Hudson Institute

Dialogues on American Foreign Policy and World Affairs: Director of National Intelligence Dan Coats and Walter Russell Mead

Hudson Institute, Washington D.C. Headquarters
1201 Pennsylvania Avenue, N.W., Suite 400
Washington, DC 20004
July 13th, 2018

TRANSCRIPT

Please note: This transcript is based off a recording and mistranslations may appear in text. A video of the event is available: https://www.hudson.org/events/1576-dialogues-on-american-foreign-policy-and-world-affairs-director-of-national-intelligence-dan-coats-and-walter-russell-mead72018

KENNETH WEINSTEIN: I'm Ken Weinstein, president and CEO of Hudson Institute. Hudson is a policy research organization dedicated to U.S. international leadership and global engagement for a secure, free and prosperous future. I'd like to welcome our present audience as well as our C-SPAN viewing audience. And I'm truly honored to welcome a remarkable public servant and a truly good friend of Hudson Institute to be with us this afternoon, Director of National Intelligence Dan Coats. Of course, Dan Coats served with great distinction as a member of the House and Senate from Indiana, as well as the U.S. ambassador to Germany. During a long career in public service, as he told me as we were coming up here today, he has twice failed retirement – once returning to the U.S. Senate for a second time in the Senate after his term as ambassador to Germany and then becoming a director of National Intelligence. He's had a long and distinguished career in public service. He's focused both on domestic policy reform – coming up with what eventually became the compassionate conservatism agenda – and on defense and national security issues. And I mentioned he is a good friend of Hudson Institute. Before he left for Germany as ambassador, he and his wife Marsha transferred the governance of their foundation, the Foundation for American Renewal, to Hudson Institute.

Now in the Trump administration, Dan Coats has been entrusted with a job with deep responsibilities and immense challenges. The director of national intelligence serves as the head of the U.S. intelligence community, overseeing and directing the implementation of the national intelligence program and acting as the principal adviser to the president of the National Security Council and the Homeland Security Council for intelligence matters related to national security. When he and the president are both in town, he does the presidential daily intelligence brief with senior members of the intelligence community.

As I mentioned earlier, we are truly honored to have him with us today. He has chosen Hudson as the venue to make remarks on a number of critical issues – including Russian cybersecurity in the U.S. and abroad – and to do so on the eve of the historic summit in Helsinki between President Trump and Vladimir Putin.

So the order of the business today will be that Director Coats will offer remarks from the podium. Then he will engage in a discussion with Hudson Institute Distinguished Fellow Walter Russell Mead. Walter also needs no introduction here. Walter's the dean of observers of U.S. foreign policy. In addition to being a distinguished fellow at Hudson Institute, he's the "Global View" columnist for *The Wall Street Journal*. And he is also the James Case professor of international affairs at Bard College. So without any further ado, let me welcome Director Coats to the Hudson Institute podium.

(APPLAUSE)

DAN COATS: Ken, thank you very much. It's nice to be here at Hudson. We enjoyed Hudson's presence in Indiana for a time. Then former OMB Director Mitch Daniels became governor of Indiana – in the meantime, lured Hudson to come to the middle of the country to get a different perspective perhaps than what we get from the coast. You were there for a number of years. I had the privilege of working with people there. We understand why you came back here, moving it to more foreign policy-focused stuff. And a lot of that is what happens here. But we do appreciate the fact that you still value Indiana. Some of your employees might be missing the ease of living and cost of living in Indiana relative to Washington – not to mention the commute to work. But nevertheless, it's very nice for me to be able to be here with you to lay some groundwork for what I think is one of – if not the – top challenge that we face in terms of threats to our country, to our people and our processes in the future.

So before I sit down with Walter to talk about a range of global threats that we face, I'd like to focus my initial remarks on the growing cyber threat to our nation's security. And specifically, I'd like to put the current cyber threat in terms of the threats that we've had in a historical context and to define who is most responsible and what are they attempting to do, and then discuss the intelligence community's response to that. So each morning when I get up, I'm given a roundtable of news on what happened while I was asleep, or what happened yesterday around the world. And almost without fail, the longest section of this news roundup is the section on cyber issues, which details multiple reports of cyberattacks and alerts. This issue affects all of us. And it is increasingly affecting numerous aspects of our daily life, as many of you are familiar with.

