EPISODE 487

[INTRODUCTION]

[00:00:00] AH: Welcome to this week's episode of SpyCast. This week's guest is Michael Orlando. Michael is the acting director at the NCSC, the National Counterintelligence Security Center. So this is one of the three centers at the Office of the Director of National Intelligence. Mike spent his career in the Federal Bureau of Investigation working the counterterrorism and counterintelligence beats, including – Now, listen to this for an interesting job, Assistant Special Agent in Charge of the Washington Field Office, counterintelligence division. This is the first in a series of podcasts that are going to touch upon the topic of cyber. I'm calling it Cyber August. I know that it's meant to be Cyber October, but here at the Spy Museum, we like to be a little bit different.

This episode is brought to you by Rise. A science-based app that makes it easy to improve your sleep to increase your daily energy. Are you tired of pseudoscientific techniques that over ensure that you'll be pounding the vending machine at three o'clock in the afternoon for candy? Are you tired of hitting up Starbucks for a venti, mochadoca frappudopaccino to try to get you through the rest of the day? If so, time to Rise. It uses a scientific, fact-based approach to help you get the sleep your body needs. It's built around the two core principles that sleep researchers agree most affect how we feel and perform, sleep debt and circadian rhythm. Go to risescience.com/spycast and download the Rise app today to try it free for seven days.

[INTERVIEW]

[00:01:49] AH: So I guess the first question would be of all of the multiple things that you're dealing with as the acting director for the National Counterintelligence and Security Center, what are the things that most concern you?

[00:02:02] MO: Andrew, first, thanks for having me on. Great opportunity to talk about the National Counterintelligence and Security Center, NCSC. What really keeps me up at night is the threat from China, the Chinese government. I am concerned the American people and our allies do not really understand the threat. And if we don't get somebody to understand the

threat, it may be too late by the time they do. There's a lot at risk to our democracy. Just not the theft of government information or our technologies on our IP, but our way of life. The Chinese government definitely would like to challenge us and our ideals of freedom. And I think it's important. It as a whole of society problem that we really need to work together on not just as Americans, but with our allies as well, because we're all in this environment. So that's really what causes me concern is and making sure people have that awareness that we can kind of work together on this important issue.

[00:02:51] AH: And just to pick up on that point, what is the threat? What is the nature of the threat that you would like the American people and allies to understand?

[00:03:00] MO: If you just look at the public messaging from the Chinese government, particularly Xi Jingping, he has no interest of having a win-win relationship with democracies. He sees China as leading the world and having an authoritarian view. And he's going to do that through acquiring our technology and our research through any legal means. I think people just don't understand that it isn't really a win-win relationship. And when you look at those plans that he is laid out, whether it's made in China 2025, or his ambitions for China to arrive in 2049 as the ultimate superpower, our interests aren't really being taken into an account.

[00:03:36] AH: And do you see the nature of that threat as being driven mainly by ideology, like communist ideology? Or is it more old-fashioned great power politics, or is it something else?

[00:03:49] MO: For Xi Jinping, it is the survival of the Communist Party. And he realizes that China is a rising power. And part of that technology and technology acquisition will really be the currency of governments of who will be the superpower. And he's really trying to take advantage of that. And unfortunately, if he had a democratic view, I think that would all be okay that China rises. But he sees it as it's all about the survival and that authoritarian view and cutting apart democracy helps with the survival of that party.

[00:04:19] AH: What are the main focuses of that threat? Are we talking economic espionage? Industrial espionage? Intellectual property? All of the above?

[00:04:27] MO: So it's all the above. 20 years ago, we were mostly concerned about the theft of government information or classified information. And over time, it has evolved into not just the theft of that information, but our economic IP and trade. And it's also been done very illicitly for a number of years. And then with the birth of cyber, it made it a lot more easier to acquire information through cyber theft. But also what's concerning me now is there's a number of legal ways that they are going about acquiring our technology by acquisition and mergers or joint ventures that force companies to give their technology over. And so that is particularly concerning when you get into like the emerging technologies of AI and bio technologies that really will drive who the superpowers are. And so they're using a whole host of tools to do that through illicit using their intelligence services, cyber espionage, and then just illegal acquisition, mergers and taking advantage of talent programs as well.

[00:05:23] AH: I guess just to get up to 30,000 feet, what is the NCSC? So for people that are out there, some of them are familiar with the CIA, the FBI. But what is the NCSC? Where does it come from? What's its role? And what is it you're doing?

[00:05:40] MO: So NCSC is a center under the Office of the Director of National Intelligence. The Director of National Intelligence is the president's cabinet level official for intelligence. And we are one component of her office that covers counterintelligence and security, and our main role is to integrate the counterintelligence and security community and work with national policy and help set strategy. We will also have a role in outreach to US government, private sector, and others to educate people on the threats from foreign intelligence services and to offer them some mitigation.

Then our third part is we're responsible to do public warnings when there is a threat. For instance, during the election, my predecessor, beloved Nina, was on TV talking a lot about foreign influence. From an evolution standpoint, the genesis of the center goes all the way back to 1994. President Bill Clinton had signed a presidential directive. This came out of the author Aldrich Ames espionage case. He felt that FBI and CIA needed to cooperate more fully. And so he had directed that they do an exchange of officers and that a counterintelligence center be built, and that they would be a policy board to talk about differences and priorities. And then he issued a second presidential directive in 2001. In the turn of the century, he believed that the counterintelligence workforce needed to get together for the evolving threats. And at that point,

he started our predecessor organization, the National Counterintelligence Executive, and an office to go along with that, which would, again, do the integration function of the mission, private sector outreach.

