# INTERVIEW 1
# Bill Evanina Full Interview Transcript
# Recorded Oct 6, 2020
# Kiplinger Research Library, D.C. History Center

**Mark Albert, Chief National Investigative Correspondent, Hearst Television** [00:00:16] Sir. Thanks very much for joining us today.

**Bill Evanina, Director, National Counterintelligence and Security Center** [00:00:18] You're welcome. My pleasure to be here.

**Mark Albert** [00:00:19] You're the director of an agency called the National Counterintelligence and Security Center. What does that agency do?

**Bill Evanina** [00:00:25] We're primarily responsible for driving the strategy and policy for America's counterintelligence and security posture. What that means is across the nation's intelligence community, the U.S. government writ large in the private sector to drive threatener awareness to those who might be victims of foreign adversaries overseas. We also set that strategy. So agencies like the NSA, CIA, FBI, can implement that strategy on an operational level.

**Mark Albert** [00:00:51] It sounds like you're almost a clearinghouse of threats.

**Bill Evanina** [00:00:55] We the centralized basis where we can convene and bring people together to connect the dots, so to speak. If you look at what happened after 9/11, the ODNI was formed, NCSC is now that vector in counterintelligence and security to bring all the requisite agencies together to solve problems to protect America.

**Mark Albert** [00:01:12] Right now, you are the point person for the intelligence community's efforts on election security. You sound like you have your hands full.

**Bill Evanina** [00:01:20] I do. But I would also say that as much as is a challenge, Mark, it's probably after the events of 9/11, probably the most important thing that I will do in my career is to lead us through this crisis point of protecting our election for the American people. I look at this as an honor, a public trust to be able to be in this position. And I take it seriously.

**Mark Albert** [00:01:39] And I want to get to that crisis point in a minute. But first, I just want to get a little bit of your background out of the way. Correct me if I'm wrong. You're from Pennsylvania, right? Career intelligence official, former CIA, former FBI. You've been in your current position about six years, which can't be sort of an eternity in Washington, D.C. in some positions. Politico did a profile of you in August. And I want to read you a couple of things that people said about you in the profile. Quote, The one man standing in the way of Russian election interference. Another, you are competing with Vladimir Putin directly and another, a man running into the buzzsaw. Have you ever been cut by that buzzsaw?

**Bill Evanina** [00:02:17] I have not. I could probably say I had not. I Pride myself on having 24 years of experience in the intelligence community and being a government employee since I'm twenty one. To be able to say that that buzzsaw is out there, but we are navigating a very - not just myself and my cohorts in the government - are navigating that

and the buzzsaw has many blades and it comes in many different flavors. So it's a, it's an art, but it's also a science. I think it's an opportunity in which makes our democracy so solid, is those buzzsaws exist.

**Mark Albert** [00:02:44] You do have a lot of heat on you right now, though.

**Bill Evanina** [00:02:46] Well, you say heat. I say accountability. Responsibility.

**Mark Albert** [00:02:49] OK. Let's dive right in then. You have issued two public statements to the public. One, a hundred days out from the elections about the election security threats. And I just want to go through a couple of the points that you raised in a statement, and hopefully you can add a little bit context to it. You mentioned, quote, We see our adversaries seeking to compromise the private communications of U.S. political campaigns, candidates and other political targets. Basically, they're trying another hacking link. Correct. Just like in 2016 when Russian linked organizations hacked into the DNC, John Podesta's e-mails on the campaign release that damaging effect. Are they trying to repeat that in 2020?

**Bill Evanina** [00:03:28] They are. As well other countries like Iran and China and others.

**Mark Albert** [00:03:31] Which campaigns are they targeting?

**Bill Evanina** [00:03:33] All the above. So I think we look at adversarial actions, whether attempts for cyber activity to gain access to personal information, personally identifiable information, candidates, campaigns, computer systems. It's what they can get a hold of and where they can get most value. And I will prophet back in 2016, I don't think the Russian government and the IRA fully knew what they were getting when they when they have, they have both campaigns. So I think it's also an opportunity there for them to say where they want to utilize information. But what has the best value for them at the end of the day?

**Mark Albert** [00:04:05] You say in 2016, the Russians hacked both campaigns. Have they hacked both campaigns this time?

**Bill Evanina** [00:04:10] So. So I will comment on what they've been able to do, if they've been able to do anything, but I can tell [00:04:15]you we've seen all three threat actors attempt to gain access to critical infrastructure that is associated with elections, as well as personal usage of their emails as well servers and for the both campaigns. [14.0s] We've seen a commensurate amount of activity by all three nation states threat actors.

**Mark Albert** [00:04:33] You mean Russia, Iran and China.

**Bill Evanina** [00:04:35] That's correct.

**Mark Albert** [00:04:35] And I just want to drill down to be very clear here. When you say election infrastructure, that's one thing. When you talk about the campaigns, that's another. And then it could be personal information, personal email accounts, et cetera, on candidates or or politicians. Which of those three buckets have these three countries tried to penetrate?

**Bill Evanina** [00:04:53] All three. I will tell you that it's a point of emphasis for what's available. But I'll also caution that when we see activity from our adversaries on the

election-based infrastructure, it's election and others. So hypothetically speaking, an adversary can impact an election infrastructure by having a ransomware or hacking dump or cyber activity, in a separate part of the county or the municipality, that's not directly related to elections but can significantly have an impact on the electoral infrastructure. So we've seen all three countries have aggressive attempts at gaining access to this infrastructure.

**Mark Albert** [00:05:30] Have any of them been successful?

**Bill Evanina** [00:05:31] I'd rather not comment on that. But I can tell you that we are very resilient and we've been very successful in pushing back the majority of these efforts.

**Mark Albert** [00:05:38] Well, respectfully, I know you would prefer not to comment, but I know a lot of the American people would want to know specifically what has been done to try to influence their vote. Do you think the American people deserve to know if one of these three countries has been successful?

**Bill Evanina** [00:05:51] Yeah, I do. And all of that. But I can tell you what we've said before, and we'll say now, is that we've seen three big buckets of activity. Number one is the attempted to gain access to critical infrastructure that's germane to an election or counting. We see that attempt on an everyday basis.

**Mark Albert** [00:06:06] So voter registration, e-pollbooks, that kind of thing?

**Bill Evanina** [00:06:10] Yep, or to the municipality for other areas or could just be unknown cyber criminals who are who are attempting to gain access for a ransomware attack. They might not be witting that that could have election infrastructure tangent accountability. [portion edited for clarity] Secondarily, the attempt to gain personally identifiable information from candidates, from campaigns and prominent Americans is a big increase from 2016. You call the hack and dump. We've seen nation state threat actors collect this data for unknown usage at the end of the day, but it's a concern to us. And also the last bucket is the disinformation and the influence campaign. We see all three countries that we mention engaging in on the nation to really sow discord, especially since our nation is involved in really polarizing events. So whether it be for the George Floyd killing, the covid issues, the debates we're having, the I would say the discourse in whites and protests, we see all three nation states playing in that game to amplify and exacerbate those issues.

**Mark Albert** [00:07:25] So before I move on, I just want to talk about that second bucket. You're talking about hack and leak, hack and dump operations. So just to be very clear, you're saying that Russia, China and Iran, all three have had, have tried to hack into the presidential campaigns, the parties and other people this cycle?

**Bill Evanina** [00:07:46] I think hack is a mysterious word. Gain access is what I'll talk about.

**Mark Albert** [00:07:50] What's the difference?

**Bill Evanina** [00:07:51] Well, I think hack is a symbol of success, right? We've seen the attempted.

**Mark Albert** [00:07:56] Penetration.

**Bill Evanina** [00:07:57] Attempted penetration both not only with the personally identifiable information with it for your e-mail, for your servers, for the campaigns. We see it every day. And I think that we expected that. But the resiliency we have now is much different than we had in 2016.

**Mark Albert** [00:08:11] [00:08:11]So all three countries have tried to penetrate the major campaigns and candidates. But you won't tell us whether they were successful? [6.5s]

**Bill Evanina** [00:08:19] [00:08:19]That's correct. [0.1s]

**Mark Albert** [00:08:20] [00:08:20]That's a key point, isn't it? [0.8s]

**Bill Evanina** [00:08:21] I don't think so. I think the efforts should be that we as a government and as a private sector and the social media companies and the I.T. companies, the campaigns, the candidates have been very resilient this go around. I think that government collaboration with the campaigns and with the candidates has been, I would say, interlocked to the point where we have great information going back and forth. And where we have seen potential successes, we have immediately notified those victims. So I would say that hypothetically, when you look at success, what that looks like, the ability for the government to notify that victim, is unprecedented. Secondarily, our protective measures against such activity is not only strong and stalwart here in the US, but we're fighting this overseas as well.

**Mark Albert** [00:09:02] How many times have you notified a victim that their information has been hacked this election cycle?

**Bill Evanina** [00:09:09] That's a good question. I wouldn't have those numbers available to me right now.

**Mark Albert** [00:09:11] I mean, single digits, double digits.

**Bill Evanina** [00:09:13] Again, I wouldn't have that. And that's primarily in the realm of the FBI's role to be able to identify the victim and make those notifications.

**Mark Albert** [00:09:20] But you would know because you are giving the intelligence to the DHS, FBI.

**Bill Evanina** [00:09:24] [00:09:24]I can tell you that's happening. [0.9s]

**Mark Albert** [00:09:26] [00:09:26]It's happening or happened? [1.0s]

**Bill Evanina** [00:09:27] [00:09:27]It's both. [0.1s] And now we expect it to happen more between now and the election.

