A Conversation With Christopher Wray

Friday, April 26, 2019

Carlos Barria/Reuters

Speaker

Christopher A. Wray
Director, Federal Bureau of Investigation

Presider

Richard N. Haass

President, Council on Foreign Relations; @RichardHaass

Director Wray discusses the FBI's role in protecting the United States from today's global threats.

HAASS: Well, good morning and welcome to the Council on Foreign Relations. I'm Richard Haass, president of the Council.

And we're honored this morning to welcome Christopher Wray, who is the director of the Federal Bureau of Investigation. He's going to be here to discuss the FBI's role in today's world. Director Wray leads the nearly thirty-seven thousand men and women of the FBI, and I just want to take a second to thank him and all of his colleagues for what they do for this country.

Timing is a lot in life, and the timing could hardly be better for us—the director may feel differently—(laughter)—given all that's going on that falls under his and the Bureau's purview. He's had a distinguished career. First served as the assistant U.S. attorney for the Northern District of Georgia in '97 to 2001. Then he joined the Office of the Deputy Attorney General here in our nation's capital. In 2003 he was nominated by forty-three to serve as the assistant attorney general for the Department of Justice Criminal Division, where he spent several years. Glad I didn't know you at that time. And then he returned to the government recently, in August of 2017, when he was confirmed overwhelmingly by the Senate to become the eighth director of the FBI.

Here's how we're going to do it today. The director will first offer some remarks from this podium, then he and I will have a conversation before turning to you, the membership, for your questions.

And with that, please join me in welcoming Director Wray to the Council on Foreign Relations. (Applause.)

WRAY: Well, thanks, Richard. It's great to be here with all of you. Listening to Richard go through my background a little bit there, I will say that if you had told me just even a couple years ago when I was back in private practice that I would be finding myself back in the world of law enforcement and national security in any capacity, much less standing in front of the Council on Foreign Relations as the FBI director, I would have been more than a little bit skeptical. My wife would probably have burst out laughing. (Laughter.) She and my grown kids—our grown kids both spend a lot of their time rolling their eyes at me and shaking their heads. But there's nothing like a loving family to keep your feet firmly on the ground. (Laughter.)

In spite of their amusement or maybe even amazement, I am, in fact, here today to talk about the national security threat from the FBI's perspective. And I want to talk about a number of things, but I want to focus in particular on the multilayered threat posed by China. I also want to talk about the need for stronger-than-ever partnerships with law enforcement, with the intelligence community, with all the communities we serve, and increasingly with our partners in academia and the private sector, because the reality is that the threats we face today are too diverse, too dangerous, and too all-encompassing for any of us to tackle alone.

As you heard, I last left DOJ's leadership back in 2005. And at the time I think it's fair to say we were still in many ways building up our national security capabilities in the wake of the 9/11 attacks. And we'd made a lot of progress by the time I left, but coming back now I see a before and after with the break in the private sector

that jumps out at me more, and I see firsthand the strides—really incredible strides—that have been made towards keeping people safe from all kinds of harm from an increasingly wide array of bad guys.

In some ways, for me it's a little bit like the experience that I'm sure a lot of you have had of seeing the child of an old friend and you think, wow, last time I saw you you were like this tall; when did you get so big? When did you get so grown-up? Of course, then I start thinking even using that analogy makes me wonder how did I get so old. (Laughter.) But putting my advancing age aside, the world is incredibly different now. 9/11 was a gamechanger in so many terrible ways, not just for the United States and for our own national security apparatus but for the whole world. And those attacks blew apart any notion of separation between foreign and domestic threats, any notion that such attacks only happen to other people in other countries.

I remember vividly standing in the FBI's 9/11 command center with then-Director Mueller and a slew of others in a jam-packed room in the afternoon of the attacks. I remember in the period that followed meeting with families of the victims of those attacks and absorbing their shock and their heartbreak face to face. And though none of us could have foreseen where we'd be now, today in 2019, we all knew that the world had shifted around us. And now when I look forward it strikes me that we face yet another paradigm shift in the way we view the world.

The nature of the threats we face is evolving. Criminal and terrorist threats are morphing beyond traditional actors and tactics. We still have to worry about things like an al-Qaida cell plotting a large-scale attack, but we also now have to worry increasingly about homegrown violent extremists radicalizing in the shadows. These folks aren't targeting the obvious—you know, the airport, the power plant; they're

targeting schools, sidewalks, landmarks, concerts, shopping malls with anything they can get their hands on, and sometimes things they can get their hands on pretty easily: knives, guns, primitive IEDs, cars. These are people moving from radicalization to attack in weeks or even days, not years. And they're doing it online and in encrypted messaging platforms, not in some camp or cave.

On the cyber front, we're seeing hack after hack and breach after breach, and we're seeing more and more of what we call a blended threat where cybercrime and espionage merge together in all kinds of new ways. We still confront traditional espionage threats—you know, dead drops, covers, things like that—but economic espionage dominates our counterintelligence program today. More than ever, the adversaries' targets are our nation's assets—our information and ideas, our innovation, our research and development, our technology. And no country poses a broader, more severe intelligence collection threat than China.

