, our adversaries will never have to get more sophisticated to impact or intrude on our systems or data. They can continue to send us emails with really cool dancing bears, and we'll click on it. Look forward to tonight. I think it’s going to be a great interview. Look forward to your questions, and it’s going to be a great opportunity for myself to partner with my old friend, Charlie, and Ted here, I think is going to be a great night. Thank you. |
| Theodore Roosevelt IV: | Both Bill and Charlie, the next follow-up question is, you talked about fishing. How hard it is, you get an email from somebody, “Oh, I know, that’s not Bill. I haven’t heard from Bill in a long time.” Or, “That’s my former girlfriend.” Or whatever it is. Then you click on the link that they send you. How do we actually verify it? What are the defensive mechanisms which are probably a pain in the neck, but what kind of defensive mechanisms, when you think that we should try to train ourselves, so we can’t eliminate it, but we will re-mitigate it or reduce it? |
| William Evanina: | Well, I’ll start real quick. Without endorsing any specific products. There is multiple products online you can get, you can download for free, or spend three, four, five bucks and buy better products to help you with preventing the spearfishing. What I do every day, and think about the optic of what you do every day. We’re in the same boat. All day long you get emails all day long with attachments. When we click on the attachments. Now, you go home, have to yell at your families, and then you look at your personal emails, and then what you have? Attachments. It’s become part of our culture nonstop. |
|  | What I’ve gotten myself to do, only because, not only the threats that we face every day as citizens, but in our role, we have little bit higher threat because we’re more of a target, I slow things down a little bit. I take my mouse and I hover over the email from Mr. Roosevelt, and it will say JohnSmith.RU. It’s a small little thing that takes a mega second, but it makes all the difference in the world. I try and categorize what the value is at, and I have a metrics to it, probably about 10 percent of my emails are bogus that I get right now. That’s all just by putting my mouse. Now, there are software that are out there they can get that will help you do that, and I have some of that, but for me, I’ve got myself in the habit of hover my mouse over the email and realizing if it’s really them or not. |
| Charles McGonigal: | A solid antivirus software will help you immensely. Also, take a hard look at the address at which you are receiving the email from first before you go to that attachment. This sounds very basic training of awareness and personnel becomes ever so important in the corporate sphere, or if you are out in any organization, training and awareness is everything. I don’t know how many times we walk into an organization, and you find that their training and awareness program of their personnel is pretty pathetic. If you have poor training and awareness as it relates to spearfishing, I can assure you, you will be a victim over and over again of some type of intrusion, release of malware, and you will be a victim. You may not even know you’re a victim for quite some time, which becomes a problem. |
|  | Strong antivirus software, and don’t think that it’s specific to your workstations or your laptop. You also have cell phones and mobile media you are carrying around. These things tend to pick up, depending on sites you are visiting, bits of malware that you can carry with you and transmit. It’s up to you, when you receive a link, to ensure you do your due diligence first before you contact security or ask the question, and then more importantly, in organizations, you have to train your personnel. That is the only way you’re going to prevent long-term and persistent threats to your network based on the Spearfish. |
| William Evanina: | I would just add on to Charlie’s great point there that some of the best things that we do in America and in the private sector are great for what we do every day. We don’t even see it, but it hurts us on the other side. For instance, data aggregation. The ability for you to turn on your Facebook and see an ad for 15 percent off your favorite store is because you’re just on Amazon. By the time you clicked on Amazon, it got in your Facebook, it got sold to Experian, Experian sold to Facebook in mega seconds. Well, that same capability is by our adversaries. They know where you go, they know what websites you go to, and they can buy that from Experian as well with a bogus company, and they could target you as well. Keep in mind, so let’s go back to the wiki leaks recently in [inaudible 00:31:19]. They put it out, and then New York Times had a link to it. We told our employees, “Do not click that link for two reasons, number one, you're going to now have access to classified documents”- |
| Charles McGonigal: | Which they do unfortunately. |
| William Evanina: | Right. And number two, there is a hyperlink in that link that identifies two wiki leaks who’s clicking on it. Then they have your email. That same, I call it, speed of business that we have in America, our adversaries have the same thing. Just like with our Internet of things, which is an amazing thing that we love every day, it’s also awesome for our adversaries. |
| Charles McGonigal: | I’m not going to go into a lot of detail, but I think it’s pertinent for this audience, be careful what antivirus you're using and where it’s from. I would also do a little research on any intrusion related activity that is publicly available on those antivirus software entities to see if, in fact, they have been a victim of an intrusion as well. |
| Theodore Roosevelt IV: | This is an audience that’s pretty sophisticated, they travel all over the world. Talk a little bit about how easy it is, unfortunately, for people to become compromised, and how strategic our adversaries are working to compromise people, even from a young age. I think just understanding what has happened. In some cases, particularly let’s say with the Russians. I don’t want to pick on them particularly. They’ve been doing this for generations, and now they have electronic tools that make them far more effective than they ever have been. They have a mindset that’s a little different than ours. Talk a little bit about that. |
| William Evanina: | I’ll start below macrolevel, and I’m sure Charlie could dig into the how. I’ll get a little bit more of the why. I’m going to bring this down to two things, electronic compromise, and human compromise. I will tell you, raise your hand if you don’t travel overseas. One person. Wow. Let’s just find out what their name is. When you travel overseas, I don’t care where it is. When you land, you turn your phone on, your phone is now the property of where you landed. Not just your phone, your emails, your texts, your database, your contacts is owned by them. Whether it’s the French, the Spanish, or the Russians, or Chinese. |
|  | Now if it’s Russians or Chinese, or, and you’re not going to land in [inaudible 00:33:42] obviously, but they own everything on your phone. Now, what they also can do is send you an email from that airport, from that location with a link, and guess what you do, you click on that link, right? Whether it be another Google like map program to get around Beijing, or in Saint Petersburg. When you click on that, now there’s malware in your phone. They have your phone forever. We come back to the states. |
|  | Remember, when you travel the seas, your phone is not connected to Verizon or AT&T anymore. It’s connecting to a foreign government, because they own and operate that. They own everything in your phone. All of your texts and your tweets, all of your emails. Second, when you travel overseas, and this is mostly for guys, and you go out, and you have a business meeting, and your marketing meeting, or your conference, and then you’re out having dinner and you’re at a bar, all of a sudden you become the best looking guy in the bar. If you aren’t good-looking here, you’re not good looking over there. Just remember that. If it’s too good to be true, it’s too good to be true. |
| Charles McGonigal: | On a tactical level, we deal with this every day. We have numerous personnel, both in the private sector and the federal government that are compromised as a matter of routine in foreign countries. You’re all aware of this, this is always made public. Look, if Russia can compromise its own Attorney General a few years ago with two prostitutes and a camera embedded somewhere outlying this activity, imagine what they can do to you as a business traveler going in there blindly with a laptop, a phone, and all the energy in the world to make a deal or to do business there. I caution everybody in traveling to Russia and China, just make sure you're doing your due diligence as it relates to your phone, your computers, or any other media you could be taking, because it will be compromised, and you will not know it. |
