Hudson Institute

Video Event | Winning the Innovation Race in the Intelligence Community

TRANSCRIPT

- Representative Jim Himes, *U.S. Representative for Connecticut's 4th Congressional District*
- Dr. Dan Patt, *Adjunct Fellow, Center for Defense Concepts and Technology, Hudson Institute*
- Bryan Clark, *Senior Fellow & Director, Center for Defense Concepts and Technology, Hudson Institute*

Disclaimer: This transcript is based off of a recorded video conference and breaks in the stream may have resulted in mistranscriptions in the text.

A video of the event is available: https://www.hudson.org/events/1913-video-event-winning-the-innovation-race-in-the-intelligence-community12021

Bryan Clark:

Welcome to the Hudson Institute. I'm Bryan Clark, a senior fellow at the Hudson Institute and director of Hudson Center for Defense Concepts and Technology. I'm joined today by Dr. Dan Patt, who is an adjunct fellow at the center, and also at the Hudson Institute. Our guest today is Congressman Jim Himes of Connecticut's fourth district. Congressman Himes is a member of the Financial Services Committee, as well as being the Chair of the Strategic Technologies and Advanced Research Subcommittee of the Permanent Select Committee on Intelligence in the House. We're here today to talk primarily about the committee's report from last year, which is "Rightfully Scaled, Carefully Open and Infinitely Agile, Reconfiguring To Win the Innovation Race in the Intelligence Community," which talks about the critical need for new technologies to be developed for today's intelligence community going into the future and some of the risks if we fail to do so.

Congressman Himes is in his sixth term in Congress. And in addition to being the chair of the STAR Subcommittee of the Permanent Select Committee on Intelligence, he is also on the Financial Services Committee. Prior to being in Congress he worked in a nonprofit world at Enterprise Community Partners, as well as being commissioner of the Greenwich Housing Authority and was previous to that a member of Goldman Sachs, where he was for 12 years. But now he's in his sixth term. We appreciate him making the time for us today in what is a very busy set of current events to step back and look into the future and what technology might hold for us in the intelligence community. So thank you for being with us, Congressman Himes.

Rep. Jim Himes:

Thank you, Bryan. Thank you. And a big thanks to the Hudson Institute and Dan for having what I think is a really important conversation.

Bryan Clark:

I appreciate it. So, to jump into the report, Dan and I were extremely impressed with the report and its focus on kind of an ecosystem approach to how do we improve innovation for intelligence. And Dan will talk a little bit about that and ask some questions along those lines. But just kind of in terms of an overview, what are some of the major concerns you have in terms of technology areas that the US might be falling short in when it comes to both observing what our adversaries are doing and also in terms of exploiting technologies for our own intelligence purposes?

Rep. Jim Himes:

Yeah, great question, Bryan. So, there's really two categories of risk associated with the trend that we're in right now. And again, this isn't something on the horizon. This is the world we are in right now. We are in a world now where we're yeah, in general, we are still at the point of the spear on innovation and pretty much all technologies. But for the first time ever, there are a lot of people right next to us. And there are some who are promising to actually get ahead of us. And I want to come back to that framing because one of the conclusions of the report is that thinking about this as a race to be won is not in some respects helpful.

But nonetheless, the point is, and of course the metaphor you use because it's familiar to everybody is imagine if the Manhattan Project hadn't succeeded and the Nazis had beat us to an atom bomb. You can go down that path, and I think that's very real, maybe not quite as dramatic as what could have happened in 1940s. But we don't want the Chinese to develop quantum computing that could break all our encryption, for obvious reasons.

The second category, Bryan, that that may be is less frightening, but is nonetheless discouraging at best is this country is enormously wealthy partly because we've always been at the cutting edge of innovation. And just look at any of the gear you're wearing or using, whether it's the iPhone or the browser you use or Facebook. I understand I probably shouldn't talk about Facebook right now. But my point is that immense wealth has been created in this country by our innovative edge.