And then in 2002, congress solidify that all into law. And then over time, we brought together not just a counterintelligence, but the security functions of our Special Security Center and our Center for Security Evaluation were merged in. And for your listeners, our special security center, to security clearance reform, the DNI herself is the security executive agent for the US government. She's responsible for making sure we protect our secure facilities, our classified information. And that center was essentially her staff that is now part of NCSC. And the main issue we work on there is security clearance reform and securing those facilities.

And then for the Center for Security Evaluation, that center goes back 30 years. It's not very well known. But that came out of the fallout from the US Embassy being built in Moscow when we discovered the Russians had penetrated with all sorts of listening devices. And congress had felt that there needed to be an entity that integrated the intelligence community to view to help consult the Department of State. And that's what that center does. And that center still exists today. And they work in partnership with the intelligence community, the Department of State, private sector, and academics to research ways that our adversaries can compromise or sensitive information overseas. And then they take those lessons learned and bring them back for our facilities here. And then lastly, in 2018, congress decided that the director of NCSC should be a presidential appointee. That is confirmed by the Senate, essentially making that official the head of counterintelligence for the US government as the chief adviser to the DNI and the president.

[00:08:49] AH: And one of the things that I was interested in when you were speaking there was, with counter intelligence, we had Frank Figliuzzi not long ago, former Assistant Director for Counterintelligence at the FBI, and he was talking about how that position at the FBI is responsible for counterintelligence across the US government. But that's more at the applied operational level, whereas you're more dealing with policy. Help our listeners understand like what's your day-to-day with the current holder of that position? Or how does it all kind of shake out?

[00:09:24] MO: Yeah, that's a great question. The director of NCSC, we're more strategy and policy. We integrate people. We don't have operational or investigative authorities. The FBI has special agents that investigate. Our CIA colleagues have officers who collect information overseas. We don't do any of that. We were able to bring people together to talk about issues and do policy. For instance, we're responsible to do a national threat assessment. We do that in partnership with the IC agencies, FBI, CIA, DoD. And then once we identify the threats, we then do a national strategy in partnership with the FBI, CIA and DoD so that the community has an agreed upon strategy and priorities to work on.

And then on tough issues, we corral the community to talk about those issues. So over the years with China, we've helped bring the community together. So for instance, a few years ago, we had found a potential vulnerability in our information infrastructure. We were able to bring the community together. They use their own authorities and capabilities to address that problem.

Recently, some of your listeners may be aware of the anomalous health incidents where some of our officers have become ill overseas. We play an integration role. We help the community integrate information, and they use their authorities to investigate and work on those issues there. But specifically to your question is like what is the difference between the FBI counterintelligence assistant director and my role here. I'm more of that integrator policy adviser to the DNI, where the FBI is responsible for the investigations and operations domestically. He is the chief spy catcher. And the FBI is really the lead counterintelligence agency domestically, which is able to bring the investigative components from the military and others to work together here domestically using those authorities there. And our relationship is we talk weekly, where we partner with each other and make sure we understand how we can help each other out. And I would say it's similar with CIA and our DoD partners as well. My role is really to be a facilitator, augment their efforts, fill gaps for them, partner with them and facilitate them.

[00:11:26] AH: To me, it sounds like one of those jobs where I just have this scene. It's a Sunday afternoon. The chicken in as setting out to rest. You smell the roast potatoes, and then the phone goes or someone comes to the door and you're just thinking to yourself, “Oh, my goodness! What the heck is it now?” Is that how it is for you?

[00:11:51] MO: Well, that's probably how it is for my partner at the FBI, because he owns the risk. I'm more policy and strategy. When I walk in on Monday morning is where when I find what the concerning issues are there. So I would say he has the harder job.

[00:12:06] AH: Who are some of your main interlocutors in the US government? So you mentioned the CIA, the FBI assistant director, and then upwards. I'm assuming you report directly to the Director of National Intelligence. Help us understand the kind of network that you're involved in on a daily or weekly basis.

[00:12:25] MO: It's a fairly robust network given everything that we do at the center. So I report to the DNI herself. And then I have frequently on the counterintelligence side with FBI, CIA, all the military components, from Air Force, OSI to Navy Criminal Investigative Service, the Army Investigative Services, NSA as well. But we also have a security mission as well. And so I have relationships on the security side with all those agencies. But we also do a lot with federal partners and trying to educate them insider threat. Helping them build programs, educating them on CI. So we also talk to what we call the non-title 50 organizations, from commerce, FAA. And so frequently be able to engage with those as well. And then congress certainly has a lot of interest in what we are doing. And so there's meetings and briefings with them as well. And then certainly, I have a lot of – Given our outreach role talking to the private sector and industries about the threats that they face.

[00:13:19] AH: It sounds like a really intellectually stimulating and rewarding position, because you're seeing across the whole sort of spectrum of the US government and you're trying to get people to sort of work together and talk to each other and make things happen. Is that how you find that?

[00:13:37] MO: That's exactly right. I operate at a very high level. I don't get to see what the cases are. But I understand the broader trends, and then help bring those partners together on areas where there needs to be partnership to help them collaborate or provide resources for them to do it. So it is a very fascinating and interesting job. You have to be right on many, many issues, not just counterintelligence, but security and insider threat. And then the new issue is supply chain risk management as well. So it's very diverse topics that I cover every day.