|  | Couple of specific stories. I don’t know if any of you have had this experience, but it is a telltale sign of compromise. If your cell phone is rather hot, or the temperature is high on your cell phone when you are in a foreign country, you can almost be rest assured that it is some form of a remote attack against that device. Just a point of clarification for you. That is one clear sign of a potential attack against your phone would be the temperature. We have seen numerous private sector entities, personnel, and also federal government employees compromise. |
|  | As Bill said, it’s as simple as starting a dialogue that leads to the development of a relationship that goes sideways quickly, and let’s just keep in mind the rule of law is not always one that is abided by in some of these countries where you’re traveling, and you should be readily aware of that. I’ll just cite the level of detainment of US persons in China right now is quite exorbitant, and it is a concern to the US government, it’s a concern to the FBI, and we're constantly giving defensive briefings on those traveling into those countries as to what they can expect. If you are a former government employee, or somebody that has worked in a capacity as a key business figure, you can rest assured they’re going to know who you are before you hit the ground, and you will be monitored while you are there. |
|  | Now, that is not meant to sound like, “Here’s Charlie from the FBI, and he’s naturally paranoid.” These are facts folks, and this is what we deal with day in and day out when we’re dealing with individuals traveling to these countries blindly and not getting a good defensive debriefing before they go out. I will offer it to you or your organizations. If you are interested in getting that type of counterintelligence briefing before you leave, or your employees leave, reach out to me. I am happy to give that. Because a little preparation on the front end is good for you on the back end, and it’s equally good for me on a resource standpoint at the FBI. Again, if there is a way we can help you, please let me know. |
| William Evanina: | Just a follow-up, if you have any pen or pencil, write this down. If not, think about it. NCSC.gov. NCSC.gov. The president Obama asked us a year ago to put together some training minuets for these type of issues subsequent to the OP and data breach, and we did. We have seven little videos on there that are three minutes or less. One of them has to do with foreign travel. Not only the technical collection of your cell phones, your iPads, your computers, the little safes in your hotel room which are not safe. Everyone in that town has that combination. It also talks about spearfishing, and there’s room for being, quote unquote, a [inaudible 00:38:42] to the conference overseas, what that looks like. They’re all good for adult learners. They’re all two minutes long. |
|  | The last one we just did, and it’s up on a website right now, were the top 10 travel advisories for counterintelligence. State Department of DHS puts out all these advisories from a terrorism perspective. Which countries are dangerous, you’re going to get blown up, or you’re going to get kidnapped. This is the first time we’ve actually gotten a communitywide consensus on top 10 things you need to know before you leave this country. The very first one is, do not take your personal phone or laptop. Do not take it. Why give it to some other country or foreign government? Then, if you’re on a business trip and you’re going to have your laptop with all your power points, and talking points, why give that up as well? |
|  | The question is, “Well, what do I do?” Well, you go to a company that probably has some, we call them, clean phones. Like what I do, I go to Walmart and I buy myself a nine dollar phone, I put in 10 phone numbers that I really need, here’s numbers to call, when I come back it cost me 22 bucks with my phone calls, and I know my cell phone is not compromised. Something to think about if you do not want to have your cells compromise. Also, Charlie talked about software, if you’ve traveled overseas multiple times last couple years, spend the time, get to a forensic specialist, or get some software to check your phone out. See if you have malware on it. Do yourself some due diligence. You might have malware, and it’s not just Russia and China. Think about that. |
| Theodore Roosevelt IV: | That’s pretty ominous. I’m leaving next week to go to China. |
| Charles McGonigal: | Call us when you get back, Ted. |
| Theodore Roosevelt IV: | That assumes I get back now after listening to him. Now, one of the questions, Charlie, this is more for you. You mentioned the Iran, China, Russia, and North Korea as being the one. Increasingly, we see the role as nonstate actors playing a role here. Some of that’s going to be counter terror, but a lot of them are trying to get clearly dual use technology. How much of that occupies your time, and how do we also be aware of that when we are here? |
| Charles McGonigal: | Yeah, let’s define that from more definitive standpoint. When we talk about nonstate actors, the way we refer to them as nontraditional collectors. Those individuals, and I’ll cite the 2010 FBI arrest of the Russian illegals. Those individuals had been in the country, some of them upwards of 20 years under an assumed identity collecting intelligence for the Russian government. We refer to that as a nontraditional collector. We also have, what we refer to as, agents of foreign governments who are corrupted by those governments and sent to the United States with the sole purpose of obtaining dual use technology, intellectual property, or carrying out whatever that government is tasking them to do through their research and development in the academic realm, the scientific realm, or the business and economic sectors. |
|  | To throw a statistic at you, there are 14 million transient visitors coming through JFK every year. In that 14 million, I can assure you, and the FBI is aware, that there are nontraditional collectors coming into the country for the sole purpose of collecting information and going after through targeting that dual use technology. We are very mindful of that, we do our best to screen that, keeping in mind the rights and privacy of individuals traveling into the United States. I’m not here to say every 14 millionth person is doing something nefarious in the United States, it’s our job, and you rely on us to make sure we are aware of those who are coming into the country, and we’re doing something about it to negate those activities without negatively impacting their stay in the New York area if, in fact, they are here as a visitor. Because we love visitors in New York City. It’s what the tourist industry is all about, it’s what makes us the city we are, and such a popular place for business and tourism. |
|  | In looking at that, the nontraditional collectors, I would say, are becoming more of a threat than the threat we have real time in New York City day in and day out. Identifying them becomes quite challenging for the FBI. We do that a number of ways. Information we receive from other federal government agencies, information we receive from our foreign partners who are aware of these individuals activities from being in their countries, and then we, again, take appropriate action to make sure that they’re not carrying out any intelligence related activities, any procurement activities, or any outright theft. |
| Theodore Roosevelt IV: | It’s interesting having both of you here, having one casework for the CIA, working. Both the 9/11 commission and Lawrence Wright, and there’s a book, The Looming Tower, we’re very critical about failures within the intelligence community to have lateral communication. I know a lot has been done. Talk to us a little bit about how effective you think the reforms have been to make that, and what are those things you really hope happen in the future to make it even better? Because we have specialization, but we’ve got to have more and more flows of information without compromising the intelligence that’s been gathered. |