**Mark Albert** [00:09:31] So I just want to be very clear here. You have notified the FBI and the DHS of successful penetration efforts.

**Bill Evanina** [00:09:38] No. So we have notified the FBI and DHS of attempts to gain access to these facilities, as well as the FBI and DHS have identified on the ground. There are multiple agencies that have the ability to identify this. All of that gets, I would say,

aggregate in the FBI. And the FBI is the focal point which goes out providing victim notifications to people, companies and people who own servers.

**Mark Albert** [00:10:01] And I just want to be clear, because you use the word victims, and in my mind, you're not a victim if it wasn't successful. If you didn't get my information hacked, penetrate me, then why am I a victim? So that's why I'm a little confused.

**Bill Evanina** [00:10:11] We look at it differently in the government. So a victim is someone if you are attempted robbery or attempted bank robbery or attempted break in and entry, you're still a victim. 'Cause it still has consequences to your ethos, your ecosystem, and I'll say your bottom line. So if you're a company or you're a person and you have an entity overseas trying to do something to you, you're still victimized.

**Mark Albert** [00:10:29] [00:10:29]And so you have made those notifications about campaigns and or candidates this election year?[6.1s]

**Bill Evanina** [00:10:36] [00:10:36]Yes. Multiple congressmen, senators, multiple people that are prominent in the US. [3.2s] I think the span of influence is great right now in our nation. And it's nothing new. It's not germane to the election, so to speak. But the foreign influence on America isn't anything new. It used to be just living, but right now we've seen nefarious activity with intelligence services. We see it every day across the United States of America, on state and local governments, on U.S. congressmen, U.S. senators and business leaders. When we see that happening, whether it be via cyber or by human, we notify those individuals so they can take mitigation steps.

**Mark Albert** [00:11:10] And these notifications of the prominent politicians that you've just mentioned were from Russia, China or Iran.

**Bill Evanina** [00:11:17] Yes. Or other countries, but primarily Russia, China and Iran.

**Mark Albert** [00:11:21] And these are people running for office?

**Bill Evanina** [00:11:23] Or currently in office and they're trying to influence their policies towards and I'd say the majority of those issues are clearly China. China has a very, very aggressive influence campaign against U.S. policymakers. Because [00:11:34]we are in, I would say, a geopolitical war with them right now. [2.7s] So they want to influence policymakers, especially those policymakers who might be anti China. So they have a full court press to influence those members.

**Mark Albert** [00:11:46] And I just want to make sure that we're very clear here. So these people that you have notified, these political high profile individuals who are in office, they are running for office or not running from both?

**Bill Evanina** [00:11:59] Both.

**Mark Albert** [00:12:00] Both. OK.

**Bill Evanina** [00:12:00] And again, I want to and it's also prominent businessmen. It's companies. It's industries.

**Mark Albert** [00:12:05] Right.

**Bill Evanina** [00:12:05] Sector folks. And it's also maybe companies that own servers that are tied to other things. So the word victim is probably vague. And I would say the American public doesn't understand the way we look at a victim. But if you look at it as a victim and what that feels like, that's kind of where we are. So if we see any attempt by a foreign adversary or an unknown actor to do something to a U.S. base, person or thing, the FBI notifies them as a victim.

**Mark Albert** [00:12:30] And have you notified the Trump or Biden campaigns that they've been a victim?

**Bill Evanina** [00:12:33] So I can tell you that [00:12:34]I have briefed the Trump and Biden campaign four times over the last few months, [3.2s] as well as the RNC and the DNC. And we've had over 20 sessions with Congress on all of these issues.

**Mark Albert** [00:12:44] But have you notified the Trump or Biden campaigns that they have been a victim?

**Bill Evanina** [00:12:47] I have not. If that had occurred, it would be done by the FBI.

**Mark Albert** [00:12:50] OK. Sorry. Before I move on have you told the FBI or DHS, notified them, that either the Trump or Biden campaign were a victim?

**Bill Evanina** [00:12:58] I have not.

**Mark Albert** [00:12:59] OK. Anyone under your command?

**Bill Evanina** [00:13:01] I have not.

**Mark Albert** [00:13:02] Anyone in your agency?

**Bill Evanina** [00:13:04] The intelligence... My my agency has not done that.

**Mark Albert** [00:13:05] OK. Perfect. I just want to make sure I'm not missing somebody or something. Thank you. Let's go on in your statement here as well. You talk about foreign nations continue to use influence measures in social and traditional media in an effort to sway U.S. voters' preferences and perspectives. Have you seen in the past week those types of foreign influence campaigns around the president's covid 19 diagnosis?

**Bill Evanina** [00:13:30] Have not. And I can be honest with you. I have not seen my intelligence this week to that. But I can tell you all three of those countries countries had utilized their expertise and their capabilities to exacerbate and enhance and amplify all issues that America is going through right now. I would say going back the last eight to 10 months.

**Mark Albert** [00:13:48] The George Floyd protest?

**Bill Evanina** [00:13:49] All the way up to covid and through everything we're seeing in the West Coast, to the forest fires. You name the issue our adversaries will use it as a driving wedge in our country.

**Mark Albert** [00:14:00] Final point on this 100 day statement that you put out and I'll move on. You also right here toward the end, we encourage Americans to consume information

with a critical eye. Check out sources before reposting or spreading messages, practice good cyber hygiene and media literacy, and report suspicious election-related activity to authorities. Report to whom? Are they supposed to call you, the FBI, 911?

**Bill Evanina** [00:14:22] Both. So they should call the FBI, your local office. They should call the local county, or the local election officials. All elections are local, and the local officials have done a great job the past few years to put mitigation practices in place to not only protect the infrastructure of the election, working closely with DHS, but also to provide a prophylactic to influence and disinformation. So we would ask each individual, each American, to ask your local authorities, what are you doing to help me as a as a confident voter?

**Mark Albert** [00:14:49] Because I have to be honest, Bill, when I talk to voters, they're hearing the messages from the federal government be on the lookout for information campaigns, foreign influence. They're looking at the Senate Intelligence Committee report that they've issued on Russian interference in 2016 and are saying, OK, I get the big picture but [00:15:05]what am I supposed to do, specifically me as a voter in Albuquerque or in Kansas City or Fort Smith, Arkansas. What are they supposed to do? [8.7s]

**Bill Evanina** [00:15:14] [00:15:14]Vote. [0.0s] At a minimum, be a confident, prepared voter. Let's be clear. All this disinformation and influence campaign we see, from regardless of what country, is all in an effort to sway the voter, the American voter. The best way to mitigate that is for have that voter get up, get out and vote in any mean, in person or by ballot, some other way. Vote. That's the best way to mitigate all the noise.

**Mark Albert** [00:15:42] To be fair, though, even if a voter does go. They cast their ballot. They could have been influenced in how they vote by some of these foreign or let's be honest, domestic misinformation campaigns.

**Bill Evanina** [00:15:53] Sure. So there's a combination. Let's see, social media, the way we see news everyday, the way we get information in our family organizations, our neighborhood organizations, our chat rooms, the the e-mails all the way up to the national news and cable news. It's really confusing. There's no doubt about it. And if you can get lost in that noise very quickly. And depending on which political side you lay, you're going to have influence from both sides as well. I would encourage voters, if they haven't already voted, get your information regard with respect to elections from your state and your local authorities.

**Mark Albert** [00:16:24] Local authorities. All Right. Let's go on. You issued another statement ten days later. You took some criticism for perhaps not being as specific in the first statement as many people would have liked. So in this next statement, you go in more detail on China, Russia and Iran. You talk about under China that they're pressuring political figures that they view as opposed to their their interests, that they're, you know, writing up as to counter criticism of China, political rhetoric, etc.. That's far different, though, than what the Mueller report, the Senate Intelligence Committee, the joint assessment of the intelligence community in January 2017 found that Russia did. Isn't it?

**Bill Evanina** [00:17:02] Well, we can't compare apples and oranges here. So our assessment here is predicated upon the 2020 election cycle. 2016 is over. It is what it is. There's been plenty of studies done on that no one disputes that. This these two memos you reference for us are about the 2020 election cycle. And I will say that, yes, we have language in there that's germane to both Russia, China and Iran. But I will say that we

have to look at this with an eye that not all three have the same ideology, not all three have the same intent or the same capabilities. And I would say the same want or wish here in the US. We have to look at it as a bucket. We have not gone. We have not put efficacy on these efforts. Nor were we categorizing on which one's more difficult than the other or which one's more successful. And yet this is what we see in that place in time, the efforts of these these countries to be able to provide this information, influence and activity, in the election cycle.

**Mark Albert** [00:17:54] And you say they're apples and oranges, but I guess a lot of voters could be wondering why that would be. They look at Russia. They've used cutouts before. They've used proxies. They've staged real events where Americans have been arguing at each other. They've done hacking leaks. They've got troll farms. They've done penetration, scanning. The scale and scope just seems so much broader with Russia that we're aware of in the public than what you say China's doing.