[00:14:06] AH: Really broad spectrum of issues and threats involved here. And to what extent are you working with traditional counterintelligence and to what extent as something new? Or is it just the area or the domain that's new? So cyber is new, quantum is new, but as the same techniques. Help our listeners understand that. A lot of them will be people that have read all the kind of classic counterintelligence books from the cold war and stuff, but help us understand the kind of world that you're looking at on at the moment.

[00:14:41] MO: I cover a range of issues. And so I will go from one meeting talking about risks to our supply chain, and then going over to another issue such as anomalous health issues. But broadly, we do still deal with a lot of traditional counterintelligence issues. We have two dedicated directorates that do counterintelligence and support to the community. And most of what they focus on are the priority issues that percolate up that are hard problems to solve. And that's where they engage to help try to provide resources or expertise on those matters there.

But essentially, the agency is using though their own authorities and us helping them integrate on those issues to move forward on those things to solve those problems, because if they could just do it by themselves, we just wouldn't be needed. And just going back to 2001 where President Clinton saw the need for that integration, it's certainly has played out in the last 20 years, is that the environment of counterintelligence has become so complex from the traditional espionage, to economic espionage, to the various vectors that come to us from cyber, human and technical. It has certainly become a very challenging area than where it was maybe 20, 30 years ago, right?

My predecessors who probably worked the Soviets, they had to track down the traditional intelligence officer, maybe that the non-official cover. Well, the environment has changed where we still have the traditional threats. But now we have a whole host of asymmetric threats that we're trying to run down with the same size workforce that we had 20 years ago.

[00:16:11] AH: That’s fascinating. You have these like one page bulletins, fact sheets on the topic of safeguarding our future. And one of them that I read was on quantum. So just on what you were seeing there, is there an extent to which, say, the FBI’s institutional history or the way that agents are trained as though really a continuation of that kind of Cold War traditional, the Americans **[inaudible 00:16:40]** now chasing people around Washington? Is there still some of

that kind of like mindset or culture? I mean, just thinking about this fact sheet on quantum, like if it was me I'll be like, "I'm an FBI agent, and then someone's talking about bloomin' quantum." Like what the heck is going on here? I mean, there're a lot to get up to speed with and a lot of things to get your head around. I mean, it sounds super challenging. I hope they're paying you very well.

[00:17:08] MO: And I think that's why the people who like working counterintelligence really like it, because it's challenging. It's very different than any other threat that you're involved in. I would say comparing the cases that I was involved in or got briefed in in counterintelligence versus counterterrorism, the counterintelligence cases are far more interesting and challenging. And I would say my peers who worked counterterrorism who went over to counterintelligence feel the same way, is very diverse. One day you are trying to understand that traditional threat of Russian intelligence officers who were maybe stationed here in the embassy. And then the next day, you're trying to understand, as you said, the quantum threat and how Chinese and others are trying to require that using asymmetric threats.

But I do think you talked about our publications. I think our publications have done a lot to help put a spotlight on these issues. I've helped the community bring resources and solutions to it, because we simply can't kind of disrupt our way out of these problems. We're not going to arrest everyone who's done this. We need the whole of society to understand some of these to better – I would say we need to build resiliency into the system where companies who are involved in quantum or other things that are important are defending themselves, while at the same time we're trying to disrupt those bad actors.

[00:18:19] AH: I'm wondering as well, like with the changing nature of counterintelligence and the various threats that you face, say, for the FBI, where you come from, is there any **[inaudible 00:18:30]** doing counterterrorism for one pause and doing law enforcement and then going back to counter intelligence? Or is counter intelligence just becomes so specialized that it's actually product differentiation? Or it's like a football player, say soccer, where I'm from, get people that are good at defending, people that are good at attacking, and people that are good at linking up, but it's very difficult to be all three. So I wonder if you had any thoughts on that, the skill set that's necessary to deal with the challenges that are coming over the horizon.

[00:19:04] MO: So it's a little bit of all that. Particularly the FBI when you're special agent, you've got a lot to learn the core skills of being an investigator from how to do all those things. And whether you work criminal investigative matters, or counterterrorism, or counterintelligence, there are some baseline there. But when you move into the counterintelligence workplace, there are other things that they do there from offensive operations, from trying to disrupt them, through recruitments and other operations, to arresting people in those cases are a little bit more challenging then, I would say, your criminal investigation. Because the standards of proof that you have to show and the protection of classified material and going about that creates a number of challenges.

But I think what we have found is having a diverse workforce. Those who have been career long CI professionals who understand the threats is very helpful. But also being able to bring in investigators from criminal investigations or CT who have a different mindset to look at the problem from a different perspective is also helpful as well. And so it's the blending of all that that I think is what's really needed right now. But also understanding that we do need to arrest people when needed and recruit sources that can help us. But we also have to be much better in the partnership with the private sector to get them to educate them to become better ways of defending themselves, because we're simply not going to be able to do it all ourselves and to the extent they can protect themselves will I think go a long way.

[00:20:27] AH: You were talking about the whole of society there. And this made me think about one of the analogies that I've kind of come up with in my head. And tell me if you agree with this. To me, cyber has done for espionage, what airplanes did for warfare, because until the invention of the airplane, people behind the front lines weren't on the front lines, but then there was the possibility for them to be. In with espionage, with cyber, I've got an iPhone in my pocket right now. We're carrying around these devices that are just emitting information, and knowledge, and so forth. So it seems to me that everybody in this country, or across the world, like everybody's on the front lines of this now and seeing the United States. How do you get 360 plus million people to kind of be those cyber citizens that are kind of doing what they need to do so that the whole of society approach works?