| Charles McGonigal: | Yeah, it’s a great question. I’ll jump on that, Bill, if you don’t mind. In New York, it has to work. We have to share information in New York given the threat stream and the constant threat information that is coming into New York City. I will tell you, as the SAC for FBI in New York, I partner with every federal agency here in looking to share information. Not only that, if you've read the 9/11 commission report, it really didn’t touch much on sharing with our various foreign governments. In my realm, as I told you early on, historically that sharing of information with foreign governments was minimized. We were more of a nationalized agency that was focused on bank robberies, kidnappings, and things of that nature. Counterintelligence was eccentric to the United States and our borders, and keeping the Cold War adversaries at bay. No longer. We are now working globally with foreign partners, and sharing information. |
|  | I see that role expanding as we go forward. I’m meeting with government entities here in New York City from the UN that I would historically not have done business with as the FBI. I think that’s very, very good for us across the board. I think the more expansive we are in intelligence sharing, the better we will be equipped here to protect New York, the United States, and more importantly, share information to make sure our allies have timely information to combat the very same threats that we’re facing day in and day out. From that standpoint, our sharing of intelligence with foreign governments has expanded tenfold. I’ll say between the federal agencies, as I said, in New York it has to work. New York, in my opinion, and I’m a little bit biased, it is the example. I know Bill’s in love with Washington DC, that’s okay. |
|  | In New York, we are the example, we share information regularly. We cannot survive without that sharing going on. I rely on every federal agency here, and now, sort of a new thing for you, tonight, historically, our counterterrorism division would link up with NYPD. We’ve started initiatives on the counterintelligence side where we are now partnering with their intelligence apparatus to work together. That’s something that we really haven’t done well in the past, but we are now expanding into that role, and mirroring that counterterrorism model on the counterintelligence side, and were finding out some terrific information, because let’s think about it. NYPD has 40,000 strong out there. They are an army in New York City. They do a phenomenal job, they are a great organization, and they gather so much street-level intelligence that the FBI can benefit from and partner with them on, it’s a fascinating revelation for us, and something we’re going to capitalize on moving forward. |
| William Evanina: | Just to dove-tail what Charlie said, I think [inaudible 00:47:32] fake news, I think the idea that’s not shared is old news. [inaudible 00:47:38] honestly from that perspective, not only having [inaudible 00:47:41] at the CIA in charge of a couple hundred folks over there on espionage, but my job now, there’s really hardly anything that’s not shared, specifically analytically for sure, because there’s a lot of cross-fertilization of people, and the joint duty program, which is called, has really promulgated that. The ability to have FBI, CIA, NGA, NSA, [inaudible 00:48:06] folks working together, whether it be in a joint terrorism task force, or in a government organization. Really promulgates the information sharing with your own equities and authorities you bring. As well as, I think, the war zones. |
|  | The last 15 years. The ability to be in a war zone working alongside, sleeping alongside members from other agencies has really driven the need to share. As Charlie talked about it, you can’t not share. I think the being in the war in Afghanistan and Iraq has really proven that to be true. Where you could say, if you’re CIA case officer, why do we need that FBI out here? Or the DIA? When we work together in that close knit group 20 hours a day for months at a time, you realize different authorities, you really get to learn that. Then they come back to DC, New York, Los Angeles, become managers, then they’re already attuned to the critical need to share authorities, equities, resources, and mindsets. |
|  | I think that’s really I think what’s driven subsequent to 9/11 and commission report, WND commission report, because we were, prior to 9/11, independent [inaudible 00:49:08] entities. No doubt about that. No one will challenge that. Right now, I think at some points we’ve even gone a little bit further. If you look at that what [inaudible 00:49:16], 1.5 million documents, a lot of those documents were on shared sites that were available to a lot of different agencies. Some question, did we go overboard here? Which we didn’t change or mitigate, so the goods sharing has some potential pitfalls for it, but I think we’re as good now as we’re ever going to be, and I think we’re in the right place. |
| Theodore Roosevelt IV: | Both of you mentioned that we’re going to be under more pressure from voting. The Russians are going to do more of that. Does that suggest that maybe we should go back to the future and go to those old-fashioned machines were you move a big lever, that you have electronic voting, it’s going to be much easier to compromise. |
| Charles McGonigal: | You know, I’m going to answer this this way, and I try to rely on factual information in making decisions, and the FBI relies on us to do that day in and day out, and I want to stress to you that there’s been a lot of spin in the media. I realize the media has a job to do, I respect that, however, at the FBI, we have to rely on factual information. Here’s a fact, no voter machine was hacked during the election. That’s a fact. Before we jump the gun and start reinventing the wheel and turning our democratic process on its head, let’s deal in factual information in making decisions about the electoral process. |
|  | With that, and I take issue with this because there’s been so much of the fake news that’s been spinning, there’s been so much put out there about what we believe Russia did and what we didn’t. I could tell you this much, and this is confirmed by director Comey’s testimony, confirming with Department of Justice authorization that there is a counterintelligence investigation going on into that right now. I will stress to you, sitting here as the FBI representative in New York, we are looking for factual information to substantiate or negate the idea that there was an influenced campaign. We have to rely on that. You have to rely on that. You have to stand with us on that in support of getting to that truth, and that’s what we’re doing today in the FBI as it relates to this whole thing. To your question and to that point, fact. Not fiction, not speculation, not spin. That’s what we’re focused on right now and trying to get to the answer. |
| William Evanina: | Little bit of context for that, so I had the opportunity to be a part of the assessment we did for the intelligence community for the president with respect to the influence of the election, and I got to work with DHS and secretary Johnson on the actual voting machine issues. Some interesting reality to it all, not only were there no voting machines hacked, what we found out through the investigation is that, if someone wanted to, and they wanted to hack voting machines in New York City, all the precincts are not connected. |
|  | Theoretically, a high school kid, or now I would say 12-year-old kid, could hack a precinct in New York voting, but that’s all they’ll get. They’ll get those 1200 voters at that firehouse, and they was not connected everywhere else. Some of the archaicness of our electoral process, and we’re still like 1958-ish is actually going to help us down the road. Because of the all politics are local, that has an impact on how we vote. At the end of the day, looking towards our next presidential election, this will end up helping us because of the lack of connectivity. It’s one of the few things in the country right now that’s not connected, and it’s probably a good thing. |
| Charles McGonigal: | Correct me if I’m wrong, Bill, each state had a different system. There were multiple different systems out there. When you’re talking about that variety of voting systems and machines, it creates a very difficult time to carry out an intrusion on something when you don’t know the infrastructure and you have that varying degree of voting machines out there from state to state that are not connected. |
| Theodore Roosevelt IV: | Good, okay, well I’ve got one last question, that I’m going to turn over to the audience. Do you think that we have the right balance between surveillance and protection of our civil liberties? |