China has pioneered a societal approach to stealing innovation in any way it can from a wide array of businesses, universities, and organizations. They're doing it through Chinese intelligence services, through state-owned enterprises, through ostensibly private companies, through graduate students and researchers, through a variety of actors all working on behalf of China. At the FBI we have economic espionage investigations that almost invariably lead back to China in nearly all of our fifty-six field offices, and they span just about every industry or sector.

The kind of activity I'm talking about goes way beyond fair market competition. It's illegal, it's a threat to our economic security, and by extension it's a threat to our national security. But it's even more fundamental than that. This is behavior that violates the rule of law. It violates principles of fairness and integrity. It violates our

rules-based world order that's existed since the end of World War II. Put plainly, China seems determined to steal its way up the economic ladder at our expense. And to be clear, the United States—our country is by no means their only target.

They're strategic in their approach. They actually have a formal plan set out in five-year increments to achieve dominance in critical areas. And to get there they're using an expanding set of nontraditional methods, both lawful and unlawful, so weaving together things like foreign investment and corporate acquisitions, together with cyber intrusions and supply chain threats. The Chinese government is taking the long view. That's probably an understatement. They've made the long view an art form. They're calculating. They're focused. They're patient and persistent.

Overlaying all these threats is our ever-expanding use of technology: next-generation telecommunications networks like 5G, the rise of artificial intelligence and machine learning, cryptocurrencies, unmanned aerial system, deep fakes, all sorts of stuff that wasn't particularly focused on during my time in the private sector but now back in government I see blinking red right in front of me and right in front of all of us. And we grow more vulnerable in many ways every day.

Taken together, these, I think, could be called generational threats because they're going to shape our nation's future. They'll shape the world around us. They're going to determine where we stand and what we look like ten years from now, twenty years from now, fifty years from now.

Our folks at the FBI are working their tails off every day to stop and find criminals, terrorists, and nation-state adversaries. We're using a broad set of techniques, from our traditional law enforcement authorities to our intelligence capabilities. We've

got taskforces all over the country with hundreds of partners from local, state, and federal agencies. We've got taskforces now targeting everything from terrorism to violent crime to cybercrime to crimes against kids, crime in Indian Country, you name it. We've got legal attaché offices all over the world now, stationed around to participate in joint investigations and information sharing. We've got rapid-response capabilities. We can deploy at a moment's notice pretty much anywhere in the world for almost any kind of crime or national security crisis. And on the nation-state adversary front, together with our partners, we've got a whole host of tools we can and will use, from criminal charges and civil injunctions to economic sanctions, entity listings, visa revocations.

But even with all of that, we can't tackle all these threats on our own. We've got to figure out more and more ways to work together, particularly with all of you in the private sector. We need to focus even more on a whole-of-society approach because in many ways we confront whole-of-society threats. It is very clear to me that the next few years will be very much defined by what kind of progress we can make with private-public partnerships.

One of the things that I've found most pleasantly surprising since coming back to government is the state and enthusiasm of partnerships. I've spent most of the past twenty months since becoming FBI director visiting all fifty-six of our field offices, and in each office I've been meeting with all of our employees to get a better handle on the work they're doing in the trenches, but I've also been meeting in one state after another with our partners: law enforcement, the communities we serve, academia, the private sector. And while I hear about the same threats and concerns

everywhere I go, I also hear about how much more effectively we're working with our partners across the board with whole new levels of teamwork. And in my view, that's exactly the kind of thing we need to be building on every day.

In our country the vast majority of our critical infrastructure and intellectual property is, of course, in the hands of the private sector. You own it. You run it. You're on the frontlines. So you know the risks, you know the weak spots, and you're much more likely in many ways to see the emerging threats coming down the road.

Nation-state actors are also targeting academia, including professors, research scientists, and graduate students. They seek our cutting-edge research, our advanced technology, and our world-class equipment and expertise.

And that's why it's so important for these lines of communication to be open. We've got to share as much information as we can with you as quickly as we can through as many channels as we can. We've also got to create mechanisms for you to share information with us so that we have a better understanding of what you're seeing, what you're worried about. We've got to keep building trusted relationships with all of you so that you know with confidence that we're here to help.

So I hope we can keep this forward momentum going. I really do believe it's the only way we can maintain and strengthen our firm footing as the world continues to shift around us. So look forward to continuing the discussion with Richard and with all of you. Thanks for having me. (Applause.)

HAASS: Well, thank you, sir. This is—this is actually now going to be one of the cool moments of my sixteen years here, because as we start the Q&A I can now read the director of the FBI his Miranda rights—(laughter)—and tell him that it's on the record and anything he says can and will be used against him. (Laughter.)

WRAY: That means I can decline to answer. (Laughter.)

HAASS: Touché. (Laughter.)

We'll get to China in a minute, because you had a lot to say about China. But I wanted to speak about another country—to use your phrase, a nation-state adversary—namely, Russia. And I wanted to begin with the special counsel, Mr. Mueller, who described Russian interference in the 2016 election, to use his phrase, "sweeping and systematic." Is that a view you subscribe to?

WRAY: Well, I think everybody has their own adjectives. I do think that Russia poses a very significant counterintelligence threat, certainly in the cyber arena, certainly what we call the malign foreign influence territory, certainly in their presence of intelligence officers in this country. So in a lot of ways, yeah.