[00:21:29] MO: I think the recent ransomware or cyber attacks were helping us get there, unfortunately. And to your point, I do think cyber has transformed counterintelligence

environment. And we had done a publication back in 2011 about how China was using cyber to collect economic information, which really put a spotlight for the first time on them. And I was reading that document the other day. And it was really insightful that everything that those authors wrote 10 years ago is all true today. That cyber is this really low-risk operation that gives them a high payoff, very difficult to defend against. And so we have to work on that. But the other threats haven't gotten away. So we're now we're spreading our workforce a little bit on these diverse threats. And if we're not able to build better security into cyber, it's going to be very difficult to kind of defend against this threat. And so we need everyone who's involved in that to understand that, share information. Making sure we're building secure software, and using good tradecraft for people who are involved in intelligence to make sure that we're protecting ourselves. Things have transformed. And I think the intelligence community has kind of got their head around that and in working on those solutions to operate in the environment that we're now and that we weren't in 20 years ago.

[00:22:44] AH: Let's talk a little bit more about the outreach role that you've spoken about. So tell us a little bit more about – You mentioned academia, tech companies, and so forth. What kind of work is the NCSC doing on that front?

[00:22:57] MO: So as I mentioned earlier, part of the law is for us to go out and do outreach. We're a very small center. So we're not able to go out all over the country. So we try to stay focused. We do a number of things. We do a number of unclassified briefings. We have the ability to bring in the private sector to do classified briefings. We often times partner with the FBI, or DHS and others, to amplify their message and assist them as well. But we want the FBI and DHS to be the ones that the companies come to. We're a more of a higher level message to get the message out there for everyone.

And over the last two years, we've done about 300 outreach events, reaching 40,000 executive. Working in partnerships with Chamber of Commerce, academia, and others to really try to get high-level messages out there to the audience. And we also do some publications as well. And then moving out into the future, we're trying to get a little bit more focus on what we deem are the real threats that we think we need to put a spotlight on, which we call the emerging technologies.

[00:23:56] AH: And could you tell us a little bit more about some of those emerging technologies, some of those threats? Again, I looked at some of your literature, and there's a really diverse range from deep fakes, to social media deception, to quantum. There's a lot of going on there. Help us understand some of those threats.

[00:24:15] MO: There's a lot of threat. And when we do some analysis on it, when you look at these emerging technologies, what we view as artificial intelligence, quantum computing, autonomous systems, biotechnology, semiconductors as that building block. When you look at those technologies, they will have a drastic impact on both our economy and our national security. And so it is extremely important that we remain the leaders in these industries. Because if we don't, it will give China or others the ability to eclipse us as a superpower.

And although these technologies can bring great things to us, there's also a bad side to these things as well. And we have to make sure that we defend against those bad things. But also, in being a leader in this, we also know that the Chinese and Russian want to be leaders in as well, and they will try to steal our information as they've done other things. And so we want to make sure that we're bringing awareness to everyone that yes, this is important, we have to protect ourselves as well.

[00:25:11] AH: But it sounds a little bit to me, like, in some respects, the NCSC is doing think tank type work. It's thinking about the different things that are going on. And it's trying to find synergies and points of comparison and points of difference and so forth. Is that a kind of fair statement partly? Or am I kind of off the mark?

[00:25:32] MO: Partly. We don't do a lot of in-house analysis. We find the experts in the community, and then corral them together or pick their brain to find out where they think those things are. And then we amplify it from there. For instance, in bio technology, bio economies, we have partnered with the FBI who has an agent who's really an expert in those things. And we've learned a lot about how the Chinese are trying to take our genomic data, both legally and illegally, and gotten that message out to really kind of get attention on that specific issue.

[00:26:02] AH: And one of the things that I love about our podcast is that the people that listen to it can range from the people that are working these issues and the IC to your average person

on the street who likes a good spy story, or who wants to learn about intelligence and espionage. So just so we're not leaving anybody behind, could you just really briefly tell us what quantum is and what bio economics is?

[00:26:28] MO: Great question.

[00:26:31] AH: I just don't want to leave anyone behind.

[00:26:32] MO: So when we get into quantum, it's really about speed of computing. And whoever has that advantage will be able to break encryption, right? And if you don't have quantum, you won't be able to protect your information. So it's extremely important that you have that edge. When you get into bio economies and biotechnology, think about precision medicine. If I'm able to get your DNA, I could analyze it and determine that you may have a history of cancer in your family. And we may be able to give you precision medicine to make sure that that doesn't develop or to cure you. That side also has a nefarious side to it as well, is that I can create a toxin that only attacks you, or **[inaudible 00:27:08]** you. And so that's what those topics are really about. And the particular issue with biotechnology, if you get into the DNA and the acquiring of that.

A concerning part is the Chinese to legal means. Hospitals have partnered with them to acquire the DNA to do low-cost genomic sequencing, which is nothing really wrong with that. It's a low-cost model. But China has acquired a lot of our DNA through this process. And that information is not necessarily going to be shared with us. And that diverse data they have will help them with artificial intelligence and other things. And we've known that the Chinese government has used DNA surveillance on the leakers in the western provinces of China. And we find that all concerning. And if you're an intelligence professional, if you think about all the data breaches we've had from OPM, to others, and your DNA tests being had, there's a lot of information that the Chinese government has on our intelligence professionals.