You only need to go back less than two decades ago to put, I think, the current cyber threat into its proper context. In 2001, our vulnerability was heightened because of the stovepipe approach of our intelligence and law enforcement communities that produced what they called "silos of information." At the time, intelligence and law enforcement communities were identifying alarming activities that suggested that an attack was potentially coming to the United States. It was in the months prior to September 2001 when, according to then CIA Director George Tenet, the system was blinking red. And here we are nearly two decades later, and I'm here to say the warning lights are blinking red again. Today, the digital infrastructure that serves this country is literally under attack.

Every day, foreign actors – the worst offenders being Russia, China, Iran and North Korea – are penetrating our digital infrastructure and conducting a range of cyber intrusions and attacks against targets in the United States. The targets range

from U.S. businesses to the federal government (including our military), to state and local governments, to academic and financial institutions and elements of our critical infrastructure – just to name a few. The attacks come in different forms. Some are tailored to achieve very tactical goals while others are implemented for strategic purpose, including the possibility of a crippling cyberattack against our critical infrastructure.

All of these disparate efforts share a common purpose: to exploit America's openness in order to undermine our long-term competitive advantage.

In regards to the state actions, Russia has been the most aggressive foreign actor – no question. And they continue their efforts to undermine our democracy. In regards to the upcoming midterm elections, I think there may have been some confusion between what we are seeing now compared to what we saw in 2016. As the Department of Homeland Security noted, we are not yet seeing the kind of electoral interference in specific states and voter databases that we experienced in 2016. However, we fully realize that we are just one click of the keyboard away from a similar situation repeating itself. Therefore, and moreover, we are seeing aggressive attempts to manipulate social media and to spread propaganda focused on hot-button issues that are intended to exacerbate socio-political divisions. Despite public statements by the Kremlin to the contrary, we continue to see individuals affiliated with the St. Petersburg-based Internet Research Agency creating new social media accounts, masquerading as Americans, and then using these accounts to draw attention to divisive issues. We have learned, just before this meeting, about the indictment of 12 Russian military intelligence officials relative to their role in 2016.

But focusing on the potential impact of these actions on our midterm elections misses the more important point: these actions are persistent, they are pervasive, and they are meant to undermine America's democracy on a daily basis, regardless of whether it is election time or not. Russian actors and others are exploring vulnerabilities in our critical infrastructure as well. The DHS and FBI – in coordination with international partners – have detected Russian government actors targeting government and businesses in the energy, nuclear, water, aviation and critical manufacturing sectors.

The warning signs are there, the system is blinking, and that is why I believe we are at a critical point. Today, unlike the status of our intelligence community in 2001, we're much more integrated and much better at sharing information between agencies. But the evolving cyber threat is illuminating new daily challenges in how we treat information. We are dealing with information silos of a different kind, including between the public and private sector.

But here's the good news. As I just mentioned – but it needs to be stated again – the intelligence community today is more integrated than it's ever been. We are sharing information across agencies at all levels. In regard to the midterms, we are partnering with DHS and FBI to provide support, information and grants to state election officials from all 50 states. We will continue to look for opportunities to support this effort. And regarding the larger cyber threat issue, the president has signed an executive order strengthening the cybersecurity of federal networks and critical infrastructure, in which the president tasked a whole-of-government risk management review resulting in a number of actions that OMB is now taking to strengthen U.S. networks with IT modernizing guidelines. The president has also authorized the use of all available tools of state power – including attribution, criminal indictments and economic levers – to punish malicious cyber actors. Our leaders at the National Security Council consider this as a top priority. And we are continuously pursuing actions on this issue. As you know, we're in a transition period with the NSC, but I have had numerous talks with our new national security adviser and members of the NSC about the importance of raising this to a top issue, and they're doing so. Within the government, we're working continuously to detect, warn and – when necessary – respond to cyber threats. We have a multi-agency Cyber Threat Intelligence Integration Center that builds understanding of cyber threats to inform decision-makers. The Department of Homeland Security and the FBI are demonstrating leadership on the foreign influence threat and applying a more assertive federal response, as we have just seen today. And my former colleagues in the House and the Senate are bringing significant attention to the threat from cyber and have expressed strong support for legislative action.

