

Center for Strategic and International Studies

Online Event

“Innovation in the Intelligence Community”

RECORDING DATE:

Thursday, October 15, 2020 at 3:00 p.m. EDT

FEATURING:

Representative Jim Himes (D-CT),

Chairman, House Permanent Select Committee on Intelligence Subcommittee on Strategic Technologies and Advanced Research

CSIS EXPERTS:

James Andrew Lewis,

Senior Vice President and Director, Technology Policy Program, CSIS

*Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com*

James Andrew Lewis: I'd like to thank Congressman Jim Himes for taking some time out of his really busy schedule this month on the topic of how we can bring innovation – strengthen innovation and the technology base in the intelligence community and in the U.S. in general.

A quick bio, I was kidding the congressman right before we got on; he reveals he's the only congressman in history to have been born in Lima, Peru. He was a Rhodes scholar. He worked a lot in local politics, particularly on housing, was at Goldman Sachs, and now chairs the strategic technology and advanced research subcommittee on the House Permanent Select Committee on Intelligence. So they've just put out a new report that he's going to talk about, about how to preserve the U.S. tech advantage and enhance our agility. That's a theme that a lot of people are picking up on, so the report is really timely. There's almost 20 recommendations. We'll get to talk about them.

The format here will be Congressman Himes will open with, you know, some remarks. He and I will then have a few questions back and forth. And then we're going to turn to you in the audience. You can submit questions to CSIS and we will – we'll tee them up as we go along. So with that, Congressman, thank you for doing this. Welcome to CSIS.

Rep. Jim Himes: Jim, thank you. Thank you very much for pulling this together. And a big thank you to CSIS for opening this forum for what I hope will be a very interesting discussion. CSIS is deeply, deeply respected on the Hill. And, you know, in a world where I know a lot of think tanks worry that their production gets put on the shelf, I will tell you that CSIS' does not. For those of us who work particularly in foreign policy or national security, you guys have done tremendous, tremendous work.

So I've been asked to give kind of a five-, 10-minute summary of the findings of our report. I do chair the Strategic Technologies and Advanced Research Subcommittee of the House Permanent Select Committee on Intelligence. And this is really a yearlong project that was undertaken first because it is always innovation and technological edge – that's always one of the important things that gets shoved aside by the urgent things. And it doesn't become urgent until somebody else demonstrates what innovation can do.

And we wanted to make this report readable to the lay person so, you know, we talked about – we started obviously with the race that gave rise to American official investment in basic research, the Manhattan Project, and the race to an atomic weapon back in the 1940s, and how Vannevar Bush really kicked us off into the remarkable generations-long partnership – it certainly evolved into a partnership – of significant government investment in basic research, in concert with the private sector obviously, giving the United States for a very long time a qualitative edge over its opponents, but also spinoff and tangential accomplishments associated with that technology.

You know, we're all wearing it, and using it, and taking advantage of what came out of government basic research. I'm a Democrat, so every once in a while when I sort of want to justify the role of government I talk about the traditional things, but then I'll hold up an iPhone and say: Semiconductors, the internet,

satellites that do location services, all of these things were originally researched or actually created by the federal government in places like DARPA.

So we set off to try to create a little bit of urgency here, and to bring it to the forefront, and to not just be academic in our approach but actually to imbue the latest intelligence authorization act with some of the ideas. I think we succeeded in that regard. Let me – in order not to simply list the recommendations, which you can look at in the report which I hope, Jim, we can maybe post a link or something up on the chat there. But in order to sort of give you a little bit more interesting presentation, we really started with the approach that we've got to get away from the idea that is the animating idea of 95 percent of conversations on Capitol Hill, which is that the solution is just more money.

I will tell you, having been in Congress for 12 years, that that is the solution to 95 percent of our problems. And not to be snarky about it, it is in fact a solution to some of our problems. But the reality is, of course, that the world is investing far, far, far more in research and development, basic research, than it ever has before, even as the U.S. official commitment to basic research has, in a real way, come down or been flat over time.

But out of that emerges the notion that animates this report, which is if that is true, if your friends and allies, and in particular the private sector – and I'll say private sector again, because that's, of course, where the bulk of basic research is occurring today – if you're doing more research than ever before, you don't want to think in terms of matching your antagonists or your opponents dollar for dollar. You really want to think about leveraging that research which is out there.

And a lot of what is in this report has to do with creating the kind of environment in which better information can flow between the IC and, broadly defined, the national-security apparatus. You'll see in this report it's hard to draw a really bright line around the IC. But how do we make sure that the government can take advantage of the remarkable basic research being done in the private sector and, of course, by our allies, and perhaps even by our opponents?

So, again, we sort of set out to say it's not just the money. It's how you think about getting the value out of the immense amount of money that is being spent globally, and in particular in the private sector.

The other idea that animates the report – again, trying to avoid giving you a list of recommendations – is there are a couple of inputs to innovation – money, certainly, which we've just talked about, environment and people. And it's no coincidence, of course, that a lot of our report is about how we can take advantage of the R&D and basic research being done out there by having better flow of people in and out of the intelligence community.

So many people in the private sector will tell you that they would love to do, you know, one, two, three, four years in government and bring their knowledge, whether it's in AI or programming or biotechnology, to the federal government. They probably don't want to do 20 years. And, of course, that's a somewhat

foreign concept to the way the federal government has always been structured and hired people. But that's obviously something that we need to fix.