**Bill Evanina** [00:18:18] But I will challenge the premise a little bit. I would say it's quite the opposite. So what we see, Russia's activities so far have been germane only to the presidential election cycle. The activities we've seen with country Communist party of China has been all elections, not just the presidential election, but I would say state and locals, congressional, Senate elections. They are more widespread with their not only intent, their capability, because they want to have true policy change. I would argue [00:18:44]that Russia wants to sow discord and wants to destroy democracy. [2.7s] They've always wanted to do that, they'll continue to do that. And the best way to do that is to and for our purposes and Americans believe that they are influencing our election. That sows discord. China needs America long term to succeed, as I would say, a parasitic entity to be the global leader of the world. They need our economy. They want to influence all aspects of policy, not just germane to the presidential election. So it's a little bit different. They're both engaged in the game. But I will say they're both different. So we have to look at it not initially to whether they want President Trump to win or not. It's a bigger span than that. [00:19:20]It's more, I would say, existential. [1.3s]

**Mark Albert** [00:19:22] [00:19:22]If you say that Russia wants to destroy America. That seems like a bigger threat than what China's doing? [6.6s]

**Bill Evanina** [00:19:29] They do. And but the point about they're both nuclear superpowers. But Russia's capabilities are germane to disrupting democracy. They've done it all the world. They want to continue to do that. Vladimir Putin is has a I would say a inferiority complex for the United States. He doesn't like democracy, democratic values, what we stand for. So he will do everything he can to sow this kind of discord, even if it's at our local level with with protests. China is a more long view perspective. They want to be able to have geopolitical and economic ties with us. They don't want to have decoupling. They want to be able to have us be symbiotic. So they're more nuanced, but they're more influential at, I would say, elections and activities across the span of the United States of America.

**Mark Albert** [00:20:15] Right. But as you've just mentioned, Russia wants to destroy this country.

**Bill Evanina** [00:20:17] [00:20:17]Yes, they do. And China does not. [1.5s]

**Mark Albert** [00:20:19] [00:20:19]So isn't that the bigger threat? Russia is the bigger existential threat? [2.6s]

**Bill Evanina** [00:20:22] [00:20:22]Not to me. Russia can't destroy. Unless they a nuclear bomb, Russia has no ability to destroy our country. Until they continue to drive wedges of of us in the socio-economic perspective in our society. China, as an existential threat, has much more arrows in the quiver. They have much more capability, flexibility, and they both have intent. But I would say China's probably six to eight times more effective and dangerous than Russia. From a counter intelligence perspective. [27.2s]

**Mark Albert** [00:20:50] You say six to eight times more effective. But Russia pretty much got what they wanted in 2016, right?

**Bill Evanina** [00:20:55] I'm not saying that. I would look at it, America... I would say Putin got what he wanted with respect to sowing discord in America. And where we are right now with our lack of confidence in our election process, wherever that value is, we can squarely put in the efforts of the Russian government.

**Mark Albert** [00:21:11] Since you mentioned Putin, I just I was gonna ask you about this a little bit later, but since you're bringing it up, where do I have it? Here. Hang on. Putin just weighed in on this, actually, and I wanted to read you what he said. So he just last week on September 25th, he offered the U.S. a deal. He proposed that Russia won't interfere with the U.S. election if we don't interfere with theirs. Are we interfering at the same level?

**Bill Evanina** [00:21:37] Last I checked, Vladimir Putin is the president until 2036. So I'm not quite sure what election he's referring referring to. But, you know, the Russian word is as valuable as how good their vodka is.

**Mark Albert** [00:21:47] All right. Let's talk about you've mentioned in this statement. Ninety days out from the elections, Iran, China, Russia. What other countries are either interfering in our election process or seeking to interfere? Saudi Arabia?

**Bill Evanina** [00:22:08] Yes.

**Mark Albert** [00:22:08] Venezuela?

**Bill Evanina** [00:22:09] Yes.

**Mark Albert** [00:22:10] North Korea?

**Bill Evanina** [00:22:11] No.

**Mark Albert** [00:22:12] Cuba?

**Bill Evanina** [00:22:12] Yes.

**Mark Albert** [00:22:13] Turkey?

**Bill Evanina** [00:22:14] Yes.

**Mark Albert** [00:22:14] UAE?

**Bill Evanina** [00:22:15] No.

**Mark Albert** [00:22:17] Israel?

**Bill Evanina** [00:22:17] No.

**Mark Albert** [00:22:18] So you said UAE, Saudi Arabia. Those are U.S. treaty allies.

**Bill Evanina** [00:22:22] I didn't say UAE. I said no to UAE. So let's just go Cuba, Venezuela, Saudi Arabia, for the most part. And I would say influence, not interfere. There's a difference. So...

**Mark Albert** [00:22:32] What's the difference?

**Bill Evanina** [00:22:33] Cuba wants to influence their voters here in the US, to for one way or another. In terms of interference is a very strong word. I think it's really important for your viewers to to, I would say really have a fundamental understanding of the difference between interference and influence, right. We can unequivocally say that in 2016, not one vote was, I would say interfered with, not one vote was changed, not one vote tally was changed. That would be a...

**Mark Albert** [00:22:59] Vote tally was changed, but it could have been changed because of the influence campaign...

**Bill Evanina** [00:23:01] That's different. So your ability to go in and to pull a lever for a particular candidate because you were influenced is separate, than that lever showed a different result. Those are two separate things. Interference is a big deal. That means a cyber activity. The one results were posted on election night. There's been a cyber hack. But your influence is the mind of the voter, right? Can could a voter went into a poll polling booth, pull the lever because they were influenced one way or another, domestically or internationally? Sure. That's influence.

**Mark Albert** [00:23:31] So when you listed these countries, Saudi Arabia, Venezuela, right? Cuba, North Korea, those are influence?

**Bill Evanina** [00:23:39] Influence only. Right. So I would say that, you know, I will ask you, you know, we don't put them in the top three. We don't put them in the top anything. At the end of the day, can can can Venezuela really influence a voter in the US that's going make a difference? I would say not. So as much as we probably have 30 countries out there wanting to play in the influence game, it's about scale, right. So there's really three we're worried about.

**Mark Albert** [00:24:00] And that's the Iran, Russia and China.

**Bill Evanina** [00:24:02] That's correct.

**Mark Albert** [00:24:02] But just to be clear, Saudi Arabia, Venezuela, Cuba and North Korea are currently trying to influence U.S. voters?

**Bill Evanina** [00:24:08] Influence, I would say influence influence their constituents based here. You know, whether it be the diaspora who can vote or policymakers. We also say influence the vote. I want to be very careful when I talk about what political influence looks like. It's also in the policy sphere. There could be members of Congress running for Congress that have pro or anti a mindset with respect to any of those countries. And they

will probably influence them accordingly. I would say, however, North Korea has none of that. North Korea has the capability to sow massive, catastrophic ill will here if they chose to do so. As can Iran because they have capability, intent and they really have nothing to lose.

**Mark Albert** [00:24:45] OK, so then I want to be very clear. North Korea has tried to interfere this year?

**Bill Evanina** [00:24:50] No, they have not.

**Mark Albert** [00:24:51] OK. So none of these four countries have tried to interfere...

**Bill Evanina** [00:24:53] Interfere, correct, yes.

**Mark Albert** [00:24:54] Interfere, but they're all currently doing influence operations.

**Bill Evanina** [00:24:57] That's correct.

**Mark Albert** [00:24:57] Isn't Saudi Arabia a U.S. treaty ally?

**Bill Evanina** [00:24:59] They are.

**Mark Albert** [00:25:00] What are they doing trying to influence an ally?

**Bill Evanina** [00:25:03] Well, it's sometimes it's geopolitical, right? So just like we put in our second memo, every country or their leaders or the people have a preference for who they would like to see that can influence their their forward leaning or their capability to have geopolitical ties. They all have different preferences. Every country has a preference. Every American voter has a preference. So we don't look at it any differently.

**Mark Albert** [00:25:23] I'm going to go to another line here that you mentioned. You say the IC, intelligence community, is also doing everything in its power to combat both cyber and influence efforts targeting our electoral process. What does that mean?

**Bill Evanina** [00:25:35] So we are fighting both here domestically and overseas. So the men and women of the intelligence community and DOD have been very aggressive the last couple years, fighting the fight, forward deployed, let's say. So we're not just doing it here domestically. We have entities working around the world to protect our elections. And we're proud of that.

**Mark Albert** [00:25:52] Like where?

**Bill Evanina** [00:25:53] Around the world. And I think so we've seen some things publicly. So I'll do some unclassified. I think there's been some stories of NSA's work in Africa against the Russians. So I'll leave it there. You can Google that yourself. But we have had some amazing successes, but they're unclassified and classified around the world. But we are fighting the fight overseas.

**Mark Albert** [00:26:12] How about any against China since you've listed China in this memo as well?

**Bill Evanina** [00:26:17] So I say on all aspects of how we fight these things, diplomatically, militarily, influence. From a negotiation perspective or publicly, we are engaged in all three, all these efforts against all three countries.

**Mark Albert** [00:26:30] OK. So but you just listed Russia as one that we've taken action against.

**Bill Evanina** [00:26:34] Right, because that became out public by, NSA released that publicly.

**Mark Albert** [00:26:36] Can you make anything public on China and Iran?

**Bill Evanina** [00:26:38] I'd love to, but I can't. All I can tell you is that the American public should be very proud of the women and men in the intelligence community, in the Department of Defense who are taking this fight globally.

**Mark Albert** [00:26:47] And use the word aggressive a minute ago, so I just want to drill down on the word aggressive. That means counter operations. That means cyber defenses, attacks. What does that mean?