Having said that, we have to do better in what we deliver to our customers: how we get it to them and the speed by which they receive it. Today, those crosscutting cyber threats have been illuminated – but how rigidly we still act when it comes to public discourse. Respective self-interests of the government, the private sector and the public have created independence rather than complimentary lines of effort and awareness. As a result, we need to think differently about our customers.

In many ways, the nature of the cyber threat requires that we – the national security community – treat the private sector and American people as intelligence customers. And that is why you will see us talking about this threat more vocally, and why you will continue to see us publish unclassified assessments and statements to inform the American people.

Everyone, if we are to succeed in dealing with this threat, we must take ownership of the challenge. It will take the government, the private sector and the American people all doing their part to better position our country for the future. As a government, we are having a more open dialogue about this threat. In particular, we in the IC need to provide the information available to us to the private sector and to the public to better inform their decision-making. And we need the private sector to

see the public good in developing greater protections in the software, information systems and applications on the market. We also need the American people to verify the credibility of the sources of information upon which they base their decisions. Whether those sources are social media reports, cable news or newspapers, it is essential that we all apply critical thinking to all sources of information. This evolution in the IC's approach is part of the transformation which we're driving within the ODNI and throughout the IC in coming years. We have brought together experts and leaders from across the intelligence community to take stock of where we are and what we must do to reach the next level of effectiveness.

The result of this effort, which brought together the heads and deputies of all the intelligence community agencies – all 17 of them – is a new vision for the future of the intelligence community. We call it Intelligence Community 2025. Where do we need to be? What kind of capabilities do we need to have? What kind of insights do we need to have in terms of the threats that we face? And we are putting together significant efforts to stay ahead of the game and ahead of the curve, to be able to deliver to our customers, starting with the president, working through his policymakers, working through the agencies, and working through the American public with both the private and the government sector. So with that, at this particular time I would like to thank you for the invitation. I know that we'll have a good discussion with Walter Russell Mead about this. We can look at the larger threats or whatever questions that need to be addressed. And I would much rather do that than continue to talk up here, even though, as a former senator, we love to talk.

(LAUGHTER)

COATS: So thank you very much.

(APPLAUSE)

WALTER RUSSELL MEAD: Well, I have to say that's one of the most dramatic comparisons I've heard a senior government official make: saying that the warning indicators now are comparable to what they were in the months leading up to 9/11. It's a different threat, but it's there. And presumably, we're looking at anything from major attacks on infrastructure to massive attacks on the sort of electronic communications and all.

COATS: We are. And, you know, it's not just from the four nation-states that I identified earlier. We see this from criminal organizations that are using cyber for nefarious purposes. We see this from nonstate actors, from terrorist groups, and from criminal groups. We see this from hackers around the world who see this as a game or, just for the hell of it, want to take something down: break into the defense community or break into Wall Street. Anon is kids in the basement or sitting in a dorm. It is pervasive.

But of course the real threats – the sophisticated threats – come from the states which have the capabilities and the resources to be able to create really great damage.

MEAD: So in your view, there is still a very significant gap between the capabilities of these states and of the various criminal, terrorist and other organizations that are out there?

COATS: Well, in terms of having the resources to continue to develop the new tools, or having the ability to adapt or the agility to up their game. In a sense, it's a game of whack-a-mole or chess, where you see a threat and then you put in a prevention. And then the threat moves over from here to there. You try stop it there, try to get over here. And you see that across the board. And so it's a 24/7, 365-day effort in terms of protecting your people.

MEAD: You know, when you read the news and listen to what people say on television, it's one story after another of one sensitive American database getting – you know – some of the real crown jewels of our community. First, that makes me wonder: how defenseless are we, and is it going to change? But it also makes me wonder: are we getting some of this stuff ourselves and not talking about all of our successes? Or is the cyber universe simply a story of American secrets being stolen on a mass basis?