Bryan Clark:

Yes, absolutely. A couple of areas I thought were interesting in the report that get talked about a lot, but maybe don't get as much in-depth attention, were quantum computing and artificial intelligence. We hear a lot of discussion about both these areas. You mentioned them yourself in your remarks. How do you think we're faring in terms of developing quantum computing technology? What are some of the areas in quantum computing that you think are going to be the most problematic earliest? Because clearly quantum computing is not a monolith, there's lots of different variations on quantum science. There's computing, there's sensing, there's encryption, there's de-encryption. What areas did you find in the subcommittee that were potentially problematic where we need to carefully examine where we stand relative to an opponent like a China, who's obviously throwing a lot of money at the idea of quantum science?

Rep. Jim Himes:

Yeah, and I'm glad you paired it with artificial intelligence, because in some ways quantum computing and artificial intelligence live on opposite ends of a couple of different important spectrums. And what I mean by that to answer your question is that quantum computing is highly esoteric. The applications are finite. A lot of people wander around thinking that a quantum computer is just a very big, fast, powerful computer. That's actually not true, of course. It blows the doors off traditional binary computing in certain very specific areas. And those very specific areas include, of course and you mentioned it and I mentioned it, the possibility that you could render conventional encryption useless. Okay, well, that doesn't sound scary to the lay person until you understand what that means. It's not just our Chief of Station somewhere communicating top secret stuff. It's also our nuclear command and control. As you might imagine and as you know, that is of course, extraordinarily encrypted. So if encryption goes away, which theoretically we could wake up one day to discover that we keep talking about the Chinese, but there's others have figured out a way to break our encryption. That's a very horrible thing in a very narrow and esoteric area.

Artificial intelligence is on the other end of the spectrum because frankly, it's sort of hard to answer your question because while quantum computing is happening, at least at the forefront, is happening in a couple of very specific places, looking at some very specific technologies with esoteric applications. AI is everything. I mean, it is literally everything. And there are 17-year-old engineers in Hoboken, New Jersey who are working on AI and Lawrence Livermore. It's happening everywhere in a fragmented way. And the applications are literally everything. Now that doesn't mean that we shouldn't focus on it. There's a lot of people. And we tried to steer, Bryan, this very quickly can become a conversation about the military. And of course, there's no bright line between the intelligence community and the military. But when you start thinking about swarms of autonomous drones driven by highly capable artificial intelligence, that's the stuff of which Hollywood thrillers are made.

Bryan Clark:

Yeah, absolutely. And that's what we've found is the same thing about quantum technology, how it is very specifically oriented towards particular applications, at least early on. And most of it is being government funded or private industry with a very specific set of objectives, but it's kind of farther out

in the future. And I think people hear quantum and they think it's going to be near here soon, and it's going to be applicable widely, and that's really not the case. But yeah, AI, so commercial industry is developing a lot of our AI technology, at least in the United States. And that's true to a degree in China. Is there a concern about, about our ability to harness what commercial industry is learning in AI and use it for the government intelligence purposes? We've got organizations like the Algorithmic Warfare Cross-functional Team and DOD that are trying to do this merging of commercial and military technology. Is that a concern that the subcommittee found is that we're not effectively harnessing that private sector effort?

Rep. Jim Himes:

Yeah, I'm not sure I want to say we're not effectively doing it. The reality is that our national security apparatus is on the ball with respect to artificial intelligence. And again, it's sort of hard to say that because it means so much. And by the way, let me just momentarily go back to what you said before, because it's an important theme in the report. So, the Chinese on quantum computing, because it's highly specific, esoteric, in some ways that's what the Chinese are configured to be good at. If you can put a thousand scientists in a room, all with ranks and hierarchy and lots of money, that kind of probably lends itself to solution. AI, of course, is very different on that spectrum as well, because it doesn't lend itself to sort of a hierarchical, regimented innovative context, which of course is where most innovation happens. It's a trope now to say that it's always the misfits and the dropouts who are the innovators. Well, there's something to that.