| William Evanina: | I’ll start off. I get this asked to me all the time in Congress, and depending on which way you look, left or right, the question comes in a different perspective. I’m going to say yes. I’m going to yield to how it’s manifested every day in investigations with Charlie. Everything I do I have three attorneys that are solely there to do privacy civil liberties with respect to policy and strategy, both on the counterintelligence and the security side. Because again, in a day, no matter what we do, we have to protect our civil liberties and privacies. The other side of the coin is, that can only go so far. Let me give you a vignette to this. |
|  | Last year, we came up with a policy that said, “As we do your background investigation, as we look to you to be a protector of the nation’s secrets, and we're going to bestow upon you the authority to maintain a top-secret clearance, we’re going to look at all your finances, we’re going to give you what’s called the financial anima. We’re going to know where you lived, who your roommates were, everything you possibly know. Now what we’ve added is the ability for the FBI to look at your public facing social media. Look at your Facebook front page, twitter front page.” Makes sense, right? How from, a smoke test, could we do somebody’s background investigation and not look at their public media? Not through the passwords, just what’s on the page. |
|  | Let me tell you, the privacy [inaudible 00:55:07] folks went bananas. They thought it was a complete invasion of privacy. It depends, again, where you sit. You have to ask yourself, is that an invasion of privacy to look at Bill Evinia's Facebook account if you want to give him a security clearance. As we move forward, every single step we make to secure our country, and provide some due diligence comes with a similar liberty and privacy issue. Snowden brought a lot of this to bare. Some of it’s good, some of it’s not so good. We’re working through it every day. In terms of the US government intelligence community, there’s not a decision we make that doesn’t involve civil liberties and privacy. |
| Charles McGonigal: | Yeah, absolutely right. The same way for us carrying out investigations. This is not taken lightly, it is not something we routinely do is run out and just initiate investigations on US persons without predication, without legal review, and to ensure that we meet the standards set by the Attorney General, the Department of Justice, and the FBI’s office at General Counsel. We take that seriously, and it’s not something I take lightly when we are evaluating whether to open a counterintelligence matter, and espionage matter, proliferation matter as matter of core. There is plenty of scrutiny, from a legal standpoint, to ensure that we are not violating anybody’s privacy. |
|  | When I’m out talking with the private sector, one thing that comes up as a matter of routine is what level of privacy, within your organization, are you comfortable with when you’re monitoring your employees? Because we stress all the time the insider threat. You’ve heard this ad nauseum. The insider's going to get you, he’s going to steal your IP, she’s going to take it out of the building. What level of privacy are you adhering to internally, or representing within your organizations to ensure you find a balance between security and privacy? |
|  | I don’t have a good answer for you, because your organizational cultures are going to dictate what your level of security and what level of monitoring you may be able to employ to protect your IP, or those keys to this kingdom, if you will, within your organization that keep you a solvent entity out there in the sector you’re operating in. Like I said, I’ve been in 1000 different companies and organizations related to security incidents, and that is probably one of the biggest, I think, or one of the most troubling things for companies is to developing that formula for privacy versus monitoring employee’s activities. |
| William Evanina: | Show of hands, how many people have responsibility, accountability, oversight and hiring personnel? A lot. I’m not asking for the answer, but think about, when you hire someone, do you check their social media? Our world is controlled by social media. Do you check it? Do you Google them? I could tell you, just last week, I had a little symposium like this with Fortune 100 companies, and some major universities and colleges. Two of them said, the University president and a major corporation, COO said, “We would never dare to do that. We would never do, that’s a complete invasion of privacy.” Wait a minute, you have major university and you’re a corporation? You’re going to hire this person? You’re going to pay them a lot of money, and you’re not going to check what’s on the front of their Facebook page? That’s a choice. It’s also a risk-based equation choice. |
| Theodore Roosevelt IV: | [inaudible 00:58:50]. All right, questions. Now, somebody has a question over there I know. Okay. It’s disappeared. Way in the back, yes? |
| Charles McGonigal: | Sir. |
| Theodore Roosevelt IV: | Guy way in the back with the man with glasses. Good. Come on up to the front so everybody can hear you. Okay, you got a microphone. All right. |
| Albert G.: | Albert [Goalson 00:59:10]. How does your organization, the FBI, specifically with the cyber division, how successful have they been in recruiting young people to work for your organizations, versus their choice to work for, let’s say, a company in Silicon Valley? What can you do better to increase that recruitment effort? |
| Charles McGonigal: | Well, I can ask you, the taxpayers, to be able to pay them higher, and that way I would be able to retain them. In all seriousness, you raise a very good question. One, we are dealing with in the FBI, as you can imagine, we have a lot of talented personnel in our cyber realm, and they’re often recruited to the private sector. It is very difficult to retain these individuals, because their talents, and obviously they’re very marketable. What we try to do is convince them that the experience they will get within the FBI in an investigative realm, and what they’re going to be learning about from foreign partners will aid them in eventually getting out into the private sector. As far as we've looked at retention bonuses, we’ve looked at a number of different things to include advanced education to try to get them to stay. That is something we’re battling within the FBI right now. |
| William Evanina: | I’m going to speak a little bit on the community perspective, because we’ve had a lot of conferences about this. I’ll go back to the FBI right now. Just little facts. Currently right now, the average entry age for an FBI agent is 30 years old. You have a 30-year-old individual who maybe is working in Silicon Valley in Texas, and St. Louis. However private sector job they currently have. They’ve [inaudible 01:00:47] for six months, and they’re asked to be assigned to go work for Charlie in New York City for $76,000 a year. And relocate the family here. G.S. [Tend 01:00:57], FBI agent, $76,000 to start in New York City. |
| Charles McGonigal: | And there’s a line out the door, I just wanted to let you know as well. |
| William Evanina: | That being said, in the community, it’s very similar. Whether you’re a CIA, NSA, and GA. let’s just make a difference. What we have in the community, the FBI, probably more than anybody, once we get them in, we own them for life. Because the mission is so strong, no one ever leaves. The hard part though is getting them in. Now, you add on the money issue with the millennial issue. What you’re saying to these individuals, “Hey, I know Mr. 28-year-old, [inaudible 01:01:34] broker here in New York City who’s making $240,000 a year. We get the fact that you take a big pay cut. |
|  | Also, you know that cell phone you live with in front of your face, you can’t bring it to work.” “What?” Now you made that to this 24-year-old analyst, 25-year-old analyst who just graduated Yale wants to come work for the FBI, CIA, you tell her, “No more cell phone at work 15 hours a day. Oh, and you got to take this big, intrusive background investigation.” It’s a tough problem. |
|  | Some of the things we talked about, the former DNI, and director Comey, and director [inaudible 01:02:08], hey, let’s look at holistically, give them the option to come in to the government and the FBI for five years, let them go back to private sector for two years. Then come back. Which right now is not possible. I think there’s some ways we’re [inaudible 01:02:19], but again, it’s a big ask, but once we get them in, we own them. Charlie’s point is valid, we have more applications now into the FBI than we’ve ever had. |