COATS: Oh, it's broader than that. But we've got capabilities. Significant capabilities. I've been to a number of our cyber operations centers. We have the resources. We have the capabilities. I don't think anybody's better than we are. Nevertheless, the range of vulnerabilities is out there because the technology is advancing so rapidly. And as I said, this is game of chess, where we make a move to protect ourselves or to identify, and then they make a move to go around. We have to be aware of that, and never be complacent about what we have now, because there are people out there trying to jump over us.

MEAD: It does seem like a domain where the offense seems to enjoy benefits over the defense. Is that...

COATS: Yeah. That's been frustrating for me because I've got a lifetime of watching NFL football games – of going to prevent defense in the last part of the game. You know, you've got a field goal and you're up on point. You go in to prevent defense,

and it opens up all kinds of holes. And the next thing you know, the other team kicks the field goal to win. It's so frustrating if you just rely on defense to win.

MEAD: Right.

COATS: And so that's why I have, when I was in the Senate – of course my job is different now because I don't do policy – but I continue to support and encourage an offensive capability. If anybody knows what punch back is more than Donald Trump, we need to approach punch back in the right way. If we're going to send the right signal to people, it's the signal that there is a price to pay: if you come after us, there will be a price to pay. The less you do of that, the more people are encouraged to say, "I've got nothing to lose." So I think combining offensive measures with defensive measures is necessary to deal with this issue.

MEAD: It's interesting to think the Constitution does expressly provide for letters of mark and reprisal.

COATS: It does.

MEAD: Perhaps in the cyber seas there's something we can do. Of the four countries that you mentioned – Russia, China, North Korea and Iran – were you giving them to us in the order of their capabilities?

COATS: Yeah, but maybe from different perspectives. China has capabilities and resources that perhaps Russia doesn't have. But they don't have the same intent. What's serious about the Russians is their intent. They have capabilities, but it's their intent to undermine our basic values, undermine democracy, create wedges between us and our allies that is serious. And we've seen this. In fact, the indictment today shows exactly what they're trying to do – or what they've done – through their military intelligence relative to elections. And we see – as I mentioned in my statement – their ongoing efforts. It's a strategy. So the intent that comes out of Russia is different than the intent of China, which wants to steal our stuff. They want to build...

MEAD: Technology, the intellectual property...

COATS: Absolutely. Intellectual property, technology – they want to try to change our vision of China in its intentions, but not through the same kind of means that the Russians use. So you have to put those two in context.

Now, Iran and North Korea. With North Korea, we're not at a pause, but we're at a point where let's see where these negotiations go relative to our relationship with North Korea. And with Iran, I mean, they did just take all kinds of malicious activities against us in ballistic missiles from ceding terrorism and, you know, on and on. But on cyber they potentially are somewhat limited because their economy is not doing well. They may be spread too thin or whatever. So probably in that order. But, you know, the top two – Russia and China – are out there every day.

MEAD: Speaking of North Korea, in cyber and in other things, have you observed any difference in North Korea's behavior since the Singapore summit?

COATS: Well, obviously I can't get into the classified parts of what we see. It's always been a hard target. We have significantly upped our game for this purpose. Reagan was trust and verify. That's what I came to Congress with. And right now I'm the verify guy. IC is the verify community. So we are focusing on what was happening both before and what is now happening subsequent to the talks. But we're at the beginning of this, and we'll continue to evaluate it. Obviously, North Korea is probably, you know, trying to figure out. I mean, we're at the beginning of negotiations. So I'm just not going to give up the ship right now. So we'll see how that plays out. But I think it's too early to determine exactly definitively that, you know, this is where they're going to end up or be there halfway through or...

MEAD: So no really dramatic, telling shift either way.

COATS: Nothing either way of it. There's been some reporting. Some of it has not been accurate, but some of it has been accurate. There are some continuing activities, but some of those that have been reported have not been verified.