But anyway, back to your question. The government is doing really a pretty good job at thinking about how artificial intelligence and machine learning can operate in the verticals that people think about. So needless to say, our intelligence collection platforms, while we won't get too specific in how we talk about them, it's not a surprise to anybody to know that they are generating massive, ungodly quantities of data that no group of analysts is going to be able to sift. So, you need, so there's lots of people thinking about that, thinking about things that are a little scary, like facial recognition. It's everywhere. So we're not willing to say that we're doing it wrong. What we say in the report is more that AI, unlike quantum computing, again which is a very esoteric thing, that is going to grow and develop in hierarchical, private sector, heavy universities, and so we better be out there. We just better be out there at every conference. We ought to be taking those scientists out to lunch. We really need to be aggressively in that unbounded ecosystem if we're not going to fall behind.

Bryan Clark:

Yeah. And so I was going to bring that to Dan. So, this ecosystem approach, it was a superb, I think, set of findings as the study had regarding how we can improve in the future. Dan, you want to talk about that?

Dan Patt:

Yeah. I mean, I think you highlighted it. You brought up misfits and dropouts. So often the conventional wisdom only focuses on pouring more money into R and D. And we thought your report highlighting, it's about more than that. It's, sure, money's involved, but it's also about people and it's also about the environment. How did the subcommittee to develop that ecosystem perspective on innovation and realize that you have to look at the help of those inputs to get what we need?

Rep. Jim Himes:

Thank you, Dan, for saying that, and you make it sound like we sort of stumbled upon something dramatic. Look, spend 10 minutes in Boston or in Austin or in Palo Alto and you realize that that innovation does come out of ecosystems and dozens of PhD theses get written on exactly what they should look like because there are a fascinating combination of innovative corporations. I mean, Xerox Park, of course being probably the iconic example of where Xerox, which at the time of course was an iconic corporation just says, "Hey, we're putting a bunch of you misfits and dropouts into a room and giving you a whole bunch of money and come up with cool stuff." And then of course, you've got the proverbial napkin being scribbled on in the coffee shop and the interaction of these people. So this is not a new finding.

The point we tried to make, and both of you have near and dear experience with government, is that those ecosystems, however defined, and they look differently depending on where you are, in some ways are the diametric opposite of where I'm sitting right here. Members of Congress and senators are not your iconoclastic misfits and dropouts. We're people who followed the rules and we went to law school and we tried to get A's and we followed the rules and we love hierarchy. We have chairman. We have vice chairman. We're seniority based. And by the way, we love nothing more than to punish failure. You get reelected when you drag some person who failed in front of your committee and make their day brutal. Well guess what? It turns out that failure, and this is a key part of innovative ecosystems, failure is a critical, maybe even the critical ingredient to learning and innovating. So there is that section in the report where I point at us and say, "Heal thyself," because everything we do here, everything we do here in some ways to a greater or lesser extent cross cuts against that ecosystem.

Dan Patt:

Yeah. Speaking of a fresh look, we found it fascinating that in your report, you recommend changes to the budget and appropriations process to enable more flexibility and responsiveness and resource allocation. What might that look like in practice?

Rep. Jim Himes:

Well, the structural problem is probably easier to solve and there are mechanisms that do that. There are mechanisms that set up long tailed projects with an R and D phase, a proving phase, and then an acquisition phase. They're always at risk, but there are structural mechanisms that I think you can do. And look, I'm a member of Congress and I take seriously that we have absolute control of the purse strings. But we ought to think back to Xerox Park. And the example I just gave there is virtue in taking a group of really smart people and maybe dialing back the oversight a little bit, not a lot, because we're dealing with taxpayer money, but dialing back the oversight a little bit. So we can say, "Hey, you thought this was only going to take a year. It sounds like it's going to take three years. That's okay. Go for it." That's a profoundly unnatural thing for the Congress of the United States to do.