[00:27:59] AH: And quantum, that refers to the speed of computing?

[00:28:02] MO: Speed of computing, the ability to break encryption, maintain encryption.

[00:28:06] AH: So we're talking like with quantum, there would be a computer powerful enough to go through every possible permutation of password so that you could break it down?

[00:28:17] MO: Correct.

[00:28:18] AH: Okay. For John and Jane Q. public out there, they need to worry? Is their genomic data now setting and communist party database somewhere? Yeah, help us understand the scale and scope of the threat.

[00:28:35] MO: So for the ordinary citizen, I think they need to be concerned, because this isn't just an issue for national security or our intelligence professionals. If China or others become the leaders in bio economies or others, those are American jobs as well. So it will impact our economy. It's a two-headed issue. And then from just a national security matter, there's a recent article about how BGI, a Chinese company, acquired, did some testing, and then shared that data with the People's Liberation Army for their own testing. And so I'm just not sure people want their data, their DNA used and these sort of things, or doesn't have that transparency. I'd also say that the future president of the United States is out there. And they have that person's DNA and information. And that's concerning.

[00:29:19] AH: One of the questions that I find quite interesting to ask people like yourself is how do you keep your head above water? Like how do you not just throw your arms up and disappear and open up the liquor cabinet and start pounding the scotch when you're doing this? Like how do you be focused and optimistic? And yeah, there is a better future to come when you're dealing with all of this rather market stuff.

[00:29:45] MO: So when you're a career – An FBI professional or an intelligence community, you're used to dealing with problems all the time. Everything you're working on is a challenge. So you get accustomed to that. But the real key is teamwork. We have a fantastic team at NCSC where we're able to share that burden. And I would say that has been my experience at the FBI that I've always worked with a fantastic team. And you're able to work as a team to kind of share that burden and delegate and work, which you just don't own it all by yourself there. And that's why I think the work at NCSC is so important, because when you talk about the

teamwork that you have in the individual agencies, we're trying to bring the team work together as a community as a whole.

[00:30:22] AH: And for the various functions that you have, So critical infrastructure, US supply chains, US economy, American democracy, cyber and technical operations. Again, we could easily do a podcast on each one of them. But I guess one of my questions is is cyber threat? It seems to me that cyber is a thread that runs through all of them. And cyber doesn't exclusively deal with everything in all five of those domains. But if we just maybe focus on cyber, we can start praising apart some of the other ones. Could you could you tell us about that, about cyber in that threat?

[00:30:58] MO: So cyber to me is a vector of how an intelligence service or a criminal actor goes about doing what they want to do. And so certainly trying to address the cyber problem is important. But I think it's important to know that the intelligence service doesn't exclusively rely on cyber. If you look at some of the espionage cases that are out there that had cyber intrusion, some of those cyber intrusions were enabled by a human insider who was able to plug something into the computer. So we shouldn't exclusively focus on cyber, and we need to look at the whole threat. And that, yeah, we have to recognize that intelligence services are essentially this well-paid, well-trained criminal enterprise. And they will create all sorts of ways of doing things if we just focus on one and eliminate one vector of a threat.

[00:31:40] AH: I want to turn a little bit now to talk about the insider task force. Can you tell us a little bit more about that?

[00:31:47] MO: Sure. And I believe it was 2011, WikiLeaks, Bradley Manning leaked all this information. And President Obama decided that there should be an executive order that stood up an insider threat taskforce that would be housed at the ODNI in partnership with the FBI, and that every government agency needed to have an insider threat program. So the insider threat task force works with all government agencies to set policies, standards training, maturity framework, and to do assessments on these programs. And I would say over the last 10 years they've done a great job of setting up these programs and government agencies that deal with classified information. And now that program is evolving where we're trying to work with the private sector, where we've done some publications on insider threats to critical infrastructure.

And the other thing we're trying to do now is really move towards how do you get left of the issue? The initiation of those insider threat programs is really focused on computer monitoring. And I would say in the private sector, insider threat is this dirty word. And people think it's just about monitoring your employees. I would argue that, no, it's really about protecting your employees. And that computer monitoring is one potential tool that you can use, but not the tool. And what we're finding is if you can get early into the HR process and make sure you're hiring people who have high ethics and then you create an organization culture where people are happy and you're able to address their issues and have good leadership, you may be able to identify issues early before they become a problem. And so that's where we're trying to head as we evolve the program is to get to that behavioral analysis and educate people on that. And so I think, if you look at espionage cases over the years, oftentimes in those interviews, they were some sort of issue that caused that person to do something. And it had to be just addressed that, we may have been able to kind of get them off the road early.

[00:33:30] AH: And what role do historical case studies play in all of this, or in the training, or in the education? So here at the Spy Museum, we have an exhibit on Hanson, Ames, and Phoebe. Do you those types of figures? Or is it something different?

[00:33:46] MO: Yes. So whether it's an insider threat training, or just basic counterintelligence training, cases are always used as an illustration of effective cases or how people have done things. I've known in the past, people have done studies on what causes people to commit espionages. And so these things are often talked about as things to learn from.

[00:34:06] AH: We're hopefully going to do a future podcast on this, but tell us a little bit more about the Wall of Spies.