**Bill Evanina** [00:26:57] All the above.

**Mark Albert** [00:26:58] All of the above.

**Bill Evanina** [00:26:59] Anything we need to do under law to protect our elections. And protect our democracy. And we continue to do that.

**Mark Albert** [00:27:06] And the U.S. intelligence agencies have done that this year related to the presidential election?

**Bill Evanina** [00:27:10] That's correct.

**Mark Albert** [00:27:11] When was last time?

**Bill Evanina** [00:27:14] Again, great question.

**Mark Albert** [00:27:16] Well, thank you...

**Bill Evanina** [00:27:16] But just be confident we continue to do it, and we'll do it, up through elections and through inauguration.

**Mark Albert** [00:27:21] All right. I want to read you something the FBI director said on the Hill on October 1st [editor's correction: September 17]. He said, quote, We certainly have seen very active, very active efforts by the Russians to influence our election in 2020 through what I would call more the maligned foreign influence side of things, social media, use of proxies, state media, online journals, et cetera, in an effort to sow both divisiveness and disorder. And I think the intelligence community has assessed this publicly to primarily denigrate Vice President Biden and what the Russians see as kind of an anti Russian establishment. That's essentially what we're seeing in 2020. So when the public hears that, it almost sounds as though what the Russians are doing are more sophisticated, widespread, covert than what China's doing.

**Bill Evanina** [00:28:07] First of all, I concur with the statement. Secondly, I think we see what we've seen Russia change its tactics and procedures, '16 to '20, has been what you referenced in there in Director Wray's comments and what we've put out publicly in our statement to the American people. The change is that the Russians are no longer using their own mostly proxies and bots and troll farms because they got caught. They're now taking U.S. citizens' information and it and they are taking it and amplifying it. Right. So they know no longer need to do their own work. They could do U.S. citizens' work, American public work, amplify that, which those folks are protected by the First Amendment. So makes it very difficult for law enforcement, the FBI and the intelligence community to not only identify it, but then maybe look at it from an efficacy perspective, and then circle that back to Russia or some other country. It's a very unique problem we have. That's germane to be an amazing democracy with awesome amendment rights.

**Mark Albert** [00:29:01] You're saying the Russians are taking what Americans are saying, that could be false, misleading, disinformation and amplifying that?

**Bill Evanina** [00:29:07] That's correct. Not just the Russians, so are the Chinese and the Iranians.

**Mark Albert** [00:29:11] They're taking our own messages?

**Bill Evanina** [00:29:13] They're they're all they've all learned from what happened with the Russia investigations in '16 and said, hey, we don't need to have our own troll farms and bots, we can use Americans and amplify their messages. True or false, disinformation or true, and amplify what suits their means geopolitically.

**Mark Albert** [00:29:28] So amplify false statements like mail in ballots, fraud being found all over the place. Unsolicited mail in ballot scam is a major threat to our democracy. Large numbers of missing ballots and fraud, mail drop boxes, voter security disaster. They make it possible for a person to vote multiple times. 2020 will be the most inaccurate and fraudulent election in history. All those false statements made by the president of the United States.

**Bill Evanina** [00:29:53] Is your question? Yes. All three countries are amplifying messages they see are germane through geopolitically. If they see a reference made by the president of the United States, a prominent U.S. senator, a business person, someone who America looks at as a voice of reason, and they believe it suits their interests, they will amplify that by a thousand to make sure that the most amount of people see it.

**Mark Albert** [00:30:14] So Americans shouldn't be tweeting or saying false statements that could be used by the Russians.

**Bill Evanina** [00:30:18] Yeah, I think well your point before was that Americans need to find out where to get the most accurate information for their purposes as they determine who they want to vote for. And I think when you it can't be the cable news outlets, it can't be what you see in the newspapers. It has to be an opportunity at the local level to identify where that. And I think this is really important when it comes to Election Day. Election Day, there's going to be a lot of activity. There's gonna be a lot of true information, a lot of false information. I think those American voters who could leave their house to go vote have to have a plan. Where are they going to identify the information they need to make their decision?

**Mark Albert** [00:30:52] Right. And you've used the phrase reliable sources many times. I just read you a bunch of statements from the president of the United States. They're all false. So it does not sound like the president of the United States is a reliable source.

**Bill Evanina** [00:31:03] So when you say false, here's my perspective from an intelligence professional as someone who's in charge of counter intelligence. The hard part we have in democracy is identifying truisms. You know who is the truth police, who is not the truth police. How is it are we able to say this person said that, this person is false? What we do is drive, in my world, drive intelligence to policymakers, not only to the President, but to the DHS and FBI so they can help mitigate this process. It gets really complicated when we as Americans have to draw lines as to what's believable, not believable. And who determines what's true and what's what's not.

**Mark Albert** [00:31:35] I understand, sir, but these statements have all been rated false by fact checkers, local, state election officials. It's just not true that we have mass fraud. It's just not true.

**Bill Evanina** [00:31:45] So I think Director Wray referenced the fraud perspective in his hearing. I can tell you from an intelligence perspective, we have not identified any foreign actors manipulating or attempting to manipulate any mail by vote systems or processes here in the US. However, we have seen all three of those big actors try and influence those issues and amplify divisive messages put forth by Americans to include the president.

**Mark Albert** [00:32:10] To be fair, you have not seen any intelligence that foreign countries are mailing in false or manipulated absentee ballots.

**Bill Evanina** [00:32:20] That's true. However, we have seen those same countries significantly utilize disinformation and influence campaigns to exacerbate these conversations we're having in America about main in voting. It's (unintelligible) for them to utilize what we talked about before, their efforts in US citizens.

**Mark Albert** [00:32:36] So wouldn't we deprive them of ammunition if we didn't say things that were false?

**Bill Evanina** [00:32:40] I think as Americans, we have to understand what makes us great as America is our biggest vulnerability.

**Mark Albert** [00:32:46] Free speech.

**Bill Evanina** [00:32:47] Free speech. And to me, we should embrace that. And I think this is an opportunity where, if I'll be honest with you, as Americans, I think we can learn from this election cycle, that not only are we all in this together, but as a civic society, our whole society is going to be accountable for all this, to include the media, to include the the administration, Congress, all the way down to the high school level students. We are all going to have to find a way to get through this and understand the difference between influence and disinformation and interference.

**Mark Albert** [00:33:13] OK, you mentioned you mentioned truth and what's true and what's not true. And so I just want to mention one other thing and we'll move on.

**Bill Evanina** [00:33:18] Sure.

**Mark Albert** [00:33:20] You've said that Russia seeks to destroy America and is a threat and isn't in interfering. The intelligence have said way back in January of 2017, that was their joint assessment. The Mueller report found that, indicted, twelve intelligence agencies, intelligence agents for Russia's GRU, 13 Russians and Russian companies. The bipartisan Republican-led Senate Intelligence Committee has issued five volumes on this report. And yet we still have the President saying, September 25th in Miami, it was a whole conspiracy. September 18th, I think we have a bigger problem with China than we have with Russia. September 16th, White House, as far as China's concerned, and Russia. And they say North Korea. They say Iran. They say places. Who knows? Who knows? Do you know?

**Bill Evanina** [00:34:09] I stand by all those intelligence community assessments you referenced before, as well as the one done by Congress.

**Mark Albert** [00:34:14] So those were not hoaxes.

**Bill Evanina** [00:34:15] They were great reports done by a lot of great people going back to 2017. Again, I think everyone wants to be like juxtapose investigations and capabilities and statements against the President. And I just think that's probably not healthy for America to do that.

**Mark Albert** [00:34:27] No and I think that people at home are saying, what is true? And when you say use reliable sources, the FBI and DHS has issued six bulletins in the last 12 days referencing people to use reliable sources. They want the President of the United States to be a reliable source. And if America's fighting, disinformation, misinformation, does it really help when the leader of our country is not always saying the truth?

**Bill Evanina** [00:34:54] That's a good question, Mark. I always I always go back to the basics of what makes our democracy great. And I would say it's institutions. So I would I would tell your viewers two things. When the FBI and the DHS put out joint bulletins about the threat of vulnerability, it is what it is. Take it for for what it is, and it's true. When you have a bipartisan report, that's pretty strong, right? If you have a report that's from one side or the other, I'd be a little skeptical because it's going to fall on political lines. But any bipartisan report, I'm a big believer in. We work with both oversight committees in Congress that are and we try and facilitate bipartisan messaging. I think that's where the value add is when it comes to Congress, is the bipartisan work. And there's been some great bipartisan work the last few years. So I would say that's what we should stick with. But when you see multiple agencies putting out statements together, that's got value.

**Mark Albert** [00:35:40] So you're saying the American people should trust the intelligence agencies?

**Bill Evanina** [00:35:43] I think the American people should trust where they (unintelligible) go institutions. Right. You might be upset about the FBI, the CIA, NSA, for whatever reason. But when the government organizations put out bulletins and statements, if you can't trust them, then what are you going to trust in a democracy in 2020?

**Mark Albert** [00:35:59] Right, and conspiracy theories can undermine that trust.

**Bill Evanina** [00:36:01] Conspiracty theory is a big part of our society. And I would say they're a symptom of having an awesome democracy.

**Mark Albert** [00:36:09] Let's talk about a couple of specific intelligence bulletins. ABC News reported the DHS withheld the July intelligence bulletin that called out Russia's attack on Biden's mental health. Is that true?