| Theodore Roosevelt IV: | Great. Right there. Gentlemen, you. |
| Victor Rudd: | Thank you very much. My name is Victor Rudd, I’m the foreign [inaudible 01:02:35] committee chairman of the Ukrainian American Bar Association. I can’t have two questions, so it’s one question with two parts. [inaudible 01:02:42]. One is very simply, what percentage of resources would you guess, and you may not want to answer these questions, I understand. What percentage of resources would you guess that Russia intelligence services attribute to traditional espionage, as compared to [inaudible 01:03:01]? The other question is, to what extent, you mentioned us sharing information with other countries, to what extent would you hazard a guess, either by quality or by quantity, UR allies feel comfortable or less comfortable in doing the opposite with us, particularly let’s say in the course of the last year, which would be [inaudible 01:03:23]? |
| William Evanina: | I’ll start real quick, and in the bigger part. We know for a fact that adversaries are sharing information. Specifically on the counterintelligence espionage angle. Let’s work for each other in the last couple years, and I’ll leave it at that. On the first part, we do have some quantifiable members on your first question, which we can’t get into here. We’re pretty aware of the effort that’s put forth by the Russian government, the FS[inaudible 01:03:46] and SVR, and what makes it more difficult now is the GRU and the SVR are very competitive. That competition breeds not a good story for us. |
| Charles McGonigal: | Yeah, sir, honestly I couldn’t give you a good percentage of that. I think, as Bill said, I’ve observed numbers. I just don’t know the veracity of those numbers, and I couldn’t give you a quantifiable number here in New York. |
| Male: | [inaudible 01:04:11]. |
| Theodore Roosevelt IV: | Okay, question way over to the left. Way left. |
| Male: | [inaudible 01:04:21] I’m just curious, having been started with the Comey bulletin, I’m just wondering what protection we have against President declaring a national emergency, and somehow transforming us from a democracy to a different type of country. |
| Male: | Isn’t that the same question that people asked Obama, and asked Clinton, and asked with Bush? |
| Charles McGonigal: | Yeah. Honestly, sir, I don’t know that I’m going to have a good answer for that. I appreciate the question, but I think that’s one I’m just not prepared to answer. I’m sorry. |
| William Evanina: | I have an answer. I’m really deep in my heart, I’m- |
| Charles McGonigal: | Folks didn’t hear the question over here. |
| Female: | We don’t hear the question. |
| William Evanina: | It’s probably better off. My answer to you sir is that deep in my heart, I’m hoping the news is fake news. I really deep in my heart hope that there’s something happened. |
| Theodore Roosevelt IV: | We have another lady, the lady in red, you get it. |
| Female: | Okay. I’m wondering, India is now progressing through an amazing experiment in a public revelation of identity, so they have 800 million of their citizens by a metrically identified, and with more than one biometric. They’re beginning to use this for virtual banking, and for voting. I wonder what you think of this. It’s an enormous experiment in the world to have this going on. |
| Charles McGonigal: | I don’t know much about that. I have heard the same thing. However, what goes on to my mind immediately is how are they protecting that data? Where is it being stored? And who would have access to it? |
| William Evanina: | My answer would be, I’m fully aware that, and they’re in a race with other countries, and the same capabilities. I’d expect that to be here soon, because at the end of the day, with our world, they’re trying to protect, and the date, US looks for speed, convenience, technology edge. I look for our companies very specifically in the financial sector to look into biometrics so we don’t have to take the little ATM cards. Warren’s starting to see pallets in that, so it’s probably not far from the US. |
| Charles McGonigal: | Ma’am, one other comment on that, Disney World. Disney is a huge biometric collector right now. You cannot go to that park without putting your print down to get in. |
| Female: | We pay to get the biometrics on our passports now we don’t have to stand in line. People would love to have biometrics on their computer so they’re not being hacked, but I’m just asking from a professional point of view. |
| Charles McGonigal: | I think we’re heading in that direction. Again, I always look at it from a security standpoint. I don’t know how comfortable we all are based on the level of intrusions and the PII that’s out there. Now they’re going to get your biometrics information, that, to me, is problematic. |
| William Evanina: | I will add on, so the questions about biometrics and what India is doing, and how they're collecting biometrics to do everything in India with respect to from commerce, to banking, to even grocery store shopping in India. We’re not far from that here. We’re almost there. Look at the data that’s collected on us as citizens. Credit cards, what Experian buys every day, billions of dollars worth, they sell what we do. Just think about what we do every day that we take for granted about how it’s collected. I’ll give you one example, Google maps. If people really knew how Google maps work, and how they get data, they would be really upset. |
|  | Could we live without Google maps? Probably not. The Google knows how fast you’re going, if it’s over the speed limit. My dad, poor dad, he says, “Let me tell you, it’s really cool. It goes from yellow, to red, to purple, automatically. I don’t know how they do that.” He thinks there’s a satellite in the sky. If my dad really knew, because he’s way far off, that that data is going from his phone in mega seconds, he would not be happy. He would write a letter to Rachel Maddow. |
| Theodore Roosevelt IV: | Okay, gentlemen in the [inaudible 01:08:39] black scarf around him. |
| Male: | [inaudible 01:08:42]. |
| Theodore Roosevelt IV: | Introduce yourself please. |
| Tarik: | Sorry? |
| Theodore Roosevelt IV: | Introduce yourself. |
| Tarik: | Tarik. I’m a student. Given that Facebook, Twitter, social media have been weaponized in this past election, this is more probably aligned with the DNI’s mandate, but the FBI probably also has an input. Do you have an action plan that’s ready to counter these measures by the time of the next election, and does this action plan include inoffensive strategy, as well as a defensive strategy? |
| William Evanina: | Yes and yes. |
| Theodore Roosevelt IV: | Way in the back, you’ve been patient. Gentleman. |
| Tullio Prieto: | All right, my name is Tullio Prieto, in view of the [inaudible 01:09:36] case, is Cuba among the list of adversaries? |
| William Evanina: | Absolutely. Charlie mentioned the top four, Cuba is in that top four. Just depending on the day and the subject matter. What makes Cuba more enticing now, obviously, the changes with Obama, the ability to travel there and become more targets. It’s not just the Cubans in Cuba right now. The Chinese and Russians have invested a lot of personnel collection capabilities in Cuba as well. Although this physical country of Cuba is so close to us, and the partnerships that have been created between Cuba and Russia for decades, now the Chinese makes it more and more difficult for us and a tough target. I think that’s probably in the top echelon of our threats right now at the global perspective, both [inaudible 01:10:29] and economically, but from a counterintelligence perspective, it’s being dealt with every day. |
| Charles McGonigal: | Very aggressive intelligence posture in New York City and throughout the globe. Also, one interesting thing that I’m always intrigued by with the Cuban intelligence services, they recruit spies based on strictly an ideology, not a financial vulnerability, which, in my mind, is quite impressive. Just goes to the level of sophistication that they utilized in recruiting their agents. |
| Theodore Roosevelt IV: | Interesting. Gentleman right here. |
| Male: | [inaudible 01:11:06]. It is with great pleasure to meet our two James Bond’s. They look as handsome as James bonds. Thing I wanted to say is this. We have touched mostly what they are doing to protect US in New York, that they do something also very interestingly, and is a big job switch they have realized up to now is that this city, for really 80 years has been the host of United Nations. One of the main functions, if not only being to protect the west side, but every US government these people had, and they had been very successful in protecting every year the heads of states of really 200 countries which visits this city, and comes to UN. I must say, I’m most grateful. |