[00:34:11] MO: So at NCSC, we have an exhibit called the Wall of Spies. And it doesn't cover every espionage case. But we have over 200 examples of espionage that started from the beginning of our country, in the Revolutionary War up to current times. And I find it's very informative, and for our professionals, it really gives them a quick oversight of everything that has happened over the years. And it's a constant reminder to our employees about the threat of espionage and doing the right thing. And it's also just a great place for people to kind of socialize and kind of celebrate our history and the work that we do.

[00:34:44] AH: Will it ever be going on the road? Will anyone who's not in the community ever be able to see a museum near them?

[00:34:51] MO: So we're looking to put the museum online so people can see the different exhibits. But I'm happy to host anybody for a tour as well.

[00:34:59] AH: I just want to pivot now to just discuss a little bit more about your backstory and coming to this position. I mean, there's a lot there, though we can dig into, the CIA, the military, the various things you've done in the FBI. Help our listeners just get a sense of your career trajectory. How did you end up over the NCSC?

[00:35:21] MO: So over 20 years, military intelligence and law enforcement, but spent most of it in the FBI doing counterintelligence. In the early 2000s, I worked on a multiagency task force on the Western Pacific trying to counter China's influence. And I would say, from my view, a lot of that, the great work we did on that task force really illuminated what we're seeing today and helped us understand some of the tradecraft of the Chinese intelligence service and how they go about influencing. And then I had the opportunity, and I think it was 2013, to work on the Benjamin Bishop espionage case. He was a contractor at Pacific Command at the time. He took information who we ultimately arrested and was convicted of taking that information.

And then in 2017, when I was the Assistant Special Agent in Charge at the Washington field office, oversaw the Maria Butina case, which many people are familiar with, unregistered foreign agent of the Russian government. And then I help stand up what is now the Iran Mission Center at the FBI, at that time was the Iran Threat Task Force, in which the FBI was trying to look at a multidisciplinary approach to that problem. Bring together counterterrorism, counterintelligence, and cyber to attack that problem. And then I did a tour over counterterrorism, which was certainly a great tour and fascinating. And I was involved in such things as the Pensacola attack, and many other domestic terrorism and international terrorism incidents. And then as that assignment wrapped up, there was an opportunity here at NCSC. And it was a good opportunity for me to get back to counterintelligence. For me, the recognition of the private sector, the public really need to be educated to defend themselves.

[00:36:55] AH: For the Maria Butina, could you tell our listeners more about that? Is there anything about that a case that is not out there that you would like to share with our listeners?

[00:37:06] MO: So I would say what I thought was informative about the Maria Butina case was it, I think, for the most part, people think as the Russians in very traditional intelligence officers operating outside the embassy. And in this case, it showed an example of an asymmetric threat from the Russian intelligence service. And so I thought that was something that was eye opening for people to understand, that there was other ways of going about doing things. But Maria Butina was a student who was really trying to work her way into political circles and acquire information and trying to influence government. Basically, for lack of a better word, cover was this kind of gun rights thing where she was looking for gun rights. And from that was able to make ties into organizations and meet people of interest to kind of get influence and then work with the Russian government.

[00:37:50] AH: Here at the Spy Museum, we have an exhibit on this, and the documentary that we have attached to that, Jack Barsky. He's kind of disparaging of Maria Butina and the Russian 10. People like me, we were highly trained and carefully selected. This is like Keystone cop stuff. What's your kind of view on that?

[00:38:14] MO: Well, whether it's Keystone cops or not, whether a person is well-trained or not, I think it creates challenges for the intelligence community, because it just adds another target, another threat vector that you have to counter. I would say if you go back to the Cold War, we knew there was a certain number of Soviets in the embassy, and we just had a cover down on that set number. Now, you have that set number plus all these asymmetric actors who are kind of “untrained” who could still do harm to you as well. And it becomes very difficult to assess whether they're a threat or not given that they're probably like a legitimate academic or student who's moonlighting for the intelligence service. Creates these challenges for you.

[00:38:52] AH: One of the other questions that I had was – Correct me if I'm wrong. You were formerly in charge of cancer intelligence for the Washington field office. Is that correct?

[00:39:01] MO: So I was the Assistant Special Agent in Charge for counterintelligence at the Washington field office. And I covered Russia and our global programs.

[00:39:08] AH: Sounds like a nightmare that job. I mean, it's a pretty target rich environment around here, right?

[00:39:14] MO: Yeah. And it was our 2016 as well. And so it certainly was a challenging time to work that threat.

[00:39:19] AH: Here at the Spy Museum, we try to look at the popular culture surrounding this and also the history and the reality of it. So for people that watch the Americans, and I don't know if you've seen it, but those types of things. What's it actually late to be working counterintelligence for the Washington field office?

[00:39:38] MO: I would say working counterintelligence anywhere in the Bureau has been very fascinating. There are great cases out there all over the place. I think people focus in on Washington because it's the capital, and it's certainly an interesting place as well. I would say that I found the Washington field office to work there to be very dynamic. There was more work than you can figure out what to do with. Worked with great people, we had a great team. Great supervisors, doing everything from trying to address the traditional Russian threat, the technical aspects of them to the asymmetric threat, and also trying to bring very emerging investigative techniques to this problem to really counter the Russians.

[00:40:14] AH: What was like the highlight? What was the one issue or case that you worked where you were like, "Yes." What gave you the most satisfaction? It doesn't have to be one and we'll have to get rid of the rest. But what's a particular one that sticks in your memory?