HAASS: Did we see any change, from your vantage point, between Russian interference in the 2016 presidential election and the 2018 midterms? Did you see any evolution in the scale or nature of the Russian threat or interference?

WRAY: Well, I think it's important to distinguish between two categories. Sometimes the word "interference" and "influence" get—even by us kind of get bandied about a little interchangeably, and I'm not sure that's quite the right analogy for each.

foreign influence—malign foreign influence—we usually use to describe the fairly aggressive campaign that we saw in 2016 and that's described in the special counsel's report, and that has continued pretty much unabated, is the use of social media, fake news, propaganda, false personas, et cetera, to spin us up, pit us against each other, sow divisiveness and discord, undermine Americans' faith in democracy. That is not just an election-cycle threat; it's pretty much a 365-days-a-year threat. And that has absolutely continued. We saw that, therefore, continue full speed in 2018, in the midterms. What we did not see in 2018 was any material impact or interference with election infrastructure or, you know, campaign infrastructure.

HAASS: Since you raised that, I assume, though, you don't—you don't assume that won't be an issue in 2020. So do you feel that we either nationally or locally—how comfortable are you with what is being done to protect our election infrastructure?

WRAY: Well, I think—on the one hand I think enormous strides have been made since 2016 by all the different federal agencies, state and local election officials, the social media companies, et cetera. But I think we recognize that our adversaries are going to keep adapting and upping their game. And so we're very much viewing 2018 as just kind of a dress rehearsal for the big show in 2020.

HAASS: 2020. You talked in a slightly different context about public-private partnerships. What about the public-private partnership between your—the FBI and law enforcement more broadly and social media companies? What do you see as the division of labor? And are you comfortable with the nature and level of effort by the social media companies to make sure they're not exploited?

WRAY: You mean on this foreign influence threat?

HAASS: Yes, sir.

WRAY: So that's one of the places where I've seen the most dramatic change from 2016 to the midterms in 2018. The flow of information back and forth between law enforcement and the intelligence community and Silicon Valley, I think, has gotten dramatically better. I think those companies recognize that there is a need for them to take action, so that their own platforms are not abused. And so there was—there were a lot of success stories in the midterms, where some of these companies were taking pretty aggressive action on their own, voluntarily, not at our behest or requirement, to enforce terms of use and so forth on their platforms and shutting down and kicking off various accounts that fit into the kind of category we talked about.

HAASS: Russia is obviously the—again, to use your phrase—the national security adversary that most people are concerned about. But what about others trying to influence our society, our political processes? China, conceivably, North Korea, Iran, all of whom have fairly advanced cyber capabilities. To what extent is this a Russia problem? To what extent is this a much broader challenge?

WRAY: Well, foreign influence is certainly a broader problem. And it's been around for decades. I think what's changed and what the Russians have really take not a different level in 2016, and continuing, is the use of social media as kind of a bullhorn to facilitate those efforts. Certainly we see other types of foreign influence efforts by all those countries that you mentioned, but they tend to take slightly different forms sometimes to influence particular policymakers, officials, to shift decision-making and analysis in the government one way or the other. But certainly

all those countries are watching and taking note of what the Russians attempted to do in 2016 and since. And I think we expect that this is going to become a phenomenon we're going to have to contend with, with a lot more than just Russia.

HAASS: Let's turn to China for a second, because that was a big part of your opening comments. You've got the challenge posed by Chinese students, some of whom seem to be more interested in acquiring technology than good grades. (Laughter.) What about the Confucius Institutes? What is your view of those and whether they are a dangerous platform, or a problematic platform in this country?

WRAY: Well, I mean, the Confucius Institutes are something that we view as part of a sort of soft power strategy that the Chinese government has, and certainly something we're concerned about. In many ways, a lot of the things that I talked about in my opening comments are things we're more concerned about even than the Confucius Institutes, though.

HAASS: Should there be clearer criteria or rules of the road, or rules of conduct, that universities put into place and enforce about scholar access and student access? And if those rules are violated, should there be penalties?

WRAY: I do think that the academic sector needs to be much more sophisticated and thoughtful about how others may exploit the very open, collaborative research environment that we have in this country, and revere in this country. And I'm encouraged, actually, by the number of universities around the country that are taking very thoughtful, responsible steps to make sure that they're not being abused, and that their information, proprietary research, confidential information isn't stolen, which is happening all over the country. And it's a real problem.

HAASS: One of the phrases you used in your remarks was: China—I think I've got it right here—is determined to steal its way up the economic ladder at our expense. And then you talked about the first layer of responsibility is obviously the firms themselves. What more needs to be done? To what extent does this require things that are really beyond the capacity of individual firms? I mean, they're up against a nation-state. It doesn't sound like a fair fight.

WRAY: Well, we are structured very differently, right, as a country, than China, where essentially everything rolls up to the Chinese Communist Party. They have scale and centralization. We have decentralization and free markets. And I wouldn't want to change that. But it does mean that we need to be thoughtful about trying to find ways to partner together in a common defense. And we're trying to take steps in that regard with things like meeting with companies, providing threat awareness briefings, telling them things to be able to look out for, in some cases even doing what in the intelligence community we would call defensive briefings, you know, in a classified setting, and cautioning them about what some business partner might mean that they don't fully appreciate. But I do think companies need to make sure that they're taking a little bit more of the long view. They can't just be focused on what's going to look good in the next earnings call. The reality is that some of these threats are existential threats to them as a business. And they need to have that perspective.