MEAD: Let's get back to the election and disinformation operations. It seems to me that social media is one of the places – at least if we look at 2016 – where disinformation was very accurate. Is that still the case now?

COATS: Yes, very much so. I think I noted that in my remarks. The exploitation of social media is prevailing, increasing and very sophisticated. Who would have thought that ISIS – using the 7th-century barbarian measures of imposing physical harm and death on people – would also be so sophisticated in using cyber early on and social media early on to recruit, to train and still inspire? The defeat in the desert has not resulted in the defeat of terrorist organizations like ISIS and al-Qaeda. We see

them spread around the world, and they still remain a terrorist threat to us. And social media is one of the ways in which they continue to raise money, recruit, train, and inspire. And we have to be aware of that.

MEAD: And when you go to social media companies, and you say, "Your platform is being targeted and used in a very, very specific way by these different hostile groups," do you get the cooperation that you think you need from these companies?

COATS: We have the obligation to learn and warn, and we do. We are in the process of working with social media companies in terms of taking responsibility for what they put out. We've had some successes, but we've also had some interactions which haven't been as successful as we would like. We are going to continue to do that. But there's a lot of brand protection. There's a lot of, "Well, listen, if we do that and our competitors don't, then we're at a disadvantage." We try to talk about the responsibility relative to their commitment to help us address these threats and keep our people safe.

MEAD: So there's a real range of responses…

COATS: There's a range of responses.

MEAD: …from pretty solidly positive to, "Well, I don't think we can help each other."

COATS: Either way, what's interesting to me is that we only collect against foreign intelligence. And so we know a lot less about the American people than our adversaries do. And we know a lot less than some of our social media outlets know about their customers. So I guess somewhat of a…

MEAD: So Google knows us better than the federal government.

COATS: Oh, absolutely.

MEAD: You know, in a way, I feel good. In a way, I feel bad. I'm not quite sure how I feel about that (laughter).

COATS: (Laughter).

MEAD: You were saying that they're trying to polarize us and magnify differences. This reminds me a bit of what the communists used to do during the Cold War, and the Soviet Union's key propaganda technique. I think maybe some of the younger members of our audience may not know what this is all about, if you could explain it a…

COATS: Well, when the wall came down, you know, we thought, "OK, I mean, this is going to be a new Russia" –, a so-called reset. And for a period of time, it was a different relationship. Then Russia reached out and said, "You know, maybe we've gone too far. Why don't we ask the guy who ran the KBG? He's a pretty savvy guy. He's been listening to Americans all his life – or adversaries and so forth – and conducting everything that the KGB did and still does, just under a different acronym." And that was a game changer. So I describe it as the Russian bear after the fall of the wall went into the cave into hibernation. Now he's out of the cave, and he's hungry and clawing for more territory and more influence, and using the same tactics that we saw in the Cold War and more. And the "more" results in a lot of that in cyber.

MEAD: It's interesting that, during the Cold War, they had the advantage of communist parties and networks of supporters around the world. They don't quite have that anymore, although they seem to be trying to rebuild loyal parties and factions. But it looks like, on balance, with the cyber tools they have they can actually do a better job than the Soviet Union could this kind of disinformation, or black propaganda.

COATS: They're really good at lying, deceit, deception, seeding – subtly seeding and not so subtly seeding – this dissension among adversaries. You know, the president made some comments about NATO. And his closing comments were ones I really thought were important, because if NATO comes unglued, Putin wins. And he sees that. He's trying to seize that potential opportunity. And I think we need to stand up against it.

MEAD: Right. And so the pattern is not so much that the Russians are supporting one side or another in a political battle – though sometimes they may do that – but that they're trying to get both sides madder and more divided. Is this part of the method?

COATS: Well, whether that's their method or not, that's what they succeeded in doing. It certainly was designed as a strategy. And they've had some success, unfortunately.

MEAD: What can we do to counter this?