[00:40:30] MO: So I get asked this question all the time. And so it's a little bit challenging to answer because part of my work has been classified, right? And so I have to sit with the unclassified answers. But I would say, really, over my career, it's been working with the people. I've worked with some really fantastic agents and analysts and support people, not just in the FBI, but in NCIS, and OSI, and the CIA. And so that has been a really rewarding those relationships and the ability to kind of spend my career with some talented people has been most rewarding. You kind of forget about the cases and everything else. It's the quality of work that you remember.

[00:41:03] AH: And whenever I speak to people who have worked in the New York field office, it's almost like East Coast, West Coast rap. There's this kind of DC, New York thing going on. What are your views in that as someone that worked in the Washington office?

[00:41:19] MO: I've never been a New York agent, but I worked with New York agents. New York has just the mindset of, "Hey, we're the New York office, and we do what we want." And I think sometimes that works to their advantage. And I've always applauded their effort for being a little bit of the renegade office at times, because sometimes that's how you get things done.

[00:41:35] AH: And is there a sense that with the technological developments that have taken place that a lot of the action is Silicon Valley, or Seattle? Or is it kind of just more of a complicated picture now?

[00:41:51] MO: So it's fairly complicated. But given the threat environment that we've talked about cyber, the asymmetric threats, the interest in things beyond classified information and government information, to everything from technology, to seeds. Anywhere you go in the country, you're going to find fascinating and interesting work that's going to be very challenging. So I would say for anyone who's maybe stuck in an area in like Iowa that they think there's nothing going on, I'm sure Iowa has some fantastic case going on. And there's a threat there that's really interesting and challenging for them to work on.

[00:42:22] MO: We've got an exhibit where we're looking at economic espionage in Iowa where people are trying to get grains and seeds and so forth.

[00:42:30] MO: And that goes to that asymmetric threat, right? We're not just looking at the classified. But here, I believe in the case you're referencing, the Chinese government was trying to acquire seeds that had been genetically modified to be more drought resistance. And so that is the type of threat that we're up against is that we're trying to defend the loss of seeds.

[00:42:48] AH: And for someone like yourself, do you have a target on your back because of your position? Or is that something you don't want to talk about?

[00:42:56] MO: Well, I mean, if I'm my target, my target. I would say when you grew up in the counterintelligence community, you grew up with a certain mindset, because you're the spy catcher, and so you understand how you go about trying to surveil the adversary. And you know that the adversaries can do the same to you. And so you look at things from a different perspective from how you operate on a computer. When you go out overseas, how you handle yourself? And so you kind of grew up with a certain mindset there. And it certainly is challenging because you were privy to understanding how a sophisticated threat operates. Where I think the general public doesn't have that same view. I think the public understands the cyber threat to a certain extent, but doesn't understand the larger threat. Particularly if you're a business person traveling overseas to Russia, and you have something of interest, I think they're a bit disadvantage, which is why we do a lot of the outreach we do to try to educate the public. And I know that the FBI for years have really tried to worked with the communities to do that as well.

[00:43:50] AH: Say there's a listener out there, and the IC, and they're trained in counterintelligence or spy catching like you, but there's someone that just something doesn't sit right with them. I guess the question is, as an experienced spy catcher, can you pick up on when someone is not kind of on the level? Or are there particular giveaways or things that other than the obvious they're speaking in Russian on the phone to someone and they're driving a new Rolls Royce into the Langley or something like that? Yeah.

[00:44:25] MO: I would just say, as just a career FBI agent and just law enforcement in general, we're taught to read people, interview people. And over years, to just get experience into seeing something that's just quite not right. But I would say for the listeners, if you want to have a counterintelligence mindset, really think about your cyber hygiene, from do you have good email security? Do you have strong passwords? Those things will keep you safe on the Internet. Not 100%. Will minimize the risks. Do you patch your system? And then if you travel overseas, I would say do not bring your electronics. And if you have to bring electronics, make sure you don't have any sensitive data that you don't want lost on there. Understand that foreign governments have the ability to surveil you, to enter your hotel, get on your computer systems. It's a lot easier than anything that's going to happen to you here. So obviously, those are some basic tips. But also, in addition, we're a social media generation. And we've seen the Chinese and Russian government try to target people on LinkedIn and other social media platforms. And I certainly understand that the purpose of those platforms are to connect. I'd just say be mindful

that those programs, you're being targeted. So when you get a LinkedIn to ask you to travel overseas, or do an interview, or provide information, just make sure you're able to do some due diligence on that before you execute those things, because those have been done. Government employees have been targeted, and others as well, in those platforms.

[00:45:46] AH: Can I just pull on that thread a little bit? Could you talk about the Nevernight Connection?.

[00:45:52] MO: So that was a video that NCSC did in partnership with the FBI, in which we took a real world example of how a government employee was targeted on social media, on LinkedIn I believe. And then that video was supposed to go out to inform the community and the American public of those threats. And so I think that video did a lot to help bring attention to this issue.

[00:46:11] AH: I guess one of the other questions that I had was, with China, I know that like you've mentioned China several times, and I know that you have worked at threat and you have been to China. Is there anything similar to the Havana syndrome for agents or officers that are going to China? Or that's not really so much of an issue?

[00:46:35] MO: The reason I talk about China so much, I don't want anyone to get the impression that Russia or others aren't a threat. But when you look at the threat posed by China, it eclipses the other threats. You have China, this rising power, that's going to challenge us economically and national security. Where you only look at Russia, it's a declining power, who is just challenging us. And so we want to make sure we bring attention to the important issue of China.