**Bill Evanina** [00:36:22] I'm not familiar with the ins and out of that case.

**Mark Albert** [00:36:23] [00:36:23]Have you ever been told by a political appointee or the White House to withhold intelligence from the public? [4.9s]

**Bill Evanina** [00:36:29] [00:36:29]Unequivocally, no. [0.5s]

**Mark Albert** [00:36:30] [00:36:30]Have you ever been told by a political appointee or the White House to change a finding? [4.3s]

**Bill Evanina** [00:36:34] [00:36:34]Unequivocally, no. [0.5s]

**Mark Albert** [00:36:36] [00:36:36]OK. [0.0s]

**Bill Evanina** [00:36:37] [00:36:37]I've got 31 years in the government. Twenty four years in the intelligence community. What I have right now is my integrity. And what I'm going to leave with is my integrity. [5.8s]

**Mark Albert** [00:36:44] [00:36:44]Would you quit if someone asked you to change findings? [1.7s]

**Bill Evanina** [00:36:46] [00:36:46]Absolutely. [0.0s]

**Mark Albert** [00:36:46] [00:36:46]You would quit if the White House, a political appointee, your boss, the director of national intelligence, the President asked you to change an intelligence finding? [7.1s]

**Bill Evanina** [00:36:54] If I believed it to be not true or not worth the value, absolutely, I would quit that day.

**Mark Albert** [00:36:58] Let's talk about another issue that came up here with the Director of National Intelligence, information given to the chairman of the Senate Judiciary Committee, Lindsey Graham. This caused a controversy last week. I'm hoping that you can address it, talking about the FBI handling of the Crossfire Hurricane investigation in 2016. The DNI sent out information to Chairman Grassley talking about Russian intelligence analysis about Hillary Clinton four years after that presidential race. I'm wondering whether that was something that you recommended against doing.

**Bill Evanina** [00:37:35] I gotta tell you, honestly, I haven't been really up to speed on that. I wasn't part of that process. So I really would be probably ill-advised to comment on any of that.

**Mark Albert** [00:37:42] So you were not involved at all?

**Bill Evanina** [00:37:44] No, sir.

**Mark Albert** [00:37:44] And I ask because Reuters is reporting that the CIA chief, the NSA chief, both opposed the release of that information.

**Bill Evanina** [00:37:50] I could just say from my perspective, I'm not familiar with that.

**Mark Albert** [00:37:52] OK. Let me ask you a broader question. We're here at the Kiplinger Research Library at the D.C. History Center. So let's talk about history. Countries have tried to influence Americans for as long as the country's been around. Lawfare points out that a French agent tried to sway the 1796, 1796 election to Thomas Jefferson. So where does the Russian interference in 2016 and 2020 fall in the sweep of U.S. history? Is there a precedence for what they're doing?

**Bill Evanina** [00:38:27] So I can answer this, I guess my opinion is, as the head of counterintelligence for America, I think the changes. And I'll proffer first by saying the Russian ideology, with respect to psychological operations and information influence is nothing new. What's changed is the format for which they utilize it. And I would also say with China and Iran, other countries, our social media platforms and our ability to communicate as society has exacerbated to a point where there's so much information, there's so many ways to get it. As a government it's hard to control on the defensive side, the offensive side. And I've got to be careful here because we live in a glass house. It works both ways. So with the social media influx, the ability to have encrypted point-to-point communications, Twitter, Facebook, the social media worlds of YouTube, it's become problematic. And it's no longer spy versus spy. These venues are all used by intelligence services around the world to garner influence and recruit. We just reduced we just released a movie last week called Never Night, which really identified the capability of a Chinese intelligence service to recruit Americans and people around the world with social media websites and chat forums. It's phenomenal.  But it just shows the vulnerability, as Americans of Western society that we have. Our best part of our society and democracy is our humungous vulnerability.

**Mark Albert** [00:39:47] Can I just focus on something you mentioned there? And I want to make sure that I'm reading between the lines correctly here. Are you talking about encrypted chat forums, whether it be  iMessage, Signal, any of these? Are you saying that those are hampering your efforts to protect Americans from foreign influence operations?

**Bill Evanina** [00:40:04] Well, if you want to play in that specific, from from I'd say any government's ability to understand foreign influence and disinformation, you need to know the vector for which it's being utilized. Without any optic to end an encryption or a lot of the social media, we have no idea. And I'll very clear the American people, the U.S. government does not monitor social media. So whether it be on Twitter or Facebook...

**Mark Albert** [00:40:26] Well but sometimes they do. For example, the protests we've heard about DHS and others monitoring posts and organizations.

**Bill Evanina** [00:40:33] I think that's a media thing. The U.S. government doesn't have the. The only way the U.S. Government can monitor a social media account if someone is under investigation and the FBI has a case, an individual, that person's social media can be monitored. Otherwise, no U.S. person could have their social media monitored.

**Mark Albert** [00:40:50] So you're saying you're not aware of anybody in the U.S. government monitoring social media accounts, to focus on the George Floyd protests or any controversy for elections?

**Bill Evanina** [00:40:59] That's correct. What I can tell you, though, our partnership with those social media companies has never been better than it is today. So if the FBI or DHS or CIA or NSA or any other organization has information of a nefarious ability from foreign nation states overseas, they notify the social media companies to mitigate them at their level, not with the U.S. government.

**Mark Albert** [00:41:19] Are the social media companies doing enough?

**Bill Evanina** [00:41:20] They are. The I think the FBI and DHS will tell you they have an amazing partnership, collaboration with with both of, I'd say, all the social media companies in the elections space right now to be able to protect our elections.

**Mark Albert** [00:41:33] Because you've been very clear in this interview about the need to combat disinformation and misinformation and using reliable sources. You know, Twitter today as as we're talking has said they are considering stronger notifications when a tweet has misinformation. Right now, there is a label with their time of changing the color, making it more pointed as to what the information is. So I'm surprised a little bit that you would say that you do think they're doing enough. A lot of people would disagree with you.

**Bill Evanina** [00:42:01] Well, people don't know. Right. So obviously, a lot of this happens behind the scenes. I think we try and protect social media companies as best we can. They're global companies and we don't want them to be accused of helping U.S. government in any way. That's not germane to lawful law enforcement purposes. But I can't tell you that you've seen a lot of these examples have been public recently about social media companies taking down sites or accounts. I think the American public is numb to that. It's a small little paragraph, but it happens every day. But there's a lot happening behind the scenes. The American people will not know because it's classified or happens around the globe. And I think the American people should be really confident that the partnership, as tenuous as it is with the U.S. government and social media sites, is as productive as it can be right now. We didn't have any partnership in 2016 at all in this venue with elections.

**Mark Albert** [00:42:51] Give us an example of something we don't know about on a partnership.

**Bill Evanina** [00:42:55] [00:42:55]So hypothetically, we see activity overseas in a foreign nation state where they are manipulating a thousand, 1500 accounts here in the U.S. on a on a known social media platform. We identify that through collection. We bring that in. We notify the FBI. The FBI notified that company. The company takes those sites down immediately. [18.3s]

**Mark Albert** [00:43:14] [00:43:14]When was the last time that happened? [0.8s]

**Bill Evanina** [00:43:17] [00:43:17]Probably last week. [0.0s]

**Mark Albert** [00:43:17] [00:43:17]And who was that? [0.2s]

**Bill Evanina** [00:43:19] [00:43:19]Classified. [0.0s]

**Mark Albert** [00:43:19] [00:43:19]Classified. [0.0s]

**Bill Evanina** [00:43:20] But I think that's the point, is that the United States government as an organization is has been steadfast and really unprecedented. And our partnership with the social media companies to protect our democracy has also been steadfast.

**Mark Albert** [00:43:32] [00:43:32]It is National Cyber Security Awareness Month. And as we sit here doing this interview, there is a congressional hearing underway called combating misinformation in the 2020 election. You've briefed Congress. What have you told them about misinformation and disinformation in the presidential election? [14.4s]

**Bill Evanina** [00:43:48] We told them a lot of really complicated things and I would say complicated is the real, real important word here, because it's complicated. So when we see disinformation and influence, two separate things with very the same church, so to speak, different view. Disinformation is also, you know, I would say brokering in false information, the brokering of that, and to be able to mass produce that at scale, utilizing vectors, whether it be the social media, the news media, cable news networks, it doesn't make a difference. That becomes pervasive and it's hard to control. Once that ball gets moving with the disinformation activity, it's hard to slow down and counteract because it's already. We need to stop it before it left the boom. So we're trying to do more of that overseas where it starts, before it gets here. Because like I mentioned before, we see our adversaries right now utilizing U.S. based disinformation campaigns. Whether it be, you know, conspiracy theorists or legitimate folks who have wrong information. They get amplified consistently. We try and stop that before it happens.

**Mark Albert** [00:44:43] So you've told Congress about these complicated items that are going on. What else have you told them about domestically?

**Bill Evanina** [00:44:50] So we. So that's a great question. So I'm gonna tell you we brief Congress on these issues. I bring with me or the DNI brings with him the FBI, DHS, Department of Justice, NSA, Cybercom, the ODNI, we have the entire government apparatus there to provide not only the threat vectors, but what we're doing to mitigate these issues and allow congressional leaders to ask questions in return. So the entire body of government work is there to answer those questions. It's been very productive. At times you've seen, sometimes there's, you know, I think the political spin of all of it. But I would say the government and the Congress has been interlocked significantly the last four months to be able to provide threat warning.