And then there's a harder problem. So the structural stuff, I think we can probably get right if we're thoughtful about it. And by the way, there's a whole other conversation about breaking down jurisdictions and committees this and committees that. Chairman are pissed off about this happening outside of their committee. The harder one is, let me tell you a very quick story. So when I get here in DC, for about a year, we talk about Solyndra. Now Solyndra, as you'll recall of course, was a photo voltaic, solar energy company that the Department of Energy, I believe it was, invested some money in in sort of a VC like way. And the theory was, look, there's going to be some technologies out there that don't get funded by the traditional market, the venture capital market. So, we ought to do that just on the off chance that they turn out to be amazing, but they don't clear the venture capital hurdle rate. Well, when Solyndra went under, we spent a year talking about it and wasn't Barack Obama awful? And

what a horrible, horrible mistake. That's exactly the wrong answer It's exactly the wrong answer. Because in fact, the program that funded Solyndra had a better success rate overall than an awful lot of venture capitalists do. And so that cultural shift of getting people like me and my colleagues to understand that failure is an inevitable part of progress, that's a tough one.

And by the way, it's not just Congress, I should say, and you guys both know this. It's also the bureaucracies. I can't remember who exactly told me, but probably nobody is incentivized to be as conservative, as a Colonel who really wants to get a star. You don't get promoted because you took a swing at a great idea and it didn't work. You get promoted because you keep your head down and do things exactly the way the guy before you did it. And there's some wonderful work happening in the Pentagon where that culture is being turned a little bit, but it's not just the Congress.

Bryan Clark:

Yeah, absolutely. It needs to be bred throughout the military. One thing about that ecosystem approach that I thought was interesting was the report seems to suggest that we need to have a lot more unclassified technology development and interactions with the outside world, particularly in the intelligence community as Dan and I have both experienced. Unless you have the right ticket, you're not having a conversation about a capability they're developing or some findings they've had from technologies that they've applied in the field. And it seems like if we want to have an ecosystem, we've got to think about how to keep the right stuff in the classified world but having a much broader discussion the unclassified world. Is that in fact what the subcommittee was thinking?

Rep. Jim Himes:

Yeah, and there's probably a couple pieces to that. There's so much knowledge and data and stuff that is valuable out there in the unclassified world. The intelligence community, as you know, is really thinking hard about the whole open source world. It's hard to take the CIA where you used to make your career by turning a couple of Soviets to betray their country and say, "Actually, you know what, you can probably get about 80% of what you want just by Googling." That's a big culture shift. So, we do need to sort of really make sure that we are putting an incentive on this new world that we live in. And then of course we need to, and this is the easy half, the easy half is to say, "You guys got to be out there. You got to be hanging out at the conferences, you got to reach out to Tim cook and you name it and build those relationships so that you're having that human interchange that is so important."

The hard part and the other half, the harder part, which the report is very serious about is any venture capitalists will tell you that they invest in people. They say, "Well look. We evaluate the technologies, but we invest in people." And so, we need to take that seriously and say, "How do we get that incredibly patriotic and motivated 35-year-old, who's made a pile of money on some company and really understands this version of AI. How do we get them a clearance super quickly and put them in to one of the national labs or put them into NSA or put them into CIA?" That's the piece that we don't have a tool to do right now. And if we don't fix that, again, I hate the metaphor of the race, but we'll be racing wearing leaden boots or something.

Bryan Clark:

Right. We'll definitely get a hamstring ourselves, which brings up the question and Dan may want to jump in on this, is when you bring that person in, how do you avoid, because I've worked with folks that come in from the venture cap or from the technology world rather. And they come into the Pentagon and they get demoralized very quickly because of the bureaucratic structures, the risk aversion of leadership. Obviously, there's some cultural issues that's going to be hard to work out. But how do you

incentivize the kinds of behaviors that you want the ecosystem to pursue within DOD? I mean, how do you get people to be, or within the intelligence community, to be willing to take those risks and pursue technology developments that may not pay off in their current form, but may pay off down the road. So it seems like there's some incentives that need to be changed or else we'll bring these people in, and they'll just end up being unhappy and go back to the technology world from which they came.