HAASS: Is your relationship simply preventative, in the sense that you would go to company XYZ and say: You ought to be doing this sort of thing? Or do you also have a reactive relationship, where you would go to them and say: We have reason to believe you have now been penetrated by this or that, some national actor, and you have to deal with that? How does it work?

WRAY: Well, first off, we try not to be telling companies what they need to do. Again, that goes along with the kind of free market world that we're in. So we try to have conversations where we're giving them facts, and information, and sensitizing them to things that they need to be concerned about. And more often than not, I've actually been pleased by the reaction we've seen in the corporate sector by companies making, I think, on their own, the right decisions.

Now, in the cyber arena, because, of course, one of the many tools in the toolbox of our adversaries are cyber intrusions, we have a whole protocol for when we make victim notification and when we try to provide information to a company that may have been hacked or where they may have had an insider who's been bought off, who helped steal information. And that's happening all the time. In the last several months alone, we've charged a number of either MSS officers or hackers associated with the MSS for what is out and out intellectual property theft.

HAASS: DOD has run into some problems with certain firms in Silicon Valley not wanting to work on certain contracts, when they felt it was being put for certain purposes, they were uncomfortable for civil liberties and whatever reasons. Have you run into that problem, where certain firms, companies in this country, have basically said: We're not going to cooperate for you because our—for example, our employees are not comfortable with doing so?

WRAY: You know, we—I would say our relationship with Silicon Valley is complicated. (Laughter.) But I think we are having, I think, increasingly positive interactions with them. We don't always agree on everything, but we're not experiencing, that I can think of, any company that just says: We don't want to work with you.

cfr AASS: OK. The most recent large-scale terrorist attack, an awful one, a few days ago was in Sri Lanka. What is your take on what lessons—what does that tell us? What lessons? How should we understand that and perhaps act in any way differently going forward?

WRAY: Well, without commenting too directly on the Sri Lankan attacks specifically—other than to confirm that, of course, the FBI has sent personnel over to assist in the investigation, to work with our partners over there—I do think it's a reminder that the terrorist threat isn't yesterday's news, isn't yesterday's problem, isn't gone. I sometimes think people in this country and in other parts of the world have started to get maybe a little blasé or a little complacent about it. And it's a pretty chilling reminder that the threat is real.

I think it also shows that folks can radicalize in a virtual way, which is a bigger and bigger problem. You know, people talk about ISIS and the fall of the caliphate, absolutely true. On the other hand we, worry very much about what is in effect a virtual caliphate where terrorist organizations can organize in a way that don't require the same kind of physical infrastructure. The other thing we see, which is, I think, a problem that people need to be very aware of, is you always hear this phrase about connecting the dots in the terrorist arena, but a lot of the terrorist plots of today are more compact, involving fewer people, less complicated attacks, shorter period of time, which means fewer dots to connect in the first place.

And then if you add on top of that the different ways in which communication is encrypted and hidden, that makes the dots even fewer. And the time in which law enforcement and intelligence community folks can act has compressed. So the

professionals sometimes refer to the time from flash to bang. Well, the time from flash to bang has shortened. And that's putting a whole new strain on our collective security.

HAASS: At the risk of worrying everyone in the room and beyond, have you seen any change in the interest on the part of these individuals, and networks, and groups in what we used to describe as grand terrorism—not content with car bombs and knives and boxcutters, but also thinking of weapons of mass destruction?

WRAY: Well, I want to certainly be careful about what I can talk about in this kind of a setting, but I will say that despite my description of the home-grown violent extremist, the ISIS-inspired attacks, the car bombs, the gun attacks, the knife attacks, et cetera, the so-called sleeper cells the efforts to conduct mass casualty attacks is still a phenomenon that exists today. And there's degrees to which some terrorist organizations are starting to rebuild and revive. So it's something we're definitely focused on.

HAASS: So—I don't want to put a words in your mouth, obviously—but implicit in what you're saying is that people have to rethink the way they think about terrorist, at times—you used the word, I think, some people are getting blasé. There's a sense of thinking it as a traditional threat there that it's time limited and at some point it goes away. And as I hear you talking about it, what you're basically saying is we have to think of this as an open-ended, ever-evolving threat.

WRAY: I think that's—I think that's fair. I mean, what I would say is there's a difference between resigning yourself to terrorism as a fact of life and becoming apathetic and numb to it. So finding that balance between staying vigilant, staying on the balls of our feet, taking it seriously, and not being consumed or distracted by

cfr is, I think, where we need to be. And I think in many ways, that's one of the things I've actually been most encouraged about inside the national security arena. The sort of robust, mature machine that now exists inside the government, collaboration, integration between different parts of law enforcement, our joint terrorism taskforces within the intelligence community, with our foreign partners is so much more well-oiled than it was in the immediate aftermath of 9/11, that I was, you know, relieved, frankly, to find it. But it just has to be also caveated with the fact that the—you know, that the challenge keeps going up too.