**Mark Albert** [00:45:29] Well, if it's very productive, why do you stop doing it for all members?

**Bill Evanina** [00:45:32] We haven't stopped doing it. Last week, we briefed the Gang of Eight, PSCI and SSCI. So the two oversight committees and intelligence.

**Mark Albert** [00:45:38] [00:45:38]Right. But correct me if I'm wrong, but your boss, the director of National Intelligence, there was a controversy a couple weeks ago. He ended all-member briefings and then agreed to continue it for the top intelligence lawmakers, etc. But those areas where you say it's so vital for the Q and A, that's what members of Congress said they wanted to preserve. [16.5s]

**Bill Evanina** [00:45:56] [00:45:56]So I can tell you the reality of all this, is that subsequent to that memo, I don't think the DNI did say that. But I can tell you, we did brief the Gang of Eight. We did brief the Senate Select Committee Intelligence, the House Select Committee

Intelligence. We provided a very, very classified document for all members of Congress to read when they choose to do so. [17.5s]

**Mark Albert** [00:46:14] [00:46:14]And what was the title of that document? [1.2s]

**Bill Evanina** [00:46:16] [00:46:16]I can't say because it's very classified. It's on election security. [3.1s]

**Mark Albert** [00:46:19] [00:46:19]On election security. And when did you present that? [2.0s]

**Bill Evanina** [00:46:22] [00:46:22]Probably about a week ago. [0.2s]

**Mark Albert** [00:46:23] [00:46:23]And what was the reaction? [0.4s]

**Bill Evanina** [00:46:26] [00:46:26]The reaction continues. Members of Congress, at their own volition and time, can go read this in a very classified room, and they can provide questions back to us. [8.0s]

**Mark Albert** [00:46:35] And some of the members of Congress have been very clear that, just as you've said, the Q&A is so valuable. That's why we're doing this interview, because a Q&A is so much more valuable than a written statement. Are there any plans before the election to do an all-member briefing where any member can have that give and take with you?

**Bill Evanina** [00:46:50] No. So what we did historically. I can tell you I did invite the whole team down. We briefed maybe 80 percent of the house and probably 90 percent of the Senate, probably two months ago. We've done this before, and we provided updated briefings the last couple of weeks.

**Mark Albert** [00:47:03] But  those will not occur again, before Election Day?

**Bill Evanina** [00:47:05] No, because Congress is out. Right. So we actually go the end of September was the last time. And right now, they're working covid bills there. Right now, the Senate and House aren't there. So our updates will be in writing and on special occasions from between now and election. They're all out back campaigning and doing the election stuff in their home districts.

**Mark Albert** [00:47:22] Right. And the Senate will be back, though, in two weeks for the confirmation hearing of a Supreme Court justice.

**Bill Evanina** [00:47:26] Right.

**Mark Albert** [00:47:26] So just be clear, there are no planned all-member intelligence briefings about election security between now and election day.

**Bill Evanina** [00:47:32] That's correct.

**Mark Albert** [00:47:33] OK. Is that a mistake?

**Bill Evanina** [00:47:34] No, I think but the Senate knows and the leaders know and the leaders of both houses know that if we have information that's germane that they need to hear about it, we would convene immediately.

**Mark Albert** [00:47:43] OK. Speaking of Congress and lawmakers, we talked about this briefly earlier. You are briefing campaigns. You are briefing candidates. Are they taking the threat seriously?

**Bill Evanina** [00:47:52] They are. I think the...

**Mark Albert** [00:47:53] Better than 2016?

**Bill Evanina** [00:47:54] We didn't do it in 2016.

**Mark Albert** [00:47:56] But are they taking a threat more seriously than in 2016?

**Bill Evanina** [00:47:58] [00:47:58]Yes, I would say both campaigns and the RNC, DNC have taken the threats very seriously and they'd done mitigation aspects that I think are above and beyond that we expected them to do. I think they've listened very well. They push back at times. It's been a very interactive discussion. [14.7s]

**Mark Albert** [00:48:13] [00:48:13]What do they push back on? [0.8s]

**Bill Evanina** [00:48:15] [00:48:15]Just knowing the threat and information, where we got it. But we give them top secret briefings. So they they all get the same briefing. So we brief the Biden campaign, the Trump campaign, the RNC, the DNC, they all get the exact same top secret brief. [12.1s]

**Mark Albert** [00:48:28] Have you briefed Joe Biden?

**Bill Evanina** [00:48:29] I have not.

**Mark Albert** [00:48:30] Do you have plans to do that between now and Election Day?

**Bill Evanina** [00:48:32] Other people are briefing Joe Biden. If Mr. Biden wants a briefing on intelligence related threats we would give it to him. But his entire team gets briefed.

**Mark Albert** [00:48:39] But are is there any plans to give Joe Biden, who could be the next president, he's got a 50/50 chance, a briefing from you specifically?

**Bill Evanina** [00:48:46] If he wanted one, he would get one, yes.

**Mark Albert** [00:48:48] Are you going to offer one?

**Bill Evanina** [00:48:50] Their campaign has been offered. It's rare that the actual candidate gets briefed. I know Vice President Biden and Vice President elect Kamala Harris has been getting threat briefs by the ODNI intelligence community on a regular basis. So that's occurring as we speak.

**Mark Albert** [00:49:06] OK, but to be clear, you're not personally going to be...

**Bill Evanina** [00:49:08] That's correct.

**Mark Albert** [00:49:09] OK. Let me ask you about a couple of things in the news for election security. [00:49:14]Florida's voter registration site crashed yesterday, the last day of voter registration in that state. It's now being extended an extra day by the governor because of that. Any intelligence that this was some sort of an attack? [11.0s]

**Bill Evanina** [00:49:26] [00:49:26]No, but you bring up a very good point. One of our biggest concerns are issues like this. And if we have them at scale -- four, five, six, seven of them -- as we get close to the election, proving the negative is going to be hard. And how do we get to a solution and mitigation without chaos, right? That's going to be what we talked about, the partnership between the patient public, the media, who's willing to understand how the government's working. And sometimes it's just an I.T. overload, sometimes it's a ransomware, sometimes it's nefarious activity. But it's going to take time to get there. We have to have a plan. But I will tell you, in Florida, in 59 other states, the amount of resiliency, redundancy that's been put in place since 2016 is astronomical. [37.0s]

**Mark Albert** [00:50:04] These Albert sensors that are now monitoring the server traffic, all kinds of different methods that have been added. Let me ask you another Florida question, if I could.

**Bill Evanina** [00:50:11] [00:50:11]Sure. [0.0s]

**Mark Albert** [00:50:11] [00:50:11]Two counties in Florida, Washington and St. Lucie, got a lot of attention after 2016. Bob Woodward's new book said that the Russians were able to plant malware on both of those county registration systems. Is that malware still there? [11.8s]

**Bill Evanina** [00:50:24] [00:50:24]That's a good question. I don't know. I'd have to direct that question towards the counties. And it would be DHS and FBI who would mitigate those. I would highly doubt it. [6.7s]

**Mark Albert** [00:50:31] [00:50:31]The counties aren't talking, but -- [0.7s]

**Bill Evanina** [00:50:31] [00:50:31]I would I would highly doubt it. [1.6s] I think, again, I'll point to the the hard work and effort DHS has done to form amazing partnerships with the secretaries of state and all the county and local officials to build redundancy, resiliency so that we have backup. So we now have 92 plus percent of every village going to have a paper about backup. That's outstanding for the American voter to know that. Secondarily, DHS and the partnership locally has never been better than it is right now, and I'm very confident at the government, at the local level and at a federal level, we've done everything we can to provide the voter with confidence that your vote will count if you vote.

**Mark Albert** [00:51:08] I want to ask very delicately worded question here [00:51:11]next: Have you seen any intelligence that any foreign actor has placed malware on any election infrastructure this year? [10.3s]

**Bill Evanina** [00:51:22] [00:51:22]No. [0.0s]

**Mark Albert** [00:51:22] [00:51:22]At all? [1.2s]

**Bill Evanina** [00:51:23] [00:51:23]I have not. Nope. [0.9s]

**Mark Albert** [00:51:24] That's good news, isn't it?

**Bill Evanina** [00:51:25] For me, it's great news.

**Mark Albert** [00:51:28] Let's talk about Election Day itself, OK? The FBI says it's going to stand up election operations on the day of the election. DHS has announced a plan to run a war room for a week around the elections. What will the U.S. intelligence agencies be doing on Election Day?

**Bill Evanina** [00:51:41] We will participate in both those. We will have (unintelligible) at both of those to be there onsite and provide system access back to all the agencies that collect information, the intelligence community writ large around the globe. We'll be working 24/7 the day before Election Day through probably three or four days after the election.

**Mark Albert** [00:51:57] And our cameras are allowed in?

**Bill Evanina** [00:51:58] Around the globe.

**Mark Albert** [00:51:59] Around the globe. And our cameras are allowed into your collaborations, right?

**Bill Evanina** [00:52:02] Of course. Of course.

**Mark Albert** [00:52:03] What will you personally be doing on election day?

**Bill Evanina** [00:52:04] That's a great question. I think I'll be in the Caribbean? No, I'm going to be working in our office trying to maintain my role as quarterback here, to be able to facilitate any guidance I can to the agencies that are involved, but also be the quarterback of where do we go, how do we get the quickest, most effective and truthful information at the beck and call when it happens? I have no doubt that like '16 and '18, things are going to come up eight o'clock in the morning, Election Day, and carry through all the way through night. We have to be nimble and agile to provide quick and accurate information to the media and to the potential victims. What's real, what's not real, to carry on, so we can instill voter confidence.