Rep. Jim Himes:

Yeah, no, I think you're absolutely right. And I'm not sure there's a fix to that. If you are used to the free-wheeling very open culture, non-hierarchical of Palo Alto, sitting in the Pentagon is going to be a new experience and probably demoralizing in a lot of ways. And I can't fix that. We can fix it over time as we're thoughtful about this. And there's a lot there. Part of the reason, of course, that the permanent staff, the officers and others may not be open and willing to take risks is the stuff that we've talked about before. But look, nobody wants to look dumb. So, if all of a sudden you're running a project on artificial intelligence and some whiz kid out of Palo Alto shows up and makes you look dumb.

I do suspect that there are fixes to that. And there's certainly no magic bullet. If you look at models of success, what Eric Schmidt did when he was chairing, I believe it was the Defense Intelligence ...

Dan Patt:

Defense Innovation Board.

Rep. Jim Himes:

Exactly, the Defense Innovation Board. I'm sure he was frustrated, but he made a massive contribution. There are people doing that right now at Kessel Run in Boston. And I'm sure they're having rough days, but these are people who say, "You just have to go in with your eyes open." It's like being a member of Congress. If you come to Washington and think that because you've arrived, everything's changing and you're going to drain the swamp and fix healthcare, you're going to have a rough time of bit. It's a lot about knowing the incrementalism, which is sort of an essential part of government.

Bryan Clark:

Right. Right. Well, it's interesting you brought up Kessel Run and you brought up the Defense Innovation Board because in their recommendations, one of the major areas that we've actually seen some effort to take action on is the acquisition of software. And how do we buy software? I mean, so much of the innovation that the report talks about that we know is necessary in the intelligence community depends on software to either support artificial intelligence, to support the adaptation of systems, to be able to deal with new phenomenology they're looking for. So, the Congress put in place a new appropriation for software and a new acquisition process for software. Is that model that's currently being used by DOD, is that something that you're looking at as being applicable more broadly so we can start to enable these smart people like Kessel Run to, this becomes more institutional rather than a bespoke project.

Rep. Jim Himes:

Yeah. No, great question. We really try to emphasize this in the report because sadly the history of software acquisition, not surprisingly, grew out of the history and culture of hardware acquisition. The problem is they're radically different animals. In fact, they're not even animals, right? They're two totally different categories. Software is never done, and the moment software is done, it's obsolete. It is a living organism that needs to, as Kessel Run demonstrates, needs to have constant interaction with the end user, literally constant interaction with the end user to update, not just for security, but for

functionality. And of course, software, you can teach a sailor to drive a ship. But if software is not usable by people, they just won't use it. And so, it's not optional and it is pervasive.

Again, we say this in the report, software is everywhere and everything. There's a great line, software is eating the world. And so, the good news is that particularly inside the Pentagon, there are folks who are cottoning on to that. There's some wonderful literature out there about this, but it remains a huge vulnerability because we're still developing software by saying, "It's going to be done in two years. It's going to look like this. By the way, we're going to spend six months talking to each other about what it looks like. We're not going to actually talk to the people who use it, and then we're going to, if it's on time, we'll pay everybody." No, no, no, no, no, no, no. That may be how you build a firearm, but it is absolutely not how you build software, and you can't change that fast enough. And I would argue that we're not changing it fast enough. We're still holding up these examples inside DOD that are getting it right, but it's still not permeated the whole national security apparatus.

Bryan Clark:

Yeah. Go ahead, Dan.

Dan Patt:

I was going to say, I really resonate with how you frame that and how software needs to be this more fluid development. And I think that also points to, if you want to have this fluid development of these software tools for the intelligence community, you also need access to data. What are your thoughts on sort of making data more accessible within the IC and across different components of the IC?

Rep. Jim Himes:

You sent a shiver down my spine when you said that because when a lot of the American people here making vast swaths of data available to the IC, they get nervous about privacy and civil rights and all that kind of stuff. But you ask a really important question because we don't have a lot of inherent weaknesses relative to the Chinese. If at the end of the day, we've got the ecosystem, we've got the culture, we still have the money, although we really tried to steer away from money as the solution to everything in this report. But we don't have the ready access to data that the Chinese have and will always have. Look when you're in an authoritarian government, there's no debate over whether every citizen in your country's financial records are entirely available to the People's Liberation Army. There's not a debate about that. It happens.