When it comes to anomalous health incidents, I can't speak too much about that. If you're a government employee and you feel that you have symptoms of this, I would recommend that you report it to your government agency. I'd say the intelligence community is taking it very seriously. We're working hard to figure out what's going on and how we can address this issue.

[00:47:17] AH: I just want to pick up on security clearance and reform and the whole process. I believe that it's kind of quite a labyrinth in process. You could say that?

[00:47:30] MO: Yes. So security clearance reform. As I said earlier, the DNI is the security executive, and she's responsible for oversight. And in 2018, I think all of us who are part of that process from DNI, to OPM, and DoD, who is the biggest customer of it, would say the system was a bit broken. We had massive backlogs of probably 700,000 employees. And depending if it was a secret or top secret clearance, it could take you a year to get your clearance. And so collectively, we initiated a program called Trusted Workforce 2.0, where we were going to revamp this program. And today, we've been able to get that 700,000 backlog down to 200,000, which is what we call pretty good, a steady state. And we've got the numbers down from six months to a year to process your clearance to somewhere between, 50 to 75 days depending on your secret or top secret. So we've made some real progress there.

And the other thing we had found is that our policies were a bit convoluted, and the agencies were executing them in different ways. And then technology was antiquated. And so working in partnership with OPM, and OMB, and DoD, we have consolidated or aligned our policies. DoD is working real hard on the technology piece. And then we're moving into the next phase, the implementation phase. And a critical component of that is what we call the continuous evaluation or vetting, where we are doing away with the periodic five year or 10 year background checked, where you will routinely get an automated records check. And so we'll be able to identify threats much earlier as opposed to waiting for five or 10 years. That will free up resources to work the initial investigations and do other things. So we're making some progress on this. It's a really challenging issue, but really proud of the team that's working on it. And the partnerships between DoD, OPM, and OMB has been fantastic.

[00:49:18] AH: I guess one of the things that I wanted to ask was what are – If someone's like, “Director Orlando has inspired me. I want to do something. I want to roll my sleeves up and kind of get involved.” What sort of things can they do?

[00:49:33] MO: So I would say that the intelligence community, which is multiple agencies, has been really one of the best places to work. And we have people of all sorts of talents, no matter what your interests are, whether it's law enforcement, or analysis, or support, like accounting and other things. I think there are job opportunities in the community. And I would encourage you to explore those opportunities. It's a great place to serve your country. But I would also say

if that's not your thing and if you think there's an area of concern, I would particularly encourage you to reach out to the FBI if there's threats or you need partnership, and DHS as well.

[00:50:07] AH: I guess I was also wondering, is there someone sitting there and they don't have very good cyber hygiene, and so forth? Like do you always use a VPN? Do you use a particular search engine? A particular browser? Do you have two-factor authentication? What are some of those kinds of steps that they can take?

[00:50:26] MO: So first, I would say, for all your listeners, if you go out to the FBI and DHS's websites, they have some fantastic resources that can help you really strengthen your stuff. But what I've picked up on from the cyber experts, if you just make sure you have good email security, not clicking on the links, the spear phishing, that will go along the way. Your strong password as well and patching will really minimize the threat. I'm sure having a VPN or other things are great, but focus on the first three I talked about before you do anything else?

[00:50:54] AH: And what does the future hold for you?

[00:50:57] MO: I expect to stay here for quite some time. They have not announced a new director yet. And so I'm happy to continue to serve in this role. And then when they finally announce a new director, I will revert back to the deputy. This has been a great excitement. We have a lot of work to do. It's an important mission. And it's been a privilege to been selected for this assignment.

[00:51:14] AH: Tell our listeners a little bit about your journey from the military, to the CIA, to the FBI.

[00:51:20] MO: Yep. Did ROTC once in the military. Certainly enjoyed that. Had a great experience. But I knew I had always wanted to be an FBI agent.

[00:51:29] AH: What era was this? Is this the 90s?

[00:51:31] MO: Oh, you're bringing me back. It as 1995.

[00:51:36] AH: Okay.

[00:51:36] MO: But there was a hiring freeze for the FBI. And so I had found an opportunity at CIA, which I thoroughly enjoyed my time at CIA. But once the hiring freeze got lifted, I was called for an interview and was offered a job. And knowing that that's what I wanted to do, I wanted to make sure I did that. Otherwise, I'd feel I would regret missing the opportunity. And so that's how I eventually made it over to the FBI.

[00:51:58] AH: You weren't ever tempted to stay with the CIA, or did you always wanted to rather than stay?

[00:52:03] MO: I certainly was tempted. I enjoyed it. I worked with great people there. But I was afraid if I didn't tried it, which what I wanted to do, I would always wonder everything. And it's worked out great, because I've worked a lot with the CIA over my years in the military. So it's all been tied together. And what I would say to the listeners, figure out what you're passionate about, because you can do that in a lot of places. And I think I've always been passionate about the national security work. And I've been able to do that at the FBI.

[00:52:28] AH: Final point. Is there anything that you would like to discuss or bring up that we haven't covered? Is there any particular ingredients that are an important part of the dish that makes up the NCSC or Mike Orlando that we haven't been cooking with?

[00:52:45] MO: I would just say, for NCSC, we have a team that does a great job of bringing people together. And that's not an easy talent or job to do. But I would say to your listeners that, as I started off with, what kind of keeps me up at night is particularly the China threat. And to the extent you can educate yourself on that and defend yourself and build resiliency and just know that NCSC is here to help and play our role.

[END]