COATS: Transparency. I've talked to my colleagues in different nations, particularly in Europe. The more we provide our people with what we know the Russians are doing, the more we can inform our public not to just believe and take for granted that what is put out in the media is truth. We need more critical thinking, I think. And we're barraged by media: by breaking news, by news outlets rushing to be the first, "Because if we don't do it, three others are going to do it. And our ratings will go down, and their ratings will go up." And so there's no filter between information that comes into the system. There's no editor as we used to have in the paper. There's nobody sitting in an office upstairs saying, "We got to run this by the boss before we print it. It's going to be too late if we do that because we want the news now. We want to access it, you know, on our iPhones right away." And so we have to inform our people: don't just believe everything that you hear out there. I mean, we are agencies that seek the truth. We can't shade it. We can't politicize it. The truth is what it is. It's just the facts. And I think our public needs to gain some ability to ask questions and seek verification before we jump to conclusions and rush to the camera to say, "I just heard this and wow," and then the next day, on page 13, "Well, that was not exactly what should have been."

MEAD: So if you had a chance to speak with Mr. Putin at this sort of crucial period in U.S.-Russian relations, what's your message at President Putin?

COATS: Well, my message would be: "We know what you're doing. And we know you know what you're doing and what we are doing. And so look: if your goal is to strengthen Russia in the proper way, we can cooperate with you. But if your goal is to strengthen Russia at the cost to us, if you're going to be a paranoid nation thinking that, you know, anytime in the next 24 hours, we're going to take over Russia – you have this paranoia about democracy –, then we're not going to get anywhere. Isn't it best for both sides here to basically say, 'Instead of taking down, why don't we build up?' But, you know, President Putin, the decision's up to you. We know you run the shop. We know you're making the decisions. You can't pass it off to, oh, that's some hacker down somewhere where we don't know. We know what you do. And so you make that choice. But if you want to stay in this tit for tat, we're going to beat you."

MEAD: OK.

COATS: And that's Ronald Reagan basically, saying, "Hey, you want to take us on? OK. We'll throw everything we got into it. You throw everything you got into it. Then you make a decision." And Russians made a decision: "They outdid us." We have the capacity to do that.

MEAD: To get from the sort of disinformation and political sphere to think more about the elections that are coming up, you know, you hear a lot of anxiety about American elections – whether it's voting machines or other elements of the voting process in the midterms. How confident can we be that we're defending the security of our political system?

COATS: We have to be confident, because if you don't have confidence when you walk into the poll and put your X on the candidate or the party that you want to support – if that becomes in question, it undermines our democracy.

MEAD: Which sounds like somebody's strategic goal, possibly: to do exactly that.

COATS: Yeah. So we have to make every effort. I tried to outline some of the efforts that we are making on that. It has to be solid: all 50 states. Look at what happened down in Florida, in one area of one county: hanging chads. That threw us into a constitutional crisis. (laughter) Think of what can happen today, if we find out that one state that might have been the critical state of the electoral vote.

MEAD: Control of the Senate or of the House or something, depending.

COATS: Exactly. Exactly. We're not looking at presidential here, but we will be starting the day after the election, unfortunately. So we have to put in everything we can, and we are. We've talked to all 50 state election officials, all 50 state governors and officers. We're providing grants. We're looking at those who provide the machines. We're trying to back it up with paper so that we have redundancy on it. And we just need to throw everything at it to assure the American people we're doing everything possible to make it a fair election not managed or massaged by anybody from the outside.

MEAD: And as you look at the progress we're making and the obstacles that remain, do you feel that on the whole we're on track to have a safe and secure election this fall?

COATS: I think that. You see it in a bipartisan way in the House and Senate. We see the executive branch stepping up big time. We see the states being warned now and reaching out for help. We have to do everything we can to assure our public that their vote counts.

MEAD: There've been some reports of different independent groups monitoring states' readiness for the election and there seemed to be a wide gap. Some states were looking pretty good, and some other states – including the state of the hanging chad – seemed to be a bit behind.

(LAUGHTER)

COATS: Got to get them up to date before the election.

MEAD: Right.

COATS: We need to assure the American people that we've worked with all 50 states, and we're ready.

MEAD: Are the laggards doing better at this point?