And so that is a weakness that we won't fix because we obviously don't do that. And so we struggle, we really struggle across the national security apparatus with, and for our viewers here who may not be fully cognizant of what AI involves, AI is basically just software that teaches itself by swimming in massive oceans of data. And the more data it has, it's like what we were talking about before software being a living thing, it teaches itself. And the bigger your ocean of data, the more effective the artificial intelligence, the more effective the machine learning is. And so I don't have a good answer. All I can tell you is that we need to acknowledge the fact that that is going to be one weakness relative to authoritarian states that we're probably not likely to solve.

Bryan Clark:

And there's also a concern, I mean our challenge with governance because our data is not always in the right format or in the right set of standards to be easily digested and moved across different uses. So that's something we're going to have to address as well. The other thing that jumped out at us from the report was the emphasis on setting technical standards. This has been mostly a discussion when it

comes to 5g, because that's something people understand and can kind of fixate on. But technical standards kind of pervade scientific and technological world and setting those standards and being involved in establishing them can give you a leg up in terms of implementing a new technology. What did the subcommittee you see as some of the major areas where we need to really buckle down and get more involved in helping set technical standards internationally?

Rep. Jim Himes:

Yeah, as a non-engineer, I don't have a huge amount of insight on that, but yes, that's exactly right. If we are outside of the room when technical standards are set, we will be surprised by some of the things that are in those standards. And it's not just important for our national security. It's important because we are the carriers of the values that we need to permeate the technical world, whether those values are privacy protection of civil liberties, et cetera. So, it's not just important, it's really essential that we be a part of that. And I'm not sure I have anything smart to say beyond that because engineers understand how inside that world that happens.

One thing I do understand better, which is maybe abstracting your question up one level is, and this is why I object or why I'm uncomfortable with the race metaphor that we use so much. We say in the report, and this gets to standards of a different kind, we say in the report, that technological races never stay won. You don't win and it's game over. I mean, it was about 15 minutes after we developed nuclear weaponry that the Soviets did. Not really, but you get my point. And so races don't stay won. So that's not the comfortable end state. The comfortable end state is when you acknowledge that technology disperses. It just does. And you plan for that world by establishing norms and standards for behavior, something we've been doing for hundreds of years in the conventional world, and which we're way behind on now.

And we see this in terms of confusion around the application of the laws of armed conflict in the cyber realm, where we need to do a lot more work. We see this when we wake up and read the headlines that some Chinese scientists has messed with the human germ line and it may be creating an alternate species of humans. Unless we come together, and the wonderful thing is of course, that we have a long tradition of coming together with our adversaries and set some basic standards and norms, which yes, I get it, they'll be ignored just the way the laws of armed conflict are ignored. But unless we do that, we are going to have a lot of really ugly surprises over time.

Bryan Clark:

Yeah, it's a great point is that to deal with technology proliferation we have to turn to this other set of tools. And often the discussion of norms and standards has been kind of left at the ethicists. But it seems like this is something that technologists need to embrace because of this realization that you're never to be going to be able to maintain that edge that allows you to have something that your opponent doesn't have, which is something that the US has gotten used to. So in terms of going forward in terms of implementing some of the report's recommendations, the report came out late last year, what is the subcommittee looking at in terms of an agenda for what are some of the first things you would hope to try to implement through the intelligence community to try to move it closer to this state where they need to be in order to improve their ability to innovate, particularly when it comes to the ecosystem?

Rep. Jim Himes:

Yeah, so I'm really happy to report that we were able to get a number of the recommendations of the report into this IAA that passed a couple of weeks ago, the Intelligence Authorization Act, so we made

some progress there. I'm happy to say that though the report may end up someday on a shelf gathering dust, it did actually have some effect on the IAA. But there is still a lot to do, Bryan, things large and small. So small, well, actually it's not that small, but let me put it in the small category. I got fascinated by the security clearance process, which of course is a big impediment and a big problem with respect to bringing people inside the IC, researchers, academics, entrepreneurs. Though we've made real progress, we are still in the dark ages with respect to being able to do what you do when you're giving somebody a security clearance, which is to identify if they're a risk. I'm not even, and I want to say this with some humility because I'm right in the middle of this talking to the people who do it, but I'm not even sure we're super clear on what the indicators of risk are, and that's critical. Because remember, it was only 30 years ago that if you were gay, you were a national security risk. That was 30 years ago.