HAASS: So a few more questions then we'll open up to our members. You alluded to domestic terrorism. How big of a problem is that? What you might call white nationalist groups in the United States? The emergence—a lot of people a few years ago would have talked about domestic terrorism and this focus of this or that Islamic cells. What about white nationalist terrorism?

WRAY: Well, we sort of separate the world of terrorism into kind of true international terrorism, which is, you know, al-Qaida, Al-Shabaab, Hezbollah, et cetera; homegrown violent extremists, which I was describing quite a bit earlier, which are more ISIS or other groups inspiring but maybe not directing—so efforts to conduct attacks by people who are already here on behalf of the global jihadist movement; and then what you're getting to, which is domestic terrorism, which is not just different kinds of violence committed on behalf of some kind of white supremacy ideology but all the way over to anarchist ideologies, and all kinds of things in between.

We have lots and lots of investigations in that space. It's a steady, persistent threat against all those different types of domestic terrorism. We've had quite a number of arrests. I think last year we had more arrests—domestic terrorism arrests, our JTTFs,

our Joint Terrorism Taskforces—than we did internationally terrorism arrests. So we're working very actively in that space. You know, we brought charges against some folks involved in the Rise Above Movement for their connection to the Charlottesville rallies and some other things. We had an individual—a Coast Guard lieutenant who wanted to commit an attack right here. We've had the so-called package IED case—

HAASS: Who might, by the way, be released, I saw, by the judge.

WRAY: We'll hope the judge does the right thing. (Laughter.)

HAASS: One issue that's come up obviously, and the president's made a—put a great emphasis on it, is the threat—the national security threat posed by, quote-unquote, "illegal immigrants" coming across the southern border. To what extent, from your point of view, are illegal immigrants in this country—to what extent do they pose a serious national security threat?

WRAY: Well, certainly the border security threat is something that I think needs to be taken extremely seriously. Having gone down and visited the border in multiple locations and been to all of our field offices that are in that area I think there are significant security threats posed along the border, ranging from drug trafficking concerns, human trafficking concerns, and a lot of the attendant violence that comes with it.

HAASS: OK. I could ask a lot more questions, but I will show uncharacteristic restraint. We've got a good chunk of time left. I guess I don't have to ask people to raise their hands. (Laughter.) You anticipated my—what I'll ask you to do is keep

cfr

our—raise your hands. We'll get you to stand up. Please identify yourselves. One question to a customer. And as brief as you can make it, and that way more of your fellow members will get in.

Jill, why won't you kick us off?

Q: Thank you very much. Jill Dougherty from the Wilson Center.

You know, Director Wray, I was thinking of a phrase, it came to mind as you were speaking, which is: dirty cops, a phrase used by President Trump. And it seems pretty obvious that the bureau has been under sustained rhetorical attack recently. To what extent has the bureau been damaged by this? If it has, how would you assess the impact of that on the bureau?

WRAY: So this is a topic near and dear to my heart. I would tell you that rumors about damage to our morale, or brand, or anything else, are grievously overstated. I say that now with the perspective of having been to all fifty-six field officers and met with—and when I say I met with, I mean, like, have a conversation with something like three or four thousand of our partners. The feedback I get from our partners is that the bureau has never been stronger and better. The feedback I get from our employees is that they're inspired. We're not focused on the rhetoric. We're focused on the work. We're focused on who we do the work with, and who we do the work for.

And I look at examples, like the woman in our Miami officer, who had twelve stitches in her face from a bad accident. Next morning, back at it. I look at the guy, the SWAT agent in Chicago who got shot up in his arm by a fugitive from an AK-47

and not only survived but retrained himself to shoot lefthanded, and then requalified for SWAT lefthanded. These are people who love their jobs.

HAASS: Have you had any issues or any changes in either recruitment or retention?

WRAY: You know, actually, I'm glad you brought that up because despite chatter—and lord knows there's enough chatter out there to keep everybody busy—I'm focused more on action and words—action than words. And so I look at recruiting. You know, we have had since October something like sixteen thousand people apply to be special agents, which is up from all of the prior year. That tells me something about brand and enthusiasm for the mission. I look at the interns applications—you know, we're in a thriving economy. So kids coming out of college have a ton of choices.

We have the highest number of people applying to work at the bureau out of college that we've ever had. And our selection rate in both of these pools is between 5 and 6 percent, which is more selective than just about any Ivy League school. Of course, I'm tempted to maybe stop using the Ivy League school analogy. (Laughter.)

HAASS: Yeah, the question is whether it's as selective as USC.

WRAY: Yes, right. But I look at retention—and then I'll be quiet. But again, this is something I feel very passionately about. You look at our attrition rate—meaning special agents leaving before their normal retirement age—and our attrition rate last year was 0.5 percent.

HAASS: Impressive.

WRAY: And I bet you that there's not an organization represented in this room that has an attrition rate that low. So we have people who are grouchy and cynical all the time, just like everybody. (Laughter.) But when it comes time to manifest their views through their work, they move the mission.

HAASS: Good to hear.

Sir.

Q: Steve Charnovitz, George Washington University Law School.