|  | I work for 30 years for UN on a high level, and that’s why I can express our deepest gratitudes. Because when you look back, I don’t remember, not only myself, we don’t remember one single case which neither a head of states, or anybody [inaudible 01:12:59] subject of killing or anything. The other thing which I wanted to mention, that’s also important. When they do this protection, they can do it only until the frontier of UN, because legally, inside of UN doesn’t belong. They have to cooperate very much with the international security which we had at UN which belongs to different country. I suppose that this is a very important questions what they did, but we didn’t touch upon that. Don’t forget about the security question didn’t started in this country with 9/11, don’t forget that nearly for 40 years, this US, this country had the Cold War. With that Cold War, the protections were much more important as compared to now. Now, the two simple questions which I may ask if I may, I mean first of all- |
| Theodore Roosevelt IV: | Get to the question. |
| Male: | Yeah, to the question. I would propose, because I’ve been [inaudible 01:14:14] to comment on what I said. The two question is, when I was working at UN, and certainly we had them, at that time, I’m talking about 10 years back, we talked about the frontier scare about Canadian airport, and so on and so forth. I was told at that time, one of the weakest point is called for the New York was the frontiers with Canada. Because from the Canada, you can pass by the [inaudible 01:14:52]. Is that still? And my second question is that- |
| Theodore Roosevelt IV: | Let them answer the question. |
| Male: | Earlier, there was a kind of imposition to these European countries that are presented here, especially for the Soviet unions, not to go to [inaudible 01:15:09]. Thank you. |
| Charles McGonigal: | First of all, I’m not going to take credit for the UN General assembly’s security alone. The FBI participates in that, the UN plays a significant role, but I also want to complement the New York Police Department that does a phenomenal job in supporting that security, and the good citizens of New York who are always aware of those events as they’re going on in the city. All of those individuals deserve credit for that. On your question related to frontiers in Canada, all I can tell you is, we work very closely with the Canadian government in support of keeping the border safe, and from a counterintelligence standpoint, we’re partnered with both CSIS, and also the RCNP in combating any threats that come across this quarter. |
| Theodore Roosevelt IV: | Okay, thank you. That gentlemen raising his hand there. Right, you. |
| Male: | Thank you. Regarding your use of politically sensitive information you might acquire, how much is that use affected by the known political elections of, say, sessions and Trump. Tough question, I’m sorry. Curious. |
| William Evanina: | Well, let’s see. How do I answer this? I’ll answer it with one name. John Podesta. You want to know the impact of a successful Spearfish, and the ability of a nonstate actor to manipulate and affect things by putting emails out there? I think no matter who you are, what you are, whether you’re a political appointee, whether you’re a congressman, a senator, or someone in the White House, or you’re in an organization, or your private sector, you can potentially be victimized. I think what I’ve learned in the last year is that I know that everything I type in my email could one day be exposed. Makes me think of everything I type. |
| Charles McGonigal: | I think the nature of your question was how do we handle information when we receive politically sensitive information? Then how do we utilize that moving forward? Well, I can tell you from my perspective, if we do receive information like that, it is not openly disseminated within the organization. In the counterintelligence realm, we survive by the idea that you have a need to know in the organization, especially when it comes to classified information, or as you cite, politically sensitive information. We have a small team that reviews that. Obviously, all the way up to our director would be aware of that, and then we try to make sound decisions based on the information and what it entails. Is it a federal violation? Is it more from intelligent standpoint? Is it something that’s potentially compromising to that individual? It depends on the situation, and clearly, it depends on who it is. |
| Theodore Roosevelt IV: | Ma’am, the second row. |
| Adrian S.: | Yes, hi. I’m Adrian [Spoll-wart 01:18:08], and I come to these events all the time. It’s wonderful, thank you. Unlike this gentleman here, I’m not concerned about a military takeover, a dictatorship of our government, but what I’m concerned about are companies as large as Amazon, and Microsoft, and Google who have access to absolutely all of our data. What kinds of protections do we have against companies like that and their abusing that? |
| William Evanina: | Well, I think in terms of protections, obviously those are questions for Amazon and Google. I will tell you in the greatest capitalist country ever created in history of the world, I think that’s part of our success. Part of our capability for us to drive capitalism involves information flow, and their ability to take our information, whether it’s a magazine reorder. I think it’s a combination of our culture, but also our capitalist society that it has to breed upon that to drive economy. Now, from the government’s perspective, the FCC, and there’s regulators out there that have the ability to regulate the way they collect data and move data, and that’s what we have to hope for for a good government, and good business amount of practices, and good relationships between big government and big business. I think that’s going to have to continue to be the success that’s driven our country the last couple hundred years. |
| Theodore Roosevelt IV: | Good, gentlemen in the fourth row. Good. You. |
| Michael K.: | Thanks for coming out today. |
| Theodore Roosevelt IV: | Introduce yourself, please. |
| Michael K.: | My name is Michael [Ka-ta 01:19:52]. I actually work for the government. I’m part of ATNF. I don’t know if you’re familiar with that at all. Question not related as much to my job, although I’d love to talk about the recruitment thing later. Not by myself. [inaudible 01:20:10], not myself. It’s my friend, it’s my friend, I swear. It’s my friend. He lives in New York. He’s about six foot, brown hair. No, I think that’s a really interesting conversation, and would love to continue that later. This is separate, and it touches on a few key things that you discussed earlier which was Fortune 500 companies, nonprofit organizations, all these leaders who are traveling abroad. Folks who are doing this type of work. |
|  | I guess my question is, they can get exposed, they can be compromised. Is there such a thing as gross negligent treason where your behavior is so careless that it could be conceived as, well, how could you be so careless as to give this away? Because where do you draw that line on what is considered an active form of treason, versus what’s considered, you should have known better? |
| Charles McGonigal: | That’s a great question. I think we need to separate the question into the economic realm, and then the national security realm. If you are traveling with classified information without having it appropriately contained, and you are exposed. You can definitely be investigated for such activity, and potentially prosecuted. As far as economic data, I would turn that back on the entities in which the individuals employed, are first they permitted to be traveling with that type of information in that capacity, and that method, and then where they’re going with it, are they permitted to have that information? Are you permitted to get on the network and then remotely access back to your organization with that data on your laptop, or your phone, or wherever you’re storing it? |
|  | Again, it’s a very good question, but there are a thousand scenarios I could throw at you whereby then we would take a hard look at the activity and determine if there is any criminal culpability, or activity, or negligence, as you say. Generally, negligence falls in the realm of more administrative within the organization. When you’re talking classified information, or your talking theft of IP, that bounces you back into the criminal realm, which would be under FBI jurisdiction. |