**Mark Albert** [00:52:42] Do you have the resources you need to be nimble?

**Bill Evanina** [00:52:45] We do. We do.

**Mark Albert** [00:52:46] You have the staff, you have the money, you have the resources, the equipment?

**Bill Evanina** [00:52:48] We do, because most of this effort, Mark, is going to be at the very local level. Our job, my job particularly would be to be that quarterback, that aggregate of information across the intelligence community.

**Mark Albert** [00:52:58] Chris Krebs, who you know well, the director of...

**Bill Evanina** [00:53:00] Good friend of mine.

**Mark Albert** [00:53:00] Yep. The director of the Cyber Security Infrastructure Security Agency. He said this in testimony to Congress on May 1st, quote, in 2016, One of the biggest challenges as we engage state and local election officials is the initial disbelief that they were on the frontlines of a nation-state attack. That a state in the Midwest may be a target of the Russian GRU. We have to get past this. Have we?

**Bill Evanina** [00:53:25] We have. Successfully. I got to give Director Krebs, a lot of credit, for the wherewithall to be aggressive in the last four years in this effort. We, we the government, and I would say primarily Chris Krebs and DHS and CISA has an amazing relationship with all 50 secretaries of state. We have brought them in. Chris Krebs has had multiple tabletops and briefings. My organization, intelligence community have provided four classified briefings to every one of the secretaries of state, and the vendors who provide election platforms, to provide them classified briefings of what the intent and capability of our adversaries are. So, they can't be in the position to be unknowing what the capabilities are of our adversaries. And I think that relationship goes to the success, goes to CISA, Chris Krebs, for the pushing of that and getting the states to understand that this is a partnership, and it's not the U.S. government trying to come and take, take over. I'm really proud of the work DHS has done this in the space state.

**Mark Albert** [00:54:17] Yes, state and local officials are very sensitive to the feds coming in. And that's why it was a big controversy when it was deemed essential infrastructure and all that. And so, they're going to hear your words.

**Bill Evanina** [00:54:26] And DHS has provided services for every single county out there if they so need some.

**Mark Albert** [00:54:31] I want to wrap up here with some more news of the day. We talked at the very beginning about COVID-19 and misinformation around that. Axios is reporting today that misinformation about President Trump's coronavirus diagnosis has, quote, swarmed social media and the broader Web with bogus claims that the president's faking it, that it's a plot, that national work, China engineered the virus, et cetera. Do you believe that misinformation, disinformation about the president's COVID-19 diagnosis is a national security threat?

**Bill Evanina** [00:55:03] I wouldn't go so far as to say it's a national security threat, but it does impact the elections and it does have impact of our American ethos because we see all three nation-state threat actors have already been playing in this COVID world since March. This only exacerbates their ability to do so at scale. And we do expect, and we have seen, we'll continue to see more aggressive activity from our adversaries on the President with respect to his COVID situation. So that is a problem for us on a national security level level. But I'm not sure it's a national security threat. I think corralling the information, providing the American people the truthful scenario is critical so that our foreign adversaries don't extrapolate wrong information.

**Mark Albert** [00:55:42] What does that mean? That you expect to see more aggressive steps?

**Bill Evanina** [00:55:46] I think it's an open wound for our adversaries to utilize not only the COVID, because they've been they've been in the COVID space disinformation since March. But now that the president has been diagnosed, it provides them an opportunity, to again, not only enhance, exacerbate and amplify messages on both sides, to the premise

of your question, we'll see adversaries use both sides of those questions to cause more turmoil in the news cycle for sure.

**Mark Albert** [00:56:11] An open wound that in some cases Americans created for themselves?

**Bill Evanina** [00:56:14] Well again, I'm gonna go back to the American creation of some of these wounds is, is a symptom of our awesome democracy. And I think we in the government have to do a much better job, Mark, of educating America, what that looks like, right. What does it looks like to have a vibrant democracy and at the same time understand the vulnerabilities of democracy. Not only in cyber, academia, collaboration, however serious, use our awesomeness of a democracy against us. The First Amendment is an amazing thing. Probably one the most effective and enduring documents ever written. It's our biggest vulnerability.

**Mark Albert** [00:56:48] You're saying that Americans aren't aware of how easily they can be duped?

**Bill Evanina** [00:56:51] They're not. And I think the government needs do a much better job of explaining what that looks like and feels like when they see it. And we're not there yet, Mark. We're not there yet.

**Mark Albert** [00:56:57] How does your agency do a better job doing that?

**Bill Evanina** [00:57:00] Well, we we are out there. Again, I think the U.S. government doesn't have an information and sales and marketing team, right? So we do the best we can. NCSC's been out. We've reached out to probably 14,000 CEOs last year. Bunch of associations on the cyber issue, the Chinese Economic...

**Mark Albert** [00:57:16] Pre-COVID.

**Bill Evanina** [00:57:17] Pre-COVID. Under COVID we've sent out seven bullitins out of our shop, on COVID, to hospitals, hospital associations, PPE supply chain threats, to make the Americans aware of not only the information, I would say void the disinformation, but the supply chain devaluation that China has produced, subsequent to COVID, right. So they're in a geo-political war right now with us. And this goes as well for the vaccine. That is something Americans need to understand so that we could show them more effectively what disinformation and influence is so they could identify it much more effectively.

**Mark Albert** [00:57:51] If we don't get a vaccine until the end of this year or early next year, whenever it happens to be, and then you've got the distribution. This situation, the COVID pandemic, is going to be here for quite some time, many more months. Do I hear you saying that you do expect more foreign influence operations around COVID-19 in the coming months?

**Bill Evanina** [00:58:08] Oh absolutely. Not only in the disinformation perspective, but I'll ask your viewers to be patient with the COVID vaccine. This (unintelligible) we're talking about a vaccine to prevent Americans and people around the world to potentially not get a virus that's killed 210,000 people. We need to do this right. We need to do this effectively and secure no matter how long it takes to get it done. We're not going to be like Russia and say, I got a vaccine and we're going to share it on people. We're going to make sure that we do it right, because there's geopolitical, economic and medical reasons for us

doing it right. I have all the confidence, so we'll be first to get it. But once we get it, and we have it, we have a supply chain to protect. We have the manufacturing, the storing, the distribution, the making of the glass vials, all the way to innoculation. We have to protect that ecosystem of supply chain from our adversaries who will for no doubt, no doubt, be trying to penetrate that.

**Mark Albert** [00:58:58] So you call for Americans to be patient with the elections. You're calling for Americans to be patient on a vaccine. And yet your boss's boss, the President, has promised it by Election Day. It doesn't sound like he's being very patient.

**Bill Evanina** [00:59:10] Well, I don't know. Again, you're talking to a guy who doesn't follow a lot of social media. But I can I can tell you that I think there's two things in my perspective that intelligence official. Number one is when we create the vaccine, we'll be first. But secondarily, from that point to inoculation of 300 million doses is a long way. In my world, in counter intelligence, is to counter the intelligence apparatus of our foreign nations to a that are trying to prevent us from obtaining the vaccine first. But once we do, they're going to surely prevent us from trying to get it into your arm.

**Mark Albert** [00:59:40] Who's trying to prevent us from getting the vaccine?

**Bill Evanina** [00:59:42] I would probably say that, for sure, China, Russia and Iran, same three actors, are trying to prevent us from getting the vaccine. Mostly China, Iran, were in the competitive nature on the world right now to produce the vaccine. Russia has said publicly they have the vaccine. You know, I'm not sure, when I saw yesterday or today that 50 percent of the Russian populous don't believe it. So I'm not sure how they're going to be able to drive that in a global market. But what America has is resiliency and a history providing amazing vaccines around the world. And I think that will carry us through the day.

**Mark Albert** [01:00:13] So just to be clear, you're saying they're trying in China and Iran, lesser extent, Russia, trying to stop America from getting a vaccine or trying to steal any vaccine that America may create?

**Bill Evanina** [01:00:23] That as well. So, we've seen multiple attempts at that. But I will say also, we have what's called Operation Warp Speed, which is a government private sector endeavor to protect the vaccine that we're making in research and development from the theft ravaged areas, mostly China. At the end of the day, once we create it, we obtain it, protect the supply chain of that until we get all the way to your arm and my arm.

**Mark Albert** [01:00:44] So you've had intelligence cross your desk about foreign countries trying to either steal, disrupt, or prevent us from getting a coronavirus vaccine.

**Bill Evanina** [01:00:52] All three.

**Mark Albert** [01:00:53] All three?

**Bill Evanina** [01:00:54] All three.

**Mark Albert** [01:00:55] And have you taken offensive action?

**Bill Evanina** [01:00:56] Absolutely.

**Mark Albert** [01:00:57] To stop that?

**Bill Evanina** [01:00:58] Absolutely. And defensive action.

**Mark Albert** [01:00:58] Like what?

**Bill Evanina** [01:00:59] So let me give you..

**Mark Albert** [01:01:00] Like what?

**Bill Evanina** [01:01:01] Well, again, some of that's classified. But let me give you a metaphor. I think it's really important for your viewers to understand I personally link this COVID vaccine to building of a modern day weapon system. If we're building a modern day weapon system right now - Department of Defense, Department of Energy, we have an ecosystem that's prepared to protect that from a counterintelligence effort against our adversaries. It's done in silos. It's done in secret with people who have top secret clearances, who have fences and guards and have cyber capabilities, defenses. That's not the case in biopharma right now. That's not the case in the research and development organizations who are working with the government to build a vaccine. They don't have that Department of Defense protective ecosystem. We're trying to now hurry up and protect. At the same time, let biopharma know, you're a target. They're like, wait, we're a target? Yes, you are a target. So there's an education. And there's a hurry up to protect those entities because we need to look at this vaccine as a weapon system to protect it. This is something, again, geopolitically, economically and medically, will be a humungous event the next five years, and around the world.