COATS: I think they are. I think nobody wants to be the one that takes it down because they didn't have their act together. We're hearing that. As I said: we have worked with them, the FBI has, we've worked with DHS, our intelligence community has, for warnings and so forth. And we've worked with all 50 states and it's ongoing. It's going to have to keep being ongoing right up to day of the election.

MEAD: And from what you're hearing back from Congress and others, is your sense that, on a bipartisan basis, people in Washington think that the work that you guys are doing is sufficient and proper?

COATS: I think we're seeing that. The Republicans are teaming up with Democrats both in the Senate and in the House to ensure that everybody's on board.

MEAD: Because this would certainly be a key. If one party or the other party said they're not doing the right thing, that would be a terrible...

COATS: Well, you know, we've been witnessing this on another subject, and we've seen the impact of it.

MEAD: Based on the kind of unrivaled exposure you have to the threats that the country faces, what really worries you most when you think about scenarios that might unfold? What are the things that really keep you up at night?

COATS: Well, you...

MEAD: Do you ever sleep?

COATS: (Laughter) Yeah. Restlessly sometimes. There are a couple of things. First, the possession of nuclear weapons of mass destruction by terrorist groups. When you think about 9/11 – two planes flying into the Twin Towers, one plane flying into the Pentagon – if either one of those planes, or if all three of them, had any kind of weapon of mass destruction aboard, we would not be talking about 3,000 deaths. We'd be talking about 300,000 or maybe 3 million or more. So preventing proliferation of weapons of mass destruction – particularly to terrorist groups that are not under any state control, where they have a theology or an ideology where victory is killing the opposition, whether its by beheadings or through a nuclear device – that's one. The second is, frankly, a 9/11 – a cyber 9/11. Think about the grid going down for three days in New England in January: a lot of people are going to suffer and die. Think about taking a hit on the banks that wipes people's lifetime savings out, and we don't know where it came from.

MEAD: Or financial markets, I suppose.

COATS: Yeah. We don't know. We don't know where it came from. We don't know where the money is, and on and on. So you know, you do toss and turn at night about scenarios that you hope will never happen.

MEAD: In your view, is the intelligence community as a whole getting the kind of resources and support that it needs to do the job that needs to be done?

COATS: We are. And thanks to this administration and to the Congress, we have really upped our ante. And we have been provided the resources we need to do what we need to do. And we have some terrific capabilities. We've got some innovative people. We've got some young people. I'm a liberal arts major with a law degree, but, I mean, I should not be in the operational efforts of cyber or technology (laughter). I look at it from a different perspective. Fortunately, we've hired a lot of really capable, smart people – a lot of young people coming on that have technological capabilities, STEM capabilities that, you know, I never even dreamed of. And so every visit I make – and I make a lot of them to our various agencies and their

components – I'm so impressed with the technical capabilities we have. We're an innovative country. Democracy and freedom produces some great stuff if it's done the right way.

MEAD: Well, thank you, Director Coats. I don't know if I should call you "senator" or "ambassador." But "director," I guess, is...

COATS: Dan.

MEAD: ...Probably the best. All right, well, thank you, Dan. The work that you're doing is important. I think everybody here and on television appreciates the importance of what you do and wishes you every possible success.

COATS: Well, Walter, I want to say something. I came across this article a couple days ago about what people are maybe thinking about Donald Trump's unorthodox foreign policy. And it ends with, "We should brace ourselves for a wild ride." Guess who wrote that?

MEAD: I did.

COATS: Walter Russell Mead.

(LAUGHTER)

COATS: *The Wall Street Journal*, a couple of days ago. I highlighted it and cut it out. (laughter) Anyway, thank you. It's a pleasure to be with you and back in Hudson. And...

MEAD: Well, great to be with you.

COATS: ...Thanks for asking me to be here.

MEAD: And I know the director has to get out quickly. As you can imagine, his schedule is packed, so if the audience could sit while he leaves quickly to get on to whatever he's doing next. I don't think he can tell us what he's doing next. But thank you again for coming.

COATS: Thank you.

MEAD: Really appreciate it.

(APPLAUSE)