You've explained that China has a formal plan to achieve dominance. And you said they're weaving together the legal as well as the illegal activities. And the FBI mission is the illegal ones. But since you mentioned the legal side, do you think the United States has a strong enough long-term plan of our own to deal with China's challenges in the world? So, for example, is the line between legal and illegal right, should it be changed? The Congress did that a little bit last year on export controls. Are there other areas where the Congress should change the line? You mentioned economic sanctions. Do they have a role, versus the legal activities of China? And then how can the United States take the long view, more than what we're doing, with respect to soft power?

WRAY: So it's an excellent question. I would say there are legislative fixes that are useful. For example, in the foreign investment space CFIUS, which a lot of people in this audience are familiar with, Congress did make, I think, very important reforms on CFIUS. That's not a matter of criminalizing or making something illegal, but it's a matter of using our laws to better protect our economic and national security. And I think there may well be things like that that can and should be done.

you know, the importance of recognizing that things like foreign investment is fine, corporate acquisition is fine, talent recruitment in the academic sector is fine. But understand that those things in the wrong hands can be abused. And so both punishing the behavior when it crosses the line and then using the tools that we have to better protect ourselves long term, I think is where the country needs to be. I do think that this country, going back the last couple of decades, has underestimated this threat. The good news is, everywhere I go in my first twenty months in this job—up on the Hill, throughout the administration with different agencies, the corporate sector, the academic sector, foreign partners—people are waking up and realizing that this is a threat that needs to be taken seriously. And I think that's good news for everybody.

HAASS: Edward Luttwak.

Q: Edward Luttwak.

I was very reassured by your—what I interpreted as a focus on China as a strategic threat. Question: Are you able to acquire the necessary human resources? Because the foreign intelligence community, twenty years after the Middle East high engagement, still has nobody who speaks Arabic in the room of fifty-two—maybe one. Question, can you acquire this expertise? Second, given that you have such wide responsibilities, but many of them are also the concern of state, local enforcement, and so on, can you offload these other responsibilities to focus on the strategic threat? These are the two questions. Thank you.

WRAY: So I'll take the second one first. We don't view ourselves as offloading responsibilities, but we do view ourselves as working more smartly, if I can use that—probably not a word—with our state and local law enforcement partners. That's

where these taskforces come into play. So take something like violent crime for example. We aren't offloading violent crime responsibility, but we are trying to focus on what does the FBI uniquely bring to bear to that problem set, and then leveraging partnership with others, like state and local. So try to imagine a care with an FBI agent at the wheel, and everybody else in the car is from another agency. We're all going the same place. We're working together. And that allows us to stay in the fight, to provide the expertise that we have without trying to be all things to all people. So that's the way we kind of view most of those phenomenon.

I think on the first issue, about whether we have enough resources to deal with the China threat—and it sounds like you're particularly talking about our language skills, certainly we are trying very hard to recruit people with language skills. Every time I go to a graduation—an agent or analyst graduation—I'm looking at language skills that are reflected in the class. So people who speak Mandarin, for example, are certainly attractive to us. But, again, that's where partnership with others helps us bridge that gap. So we're not the only agency working on this problem, so therefore we're not solely dependent on our own linguists. We work so much more closely now with our intelligence community partners, so we can share and collaborate with each other. And if we work more and more closely with the private sector, there are ways for us to leverage their expertise. Our foreign partners, we're able to leverage their expertise.

You know, there are very few people in this world who, having seen what it's like to work in silos and seen what it's like to work in teams, would pick silos. And it took, I think, the national security apparatus a little while to get to that recognition. But now that we're there, it makes it so much more efficient and effective to deal with some of these kinds of problems.

HAASS: What about on the technology side? Last I checked, your stock option plan is not very generous. (Laughter.) And how is it you compete with the private sector there to get people not who speak Mandarin, but might be able to also to be familiar with some of the cutting-edge technology, say in AI? How do you compete there?

WRAY: Well, certainly in terms of recruiting it's a challenge, but we find that most young technically savvy people today are drawn less to financial incentive and more to trying to do meaningful work and tackle hard problems. And so what we have to offer in terms of recruiting is we're dealing with the most sophisticated adversaries there are. And we're able to give them an opportunity, some of these kids, to do things that they can't legally do—(laughter)—in the private sector. So there's that. (Laughter.) And then second, we also—through our partners, we have a lot of ways in which we're partnering with the private sector to take advantage of their innovation. I've been out to northern California a couple times. A lot of my direct reports have done it as well. And so we're looking at ways in a variety of settings to capitalize on what they see in terms of innovation and technology.

HAASS: OK. Sure, yeah.

Q: Hi. Jeff Pryce, Johns Hopkins.

On the Russian intelligence adversary, one of the evolutions from the old days has been the increasing role of the GRU military intelligence in the Russian intelligence services. And I wonder if you have any thoughts on that shift in the balance of the Russian challenge. The GRU has a reputation of being more aggressive, operating by a slightly different set of rules than their sister Russian agencies. So thoughts on that shift in the Russian challenge, and implications for us.

WRAY: I'm pausing because I want to think about what's appropriate for me to talk about in this kind of setting.

HAASS: You're just among friends here.

WRAY: Yeah, exactly right. (Laughter.) Small, intimate collection.