| Theodore Roosevelt IV: | Gentleman that [inaudible 01:22:31]. |
| Male: | Hi. [inaudible 01:22:37] in private equity. I was wondering if you could please address economic espionage from friendly states. Particular that might be state sponsored economic espionage, and how you go about in dealing with your counterparts in trying to address that, mitigate it, and discourage that. |
| Charles McGonigal: | Yeah, it’s a great question. Many times it is from the countries that are obtaining IP. Again, a hundred different scenarios I could answer your question. The bottom line is, if we believe or we have reason to believe, or the fact pattern is that it is theft, the first question we have to ask is we look at the employee. Or is the employee, or the individual associated with that organization. Another question we ask is, what type of controls are in place to prevent that theft? Very, very important question when we’re talking about economic espionage. Then when we feel or reestablish, either through working with the organization that’s a victim, we make an assessment on whether how ready the country, whether it be a friendly or an adversary, is to the procurements of that specific information. |
|  | It’s a judgment call along the way as you investigate, and you let the fact pattern dictate if and when you would reach out to the friendly. Generally not the adversary, more the friendly then trying to coordinate. Now, if there is a third country involved whereby the individual may be transiting, if I could take your question in that direction, and we know that the individual is already out of the country, absolutely. We will be going to that third country to coordinate with that security service or that government in support of stopping that individual or that travel into a country where we believe we’ll be getting their hands on that intellectual property. |
| William Evanina: | I’ll take it a little bit more global, just something to think about to Charlie’s answer. Because we are the biggest country ever invented, we do a really good job here bifurcating the government, private sector, and the criminal element. We do a really good job of that for the most part. We slip sometimes, but for the most part we do. No other countries do that. Not even in Europe. When you travel over there, prior to the information trade data, and the states sponsored theft is helping the economic structure. |
|  | For instance, when there’s a meeting here in the US and we have businesses come from all over the globe, the FBI and CIA are not stealing the economic data to help the United States government. We just don’t do that. That’s not the case everywhere else. There's really no, not even a blurred line between state and equity. On thing that I’ll give you years and years ago, only because the ridiculousness of it makes sense. There’s a big acquisition measure between our country, and a prominent European country. We’re going back and forth, flying back and forth to negotiate this acquisition and merger, which turned into be a monster company we have now. |
|  | What that country did through its intelligence services were microphone all the seats on the airplane so they could hear all the conversations of their business people. Before they got there, they already knew the positions. That’s before they were able to do collecting of our electronic data. You take that and you put it with your cell phones, and iPads, and IT collection, it’s even worse now. That’s what happened 15, 20 years ago. Again, we are an amazing country, and it’s because we don’t do that. |
| Charles McGonigal: | Sir, did that answer your question? |
| Male: | It did, yes, thanks. |
| Charles McGonigal: | Alright. |
| Theodore Roosevelt IV: | Okay, ma’am? |
| Male: | The non-traveler. |
| MJ: | Hi everyone, my name is MJ, and I work at Barclays. My question is, besides worrying about the nonstate actors being the threat to organizations, how do you feel about organizations trusting third-party vendors with their systems these days? |
| Charles McGonigal: | That’s a terrific question. |
| MJ: | Thank you. |
| Charles McGonigal: | Yes, we all live in a world where we hire a lot of contractors. I will tell you point blank that we have had major issues with security breaches with vendors and contractors getting access to not only classified data in the federal government, but also to proprietary data in the private sector. It’s a risk. What type of vetting are you doing of the contracting entity you are accepting personnel from, and don’t tell me it’s the lowest bidder? Because if you do, you’re asking for it. I will tell you a story, and I won’t go into detail as to the organization. |
|  | I was called in at one point to give advice and guidance on a entity in the medical industry who had had, for the last 14 years, vendors handling a lot of their network security and activity rotating in and out. Now, when I asked for an accountant of those vendors and the contractors, they couldn’t provide it. I basically walked back out the door and I said, “When you can come up with a list, let us know, and we’ll try to help you.” A little due diligence on the front end goes a long way on the backend to your network security, and to the security of your information. There are hundreds of examples like that. It’s a natural risk. It depends and it goes back to many of you in that human resource element. You have a tough job. I don’t envy the position you're in. You have to do a lot of extreme vetting, and I think with that, you have to make sure you’re protecting your equities. I hope that answers your question. |
| William Evanina: | To add on, that number of the PII theft that we [inaudible 01:28:36], 60 percent of that was from the third-party vendor. From OPM, to Target, to Anthem. All those breaches came from a third party vendor. |
| Charles McGonigal: | The last part I’ll make on that, when you’re doing your due diligence, there is a lot of information online about vendors and contractors. Ask yourselves and look for data as it relates to any intrusion, breach, hack, or any issue with that entity in the past. If that is indeed the case, it should give you some indication, may be of their security posture as an organization, and then apply that to what you’re asking them to do in your organization. |
| Theodore Roosevelt IV: | [inaudible 01:29:15]. Two questions. This is going to be hard. I’m going to ask three people to give their questions in sequence, and then we'll take those. Gentleman there, gentleman there, and then gentleman there. Okay. Give questions very quickly. They’ll remember what they are. Then go to the next one and will have three questions at the end. |
| John George: | I’m John George from the United Nations foundation. Given the recent news around 545, does the FBI have a plan in place before something like this would happen to avoid any disruptions going forward in terms of intelligence? |
| Theodore Roosevelt IV: | Next question. |
| Mike Colt: | Hi, my name is Mike Colt, I’m a wealth manager with Beacon Trust in Morristown, New Jersey. You indicated that sometimes your objective is to neutralize these threats, as opposed to prosecuting them. Does that apply across the board outside of just the private sector, and why? Thank you for your service. |
| Theodore Roosevelt IV: | Pass your microphone to your right. |
| Male: | [inaudible 01:30:18], I am a grad student at [inaudible 01:30:20]. I have two questions, considering first that [inaudible 01:30:24] is going to be tried here in New York. How big of a threat is posed by transnational organized crime when it comes to counterintelligence? My second question is, while third-party information vendors pose vulnerabilities, we’re looking at a block chain in the future where there are no third-party vendors. That also poses less capacity of the state to monitor those transactions, get back to the people that are exploiting those types of opportunities. How is the government preparing for that? Thank you. |
| William Evanina: | I’ll start, and then Charlie [inaudible 01:31:03] get more details. It will go backwards. The transnational organized crime is a horrific problem were dealing with right now. It’s not anything new, but this administration has taken it head on. There’s three major councils and multi agency organizations working on it right now. It’s been probably in 30 percent of the presidential debriefs, and there’s been a lot of national products written towards the counterintelligence aspects that they have learned from major breaches that these organized crimes organizations have done. |