**Mark Albert** [01:02:10] And specifically, what are you doing to hurry up and protect those biopharmaceutical companies?

**Bill Evanina** [01:02:14] One, that's classified. But a lot of it starts in my organization with education to the CEOs, the board of directors, the chief security officers, the CISOs. Here's how you can be attacked. Here's the cyber activity you're going to see. Here's a human enabled activity you're going to see. Some of it's the FBI working. And we're doing surveillance. We're doing overseas surveillance. We're identifying nefarious actors around the world who are trying to penetrate this vaccine and our manufacturing. We're trying to stop it before it occurs.

**Mark Albert** [01:02:41] So just like on the election security, that you're giving intel to DHS and FBI, are you giving intel that you're getting to these biopharmaceutical companies?

**Bill Evanina** [01:02:48] We are, via the Department of Defense, U.S. Army, HHS, FDA and the FBI are all working in partnership with these biopharma companies who are on the front lines producing, who don't have the defensive mechanisms in place that the military apparatus would have. So we are a little bit behind. So we have to play catch up. And I think the President mentioned it. Many members bipartisan on the Hill had said we need to be first in this vaccine, but we need to do it right and safe and that it's secured.

**Mark Albert** [01:03:16] When was the last time you shared intelligence about this with the pharmaceutical companies?

**Bill Evanina** [01:03:21] Me personally?

**Mark Albert** [01:03:22] Your agency.

**Bill Evanina** [01:03:23] I say that U.S. government? Yesterday.

**Mark Albert** [01:03:25] Yesterday?

**Bill Evanina** [01:03:26] Yesterday.

**Mark Albert** [01:03:27] You shared information as recently as 24 hours ago?

**Bill Evanina** [01:03:30] That's correct. It's constant. It's enduring. We have subgroups that are in place. I would give credit to the Department of Defense, Department of the Army and HHS for Operation Warp Speed. They have a humungous body of people, of men and women who are in this business process to do this. We just provided advice and counsel to them, provide some strategic guidance. But they're the women and men on the front lines protecting this event. And it's really impressive to see every day.

**Mark Albert** [01:03:54] Sir, thank you so much for your time. Is there anything on election security, or COVID, or any classified information that I have not asked you about that you'd like to share?

**Bill Evanina** [01:04:01] Well Mark, I think it's nice that you ask. I will say to the American people, if there's one thing you can do to escape the noise, understand the influence, you as the American voter are the one that they're trying to influence. The best way we can get out of this dilemma that we're in is for you to be an educated voter and vote. Your vote with confidence is what we're going to need as Americans to show adversaries that we decide who elected officials are, not disinformation influence or another country overseas. So go out and vote with confidence.

**Mark Albert** [01:04:32] You're saying vote an educated vote?

**Bill Evanina** [01:04:34] An educated vote. Don't fall victim of the noise. Know who you want to vote for. Plan. Prepare how you're going to vote, in person or via mail-in vote. Have a process. Be patient. And as you vote on Election Day, or if you've already voted, just know they we're probably not going to have a president identified on November 3rd. Be patient. But most importantly, vote. I think I saw recently that in 2016, less than 65 percent of the eligible American voters voted. Can you imagine how awesome this country would be if even 80 percent of our eligible voters vote? I'm saying to the American people, be educated and use your voice to go out and vote and you choose who our next the president is.

**Mark Albert** [01:05:13] Sir, thank you very much for your time.

**Bill Evanina** [01:05:15] You're welcome Mark. Pleasure to be here.

---

## INTERVIEW 2
## Bill Evanina Full Interview Transcript
## Recorded Oct 6, 2020
## National Mall, Washington, D.C.

**Mark Albert** [00:00:01] Sir, what is the number one threat to our elections?

**Bill Evanina** [00:00:08] Public confidence. I would say that we have to make sure that we do everything as a nation, as a government to ensure the confidence of the American voter. The American ethos is there that confidence in our systems, our infrastructure and the way that we vote is there. I think if we can overcome the American voters' confidence, we'll win.

**Mark Albert** [00:00:27] Are foreign countries trying to shake our confidence in our election?

**Bill Evanina** [00:00:30] They are. They're using aggressive forms of disinformation and influence to influence the voter. At the end of the day, their goal is to influence the voters with respect to where they want their geopolitical goals to be. And I think the voters need to understand, they're the ones being influenced, not institutions or not organizations.

**Mark Albert** [00:00:47] When you look at all the countries trying to influence Americans, whether it be China, Russia, Iran, combined, is the effort to influence the vote greater than in 2016?

**Bill Evanina** [00:00:59] I'm not sure we could put a value on that. It's hard. So I think if you're looking back on 2016, it's really hard to quantify the efficacy of the event. So I think it's hard for us to still measure the influence factor. So I don't know if we can say that. We can say there's more countries involved now than there was in '16. In 2016 we had one country involved, Russia. Now we have at least three. So I would say it's a three-fold increase of influence.

**Mark Albert** [00:01:23] At least three countries, but as we talked about in our interviews, there are other countries who are trying to influence what Americans think.

**Bill Evanina** [00:01:31] Correct. So if you look at, say, Cuba or Venezuela, they both have Venezuelan-Americans, Cuban-Americans that are here, that they believe can make an influence to sway the election one way or another albeit in Florida or some other state. So they also have a geopolitical interest in the election as well.

**Mark Albert** [00:01:48] Right. So a lot of Cubans live in the Miami area. Miami is a huge battleground state every year.

**Bill Evanina** [00:01:54] So just imagine if you are the Cuban government and you want to influence your diaspora in Miami, in South Florida, what impact can that have from an influence perspective on who they choose to vote for on Election Day? [interview stops for lawn mower]

**Mark Albert** We have less than four weeks before Election Day. What does the final sprint look like for you and the intelligence agencies?

**Bill Evanina** [00:02:39] Great question. I think the sprint from the intelligence agencies is to make sure that we're crossing every T and dotting every I with actionable, real time intelligence that we can provide to the FBI and DHS. And then from DHS to provide it to the state and local officials to potentially thwart any activity we see by nefarious actors. So I think effectiveness, efficiency at scale right now, moving forward, and be prepared for anything.

**Mark Albert** [00:03:05] In other words, you can't sit on a piece of an intelligence or you don't have the luxury of three weeks to figure out if it's actual or not. You have to do something right away.

**Bill Evanina** [00:03:14] That's correct. And I would say is very analogous to the counterterrorism threat. We have to look at these threats as they are, how they will affect America if they end up happening. What have we done? How do we stop? How we plan to mitigate it? Have we done everything in our power to provide the information for those who would mitigate it? Have we done that due diligence? I think that's a question we ask ourselves everyday around the world. Are we doing enough to help the FBI and DHS do their job?

**Mark Albert** [00:03:38] November 4th is too late.

**Bill Evanina** [00:03:40] November 4th is too late. But also say November 4th, I look at it as half as halftime. So I think what we have to be a patient country, a patient voter, that the election probably won't be decided at midnight on November 3rd. So we have to be patient as a nation to say, we might not have a winner until the 5th or 6th, depending on how the mail-in votes get counted. So let's be patient as a nation. The same time the intelligence community is working around the globe to identify potential nefarious activity the same time. What we don't know is what we don't know. So we are digging through those files to identify potential actions from adversaries. Every every minute of the day.

**Mark Albert** [00:04:16] So adversaries overseas or here at home could use that period after Election Day, but before the results are known, to try and divide us even more.

**Bill Evanina** [00:04:26] Absolutely. And I think we look at all the realms of possibility from nefarious activities. We have table talks consistently in the government. What could happen? What am I to look at? We look at what the Russians did in Ukraine in 2014, changing their election results, from the state to the cable news stations. Everything that touches the Internet is vulnerable. And we have to make sure that we are on top of that before we get to November 3rd.

**Mark Albert** [00:04:48] And correct me if I'm wrong, but I thought I saw that an FBI SSCI bulletin just a couple days ago did say that while someone may be able to hack in and change the results on a secretary of state Web site or something else, those are unofficial results. They can't physically change the official results on a wide scale.

**Bill Evanina** [00:05:03] Correct certification process is resilient, redundant and set forth by the Constitution. That will be the ultimate factor in any state when they certify the results. But also the resiliency, redundancy that we see at each state level is unparalleled and a precedent that we've not seen 2018 or 2016. So I think no matter where you live as an American voter, you can have confidence that your local officials are ready for this activity.

**Mark Albert** [00:05:28] My final question, sir. You have a ton on your plate. You rarely give interviews. Why did you give this one?

**Bill Evanina** [00:05:34] I think this is an opportunity for the U.S. government, the intelligence community, which rarely does provide information to the American public, an opportunity for them to understand that the United States government writ large is working very hard for you, the American voter, to protect our election. And further so that our democracy, your men and women around the world are working day and night, to protect

America, and also our elections, so that we can have elections moving forward and continue to be the greatest democracy ever invented.

###