HAASS: Exactly.

WRAY: Well, look, we've taken a number of steps to be more aggressive to call out GRU actors for some of the more brazen things that have occurred. I think about, for example, you know, we charged a number of GRU officers for their role in an extensive hacking campaign to undermine in the international anti-doping arena, for example. Some people sometimes question whether it makes sense to charge—you know, to indict foreign intelligence officers. I actually happen to believe that it makes sense because sometimes in the foreign intelligence arena you get into questions of attribution. I'm tempted to say nothing saying attribution more than an indictment. We believe very strongly in our criminal justice system. And that's our way of saying: We're so confident that we're right that we're willing to have these people come into a U.S. courtroom and take our chances with the jury, beyond a reasonable doubt. And also, we find that a lot of these folks like to be able to travel. And once they've been indicted, their travel options get decidedly smaller. And the FBI has a long memory and a broad reach, and I wouldn't be surprised if we see some of these people in orange jumpsuits one day.

HAASS: Nelson Cunningham.

cfr: Thanks very much. Long ago I was an AUSA in the Southern District of New York. And on behalf of all the great agents I've worked with I want to thank you for spending a lot of time on the integrity and the reputation of the FBI as director.

My question, though, goes to the cyber intrusions—the celebrated cyber intrusions we've had—North Korea's hack of Sony, the Chinese hack of the Office of Personnel Management records, others. My question is: Do we have the right tools, the right framework for retaliating? In other words, not just saying: Stop doing that, don't do it again. But you did it, we know you did it, and here's the way that we've retaliated against you. Do we do that in the right way?

HAASS: You can even extend that to those who might try to influence our elections. Do we have the right retaliatory framework there?

WRAY: Well, the thing about offensive cyber is that it works best if people like the FBI director don't talk about it on television. (Laughter.) But suffice to say we're looking at an all-tools, all-agencies approach. I will use your question as an opportunity to say that what we're not a big fan of is what some in the private sector sometimes refer to as hack back. We don't think it's a good idea—

HAASS: Just can you explain what you mean?

WRAY: Yeah. We don't think it's a good idea for private industry to take it upon themselves to retaliate by hacking back at somebody who hacked them. That creates all kinds of potentially unintended consequences. And so not something we would recommend, any more than we would recommend people taking justice into their own hands privately in another arena. I do think we have to get more and more agile in dealing with the problem. And one of the—in the cyber arena in

particular. And one of the things that I think is still kind of lost, even among sophisticated audiences, is people tend to think of cybersecurity as their perimeter, whereas in fact in many ways the most important part of cybersecurity in today's world is inside. It's your own insiders.

So think about the analogy of a house, right? Yes, it's very important for you to have an alarm that goes around your perimeter. Yes, it's important for you to have locks. Maybe it's important for you to have cameras on the outside, and lights, and everything else. But all that stuff is kind of useless if the person who's in your house already got a key from somebody and is just hanging out in your basement and whenever you go off to work is rummaging through your personal and confidential information. So a big part of cybersecurity is encouraging companies and other organizations to much more quickly look inward, because it's not a question of if you get hacked, it's when. And so mitigation is in some ways more the appropriate concept than just out-and-out prevention.

HAASS: So you're going to say here on the record that you do not keep your password written on a yellow stick-um next your computer? (Laughter.)

WRAY: I am.

HAASS: OK. Good. I just want to—just wanted to clarify that. (Laughs.) Yes, sir.

Q: Thank you very much, sir. My name is Andy Maslowski (ph) with the U.S. Department of State.

A question for you that may not be immediately within your purview but based on something you had shared with us. You said that you feel that malign influence from other countries targeting the United States with the intent to divide us is

ongoing. I think, you know, any good analysis of threats requires a good analysis of the vulnerabilities of that threat. From your perspective, what makes us so vulnerable to attempts to divide us as a country? And what could we, as the federal government or leaders such as yourself or others, be doing to address that vulnerability? Thank you.

WRAY: Well, I don't think we in the FBI, or we in the federal government, can or should police content. And that's a core tenant of who we are as a nation. And so in a sense, though, that makes us inherently more vulnerable. So part of what we need to be doing is raising public awareness, so we have a more resilient, less reflexive, more thoughtful populace. So people need to be careful what they read. People need to try to do a little thought about maybe what's the sourcing of what I'm reading. People ought to get their news from a variety of different sources. People ought not to believe everything they see on Twitter.

HAASS: You don't think there ought to be any—just so I understand what you said—you don't think there ought to be any limits or constraints on content dealing with incitement, how-to to do certain things? You think all—that we basically ought to leave it up to the judgement of individual Americans and others to make of it what they will?

WRAY: I don't know that I would say that. I just think when it comes to passing laws or providing criminal tools that deal with content, we're in very delicate First Amendment territory, and we need to be very thoughtful about how we do that. We are trying to do our partner to raise people's awareness about what the issues are, what they should be on the lookout for. You know, we put out a website at one point called protected voices, that sort of tried to raise campaign awareness in other people in the voting public about how to be a little more intelligent consumers of

information. And, again, back to the private sector, there's an incredibly important role for Silicon Valley and a lot of the social media companies to be able to do things that they can do as a business to enforce terms of use on their own platform to prevent those platforms from being abused and manipulating our public.