|  | I’ll leave it to Charlie, but on the FBI issue, you got to remember that majority of the FBI’s business is done in their 56 offices around the country. They operate regardless of who’s in charge in Washington DC for the most part. As Charlie can tell you in New York City, he has no idea what goes on in Washington, nor does he care. He will continue to do his business here, and that’s the value of the FBI is that it’s done at the lowest denominator of the hard work of the agents and analysts. |
| Charles McGonigal: | Yeah, to echo Bill’s comments, of course there is a continuing operations plan when we experience something like this. We experienced the same thing when director Mullah retired and moved on from his term. We had, like I said, Deputy Director, McCabe will stand in place most likely as the acting director until a new director is named by this president. Yes, nothing changes as far as our operational pace. Honestly, we’re expected to do this. We can’t tell the good citizens of New York our director is gone, we’re going to have to stop what we’re doing. It’s just not going to happen. It’s a great question, and one that just know the organization will continue to do what it does every day. |
| William Evanina: | I apologize sir, what was your question? |
| Mike Colt: | My question was, sometimes your objective is to neutralize these threats as opposed to prosecuting them. I’m wondering if that applies outside the private sector, and why. |
| Charles McGonigal: | Outside the private sector, meaning within the FBI? |
| Mike Colt: | For example, someone mentioned economic espionage. |
| Charles McGonigal: | Sure. In the case of economic espionage, that’s really one where you get into neutralize or prosecute. I’m not a big fan of neutralization. Even though that is a famous word in the counterintelligence realm. I like to just say we hit it head on, we combat it, we negate it, we eliminate it. With that, in the economic espionage realm, neutralization is effectively working with the company to come up with a reasonable solution. Now, the FBI is not a mitigator. We are not a mitigation service. |
|  | However, we will work closely with the organization’s executives to make a final decision based on taking into account how that organization sees itself post a disclosure. Because clearly, we can protect the idea that that intellectual prosperity has been stolen up to a certain point. Eventually, if we go into the criminal prosecution realm, there’s a good chance that it will be disclosed. If we decide not to go to the criminal prosecution realm, we may do a number of things. What might we do? |
|  | I’ll give you a perfect example. If we know who the culprits are, and they are already out of the country, we will do what we can to coordinate with a foreign government, or singularly with the FBI and some of our investigative partners in the intelligence community to try to lure those individuals back, and take action that way in lieu of some type of prosecution. We don’t always have to end a counterintelligence matter with a prosecution. I yield on that side only because, to me, that is the biggest deterrent. There are many instances whereby the FBI will simply neutralize a threat, or try to recruit the threat so that it gives us information that is of value moving forward about adversary intentions. I hope that answers your question. |
| Male: | [inaudible 01:34:58] Chairman Roosevelt [inaudible 01:35:00] ask one question. |
| Theodore Roosevelt IV: | All right. |
| Male: | Mic please. [inaudible 01:35:06]. |
| Theodore Roosevelt IV: | Okay, if you answer it very quickly. |
| Male: | [inaudible 01:35:15]. Would use distinctly describe in layperson’s terms the exact legal steps that are required for the United States government to initiate a surveillance of the United States domicile citizen? Layperson’s terms please. I’m not in a jury. |
| William Evanina: | I’m going to try it first, because it’s been a while since I’ve been a real FBI agent. I’m going to give the layman’s version which I would tell my dad. There is a real suspicion that you are working on behalf of the Russian government. Charlie’s shop, and agent has to go in and convince Charlie that that’s the case. They have to do paperwork to say, “Hey, we believe this individual might be working on behalf of the government.” Charlie then has to do a communication to his attorney’s office and say, “We believe this to be true.” Which allows the FBI to open up investigation. There’s four layers right there. |
|  | Then, to be able to survey you, basically survey you in a car, only Charlie has to authorize that. We want to collect your cell phone information, your metadata, who you're calling. They have to get a court order. It has to go from Charlie, to an attorney, to a judge. Who then authorizes the FBI to go to AT&T and find out who you're calling. Not only just who you're calling, who’s calling you. Then beyond that, if they want to see the data in that call, or they’re going to listen to calls, it’s got to go through that same process, and to a different court, which is called the Pfizer court to get that. All of those efforts, there’s probably seven layers of protection to ensure that you, as a US citizen, actually have predication by the FBI to ensure that it’s worth everyone in that chain their careers to okay your surveillance. |
| Charles McGonigal: | That’s a great answer, Bill. A couple of additional steps that add to this so that it’s not simply the FBI flipping the switch and saying, “Please monitor that gentleman. His phones, his emails, and everything else.” First of all, we have to meet the standard under Pfizer agent of a foreign power. That is not an easy standard to meet these days. Clearly, as Bill cited, we have to establish you specifically as an agent of a foreign power in some capacity, meaning you’re working on behalf of a foreign government carrying out some clandestine related activities. Again, a standard not easily met. |
|  | Once we establish that, we have to verify the facilities you’re utilizing are being used in furtherance of carrying out that clandestine activity. Once we have that verification and we can establish you as an agent of a foreign power, we will then coordinate with our FBI headquarters, the Department of Justice in support of putting together an application for a court order to then monitor those facilities with the hopes that we can capture foreign intelligence about your relationship and your activities, what that adversarial government. This is not something that happens overnight. We do have the ability, under exigent circumstances, which is a phrase you will routinely hear in the FBI and the Department of Justice whereby we feel there is an eminent threat to national security, whereby that process can be sped up. |
|  | Otherwise, it is a tedious process, and I don’t take that lightly, and we fact check everything we’re doing, and there are multiple layers of oversight, both within the FBI, and the Department of Justice before we’re able to exact that type of surveillance. To Bill’s point, physical surveillance, as long as the FBI has an investigation predicated, meaning it’s not simply, “I want to investigate this gentleman because he’s wearing a brown suit and a blue tie today.” It is, “We have some predication, a reason to believe he’s either engaged in intelligence activity, or he’s involved in criminal activity.” |
|  | At that point, I can initiate or predicate an investigation by writing a factual statement that predicates that investigation, and then from there, under that authority of that investigation, I am permitted to put physical surveillance on this gentleman in the front row, and that is simply, but not simply stated, agents in vehicles surveilling and watching what this person is doing with the hopes of what? Identifying that intelligence activity which then takes us to the statement we’re looking to predicate through that affidavit for a court order. All of the investigative activity is summarized in that application in support of such an aggressive technique. Remember, I want to leave you with this, the FBI prides itself on least intrusive techniques in establishing that. Least intrusive techniques. Very important. I take that seriously, and that’s not something we are flagrant with when it comes to determining, especially on the US person, that level of aggression. |
| Theodore Roosevelt IV: | Great. [inaudible 01:40:29] joining in on thanking our two panelists for just an excellent presentation. They were very nice. |
| William Evanina: | Thank you. On behalf of the college, I’d like to thank the Foreign Policy Association for bringing this conversation to us tonight. Again, thank our panelists and Mr. Roosevelt for a wonderful conversation. |