And so, if you haven't gotten the sort of data scientist and the psycho analysts and anthropologists in the room to really tell you in an evidence-based way what the risk factors are, you end up running down a lot of rat holes. And the other area, and again, I'm pretty fired up about this, we are still sending guys and raincoats around to interview your college roommate for a security clearance. And it takes that guy in the raincoat 10 years to learn what Facebook and Google know about you right now. And I think, and I say this with some humility, I don't want to denigrate anybody's efforts, but I think we have a lot of work and thinking to do about how we think in 21st century terms about security risks. So, I probably shouldn't have called that small, because that's important.

Then you've got big. How do you fix the turf issues between House Armed Services and the Intelligence Committee and the cyber realm? That's big, that's big. You've got staff who are dug in, who have built careers around what they do, and change is going to comfortable and chairman who love ... that's one that we're just going to need to beat our pick on the rock for a while on.

Bryan Clark:

Yeah, title 10 and title 50 are huge areas of controversy inside DOD and over at Cybercom. And it's getting harder and harder and harder, especially with the idea of a defend forward approach to cyber operations where it's no longer that clean distinction between what's going on in the intelligence gathering or exploitation and what's happening in terms of ops. So, it's admirable that you're trying to tackle that because that's going to be a long-term problem.

Well, thank you very much Congressmen. Before we close, I wanted to make sure we didn't miss something that you wanted to make sure we addressed in terms of the report and what the subcommittee has been doing. But we really appreciate you taking the time today in what is obviously a very busy legislative calendar to be with us.

Rep. Jim Himes:

Yeah. Well thank you very much, Bryan and Dan. I'm just thrilled that the Hudson Institute is helping us get this out there. We covered a lot of ground. The one thing we didn't talk about, maybe I'll just spend 30 seconds on it before I run to the Florida vote. One of the things that report calls for that we didn't spend enough time on is the IC has work to do not just in building relationships with the outside world, with the leaders of social media platform companies, that sort of thing. We have work to do all of us in terms of better explaining the IC to the American people. I've been doing this for a long time and I can't tell you how often, every week somebody comes up to me to tell me that the NSA is listening in on their phone calls or some other Bourne Identity or Hollywood generated fantasy. And people fear things they don't understand. And I'm deeply committed to civil liberties. I'm practically a first amendment absolutist. I'm a pretty progressive Democrat, but the more I've gotten to know the IC, the more I come to understand that that is an institution that is profoundly dedicated to operating inside the law and to staying on the right side of constitutional protections.

And look, I have a master's in Latin American studies. I know the history of Nicaragua and I know the history of Chile. I know that stuff. But today this is an organization, it's a 17-member institution that is really trying very, very hard to do the right thing. And we need to tell that story out there. And look, you may as an American citizen, decide that you don't like what the CIA does. That's fine. I just want you to be informed as to how you arrive at that conclusion. Because if not, suspicion and lack of knowledge drives a desire to somehow not do what Americans have always done, which is support their government. And so anyway, that's the one area that we didn't cover, Bryan, that I just wanted to want to tack on there.

Bryan Clark:

Well, that's an important one to address because clearly there's a lot of suspicion of government. There's a lot of concern about what the government's doing. So, making sure that people understand what the role of the IC is and how it does its job is going to be important going forward and probably get increasingly important. So, Congressman Jim Himes, thank you very much for being with us today. We appreciate you taking time from what's a busy time on the floor to come talk with us. And we will definitely be doing some more research in this area and so we appreciate the subcommittee's efforts in terms of this report on innovation in the intelligence community. So, thank you very much for being with us today.

Rep. Jim Himes:

Thank you. Really appreciate the conversation.