HAASS: Sure. Yes, sir.

Q: Hi. I'm Andy Sullivan with Reuters.

If we could return to domestic terrorism for a minute, when you're investigating somebody who's inspired by ISIS, for example, you've got a very valuable tool you can use, which is it's against the law to provide material support to a foreign terrorist organization. When you're looking at somebody who's inspired by white supremacy or other ideologies like that—the Coast Guard guy is a good example—you don't have that. Do you need more tools from Congress? Do you need more laws to help go against people like this? The Coast Guard guy might go free today.

WRAY: Well, I would say that, look, we always like having more tools. That makes us more versatile and more effective. So I would never be one to turn down the offer of new weapons in the fight.

But I will say that what distinguishes the international terrorism arena from the domestic terrorism one is not just the existence of a material support statute. It's also true that we designate foreign terrorist organizations, and that's what people are providing material support to. The State Department is involved in those kinds of designations. In the domestic terrorism context we are not seeing so much terrorist organizations in the same way that you might think of ISIS or al-Qaida or al-Shabaab or Hezbollah as an organization. We're seeing more lone actors, more

people kind of informally kind of associated with each other. It's much more uncoordinated, decentralized. And so it's not really clear to me that you would be able to designate, for example, domestic terrorism organizations and really move the needle much.

We rely very heavily on all sorts of other charges in the domestic terrorism context: gun charges, you know, mass explosive charges, false statement charges. We work with state and locals, with all kinds of, you know, murder charges, attempted murder charges, assault charges, you name it. And so I think we've actually been pretty effective. But it does put a premium on the theme that I've been pounding on today, which is this partnership concept.

We certainly—we've also brought hate crime charges in the context of some of the domestic terrorism settings. One of the Charlottesville actors, for example, we had a twentysomething-count hate crime indictment.

HAASS: Got time for just a couple more. Mr. Slattery, you've been patient.

Q: Yeah. Jim Slattery, Wiley Rein.

I get the whole issue about regulating content—(comes on mic)—under the First Amendment. What can we do, though, to disclose origin of content and provide that information to the consumers of the content?

WRAY: So you're—I think you're—well, we sometimes use the word "source" instead of origin, but I think that's the right concept, which is we're focused on who's doing it, not on what they say. So I think it's important to understand that in

the space of foreign influence we don't start by looking at inflammatory content and then trying to figure out who's responsible for it. We're focused on the threat actors, and then we try to figure out what content they're generating.

And I think when we have something that we can expose publicly to raise awareness, we try to do that. We are also mindful, though, of the fact that the sort of perplexing thing about the sowing divisiveness and discord strategy is that we don't want to play into the adversary's hands by giving more amplification and volume to something that we might be able to nip in the bud fairly quickly, right? So think about some completely fake news effort using a false persona, bots, et cetera. If we're able to, working with Silicon Valley, get that shut down within a matter of days before it got a ton of traction, we don't want to then add to the problem by increasing everybody's concern by, you know, broadcasting information that we were able to prevent from really going viral. So there is sort of a balancing act tactically that we go through on a case-by-case basis.

But I do think you're right in general that focusing on the source or the origin, as you say, is really the name of the game. I think people would be surprised at how much content is a couple steps removed sourcing back to, you know, the IRA or some other Russian propaganda arm.

HAASS: Are you yourself on Facebook or Twitter?

WRAY: Nope. (Laughter.)

HAASS: Will you do it—after you're out of this job, will you—will you start?

WRAY: Nope. (Laughter.)

HAASS: Dan Yergin.

Q: Director Wray, as you know, there's been some discussion recently about the issue of visas involving academics and researchers from China who are not in artificial intelligence, but rather things like international relations. Could you share your thinking about that and how you see that kind of issue evolving?

WRAY: Well, I don't want to comment on any specific visa-related decision or a specific academic center's decision. I will say that we have seen many instances in which the visa process, which I think is very important to ensure an open and collaborative research environment, which I have no desire to change in that sense, is being abused and exploited. And in those instances where we have information that exposes that abuse, we want to share it with the right people so they can make the right decisions. And as I said, I think that's starting to happen more and more often, and I think you can expect to see that happening more and more often.

HAASS: Got time for one last question. The gentleman in the back has been patient. And then—

Q: My name is Tarat Puladia (ph). I'm with the Voice of America Persian Service.

My question is that—so White House, in an unprecedented move, last week designated IRGC and Quds Force as FTO. So my question is this. In this context, the role FBI plays in combating IRGC, Quds Force, Hezbollah presence here in the U.S. And is there any credible threats from these individuals or these entities in the U.S.? Thank you.

WRAY: Well, I don't want to discuss any specific investigation, certainly. I will say that with or without the designation we've had any number of matters related to Quds Force activity, including here in the United States, as have some of our closest partners. And I think it's high time that that threat be taken even more seriously.

HAASS: When the director hears the initials CFR, his first instinct is the Code of Federal Regulations. (Laughter.) I want to thank him today for visiting the other CFR. And again, thank you not just for being with us today, but for all that you and your colleagues do.

WRAY: Thank you. (Applause.)

(END)