The other animating theme, though, if you think about people, money and the environment in which those people and money come together, which is one way, I suppose, of thinking about entrepreneurship and innovation, the other intangible that is, in some ways, inimical to the culture of government but which is critical to innovation is risk.

You know, there's wonderful thinking being done, as I think most people who are watching this know, about why the United States is so innovative. And there's lots of good reasons. But one of the underappreciated reasons, of course – and I think The Economist wrote about this many years ago – in the United States, our bankruptcy policy.

The way we think about bankruptcy, which represents what happens when risk goes wrong – in the commercial sector, anyway – you know, in Europe and in Asia, bankruptcy is game over for people. If you go bankrupt, that's sort of a shame on your family. You know, your friends don't return your phone calls, et cetera.

Here in the United States, of course, we have a process that is designed to, in bankruptcy, get you back on your feet. And, in fact, having been a technology banker for a number of years, I know that there are those venture capitalists who actually like to see failures in the background of the entrepreneurs that they sponsor, because that, of course, is in many cases the best way to get educated.

That, of course, is an idea that is profoundly foreign to the government. And one of the things we do in our report here is say Congress, you've got to heal yourself in that regard. There are lots of good reasons for a colonel or a midlevel executive inside one of the IC agencies to be deeply skeptical of doing things differently; not hard to understand what those incentives are that push you away from risk.

But quite frankly, you know, members of Congress are by definition not subject-matter experts. And, you know, one of the political tools that we have is to get worked up about waste, fraud and abuse or failure. And all too often we, I think, create a culture that is inimical to innovation. I didn't put it in the report because I really wanted this to be a bipartisan report, and it's hard to go here in a bipartisan way.

But if you just think back to what happened my freshman year with a company called Solyndra – many of you will remember that – Solyndra was funded out of a Department of Energy – it was basically a debt fund designed to fund those entities which could not be funded in the private sector. That, of course – that, of course, says something about the riskiness of the funding that was to be deployed out of that fund. And it makes all the sense in the world. Look, if you're a venture capitalist, require 20 percent IRR, and the government is willing to tolerate a 5 percent IRR because, you know, it doesn't need to answer to limited partners, that makes all the sense in the world. But, of course, the universe blew up when a Solyndra went under, even though that is probably an exemplar of actually a fairly successful fund, which, in fact, it was.

So, again, I don't want to list all of the recommendations here. But we have a broad array of recommendations of how to get people moving in and out of the IC better and faster, about how we might work more intensely with our foreign counterparts, you know, on communications technology. The Israelis are second to none.

Different NATO allies have different competencies. A lot of this relies, and then I'll leave the people thing behind, around a fairly prosaic issue, which is modernizing and streamlining our clearance process. That is underway. I will stay neutral about that because I'm still really fully understanding whether we're taking this far enough.

But look, when bringing in one of the world's top minds to the IC can take two, three, four years, you have a profoundly broken system. And in this era in which, you know, digital dust makes human intelligence very, very difficult because everything that you have ever done is discernible, we ought to be a lot quicker than we are on security clearances.

Last thing I'll say, in the interest of keeping this to 10 minutes or so, another one of the maybe nonobvious ideas, along with it's not just the money and we need to take more risk that we embrace at the end of this report, is that all too often, and I did it myself this afternoon, this is framed as winning a race, which is actually a metaphor that serves to get some sense of urgency in policymakers.

But it's also probably not the best metaphor in which to think about innovation, and the reason for that, of course, and it's in the report, is that technological races can be won but they very rarely stay won for very long at all.

The United States, of course, uses a nuclear weapon in 1945 and it's just a couple of blinks later, of course, that the Soviet Union and China are nuclear capable, and this, of course, just is a theme that repeats itself in every form of technology. There will never be a form of technology that will not disperse and fragment, and so – and this brings me to the sort of last point, which is a little prosaic. It's not as exciting as talking about the downside of biosynthesis.

But if we don't invest a lot in the – and not just invest but reanimate and breathe new life into our international leadership around the establishment of norms for the use of new technologies, we'll be in a lot of trouble because we're not ever going to win every single race and, as I said before, not every race will stay won. And so it's absolutely essential that we have the norms established for things like biosynthesis, and we'd cite the example of the Chinese academic who actually started messing around with the human genome and stem cells. But it's not hard to conjure scenarios where, you know, either through artificial intelligence or other technological advancements – you really want a set of norms and rules and laws and protocols around the use of a new technology, hopefully, faster than occurred in the creation of the obvious historical analogs, the Geneva Conventions and that sort of thing.

So, Jim, I hope I stayed more or less to 10 minutes with a little bit of an overview there and, again, thank you to you and to CSIS for having this conversation.

James Andrew Lewis: No, that was great, and I think it's – there's a lot of good parts in the report. I'm going to cherry pick a few of them.

A couple weeks ago, the Defense Innovation Unit out in Silicon Valley had an event where they had John Hyten, who is the vice chair, talk about what he thought some of the obstacles were to innovation and national security, and he, like you, said a risk-averse culture. You know, he said that when he was a captain he got a \$60 million project, and nowadays that project would be managed by three committees in the Pentagon.

Changing culture is hard, though, so tell us a little bit more about what you're thinking on how you move the U.S. It's funny, because I've seen and I've been trying to figure out when did we become more risk averse but, certainly, in the last decade. This is a risk-averse culture. How do we change that?

Rep. Jim Himes: Yeah. Great question, Jim, and I would recommend a book that was influential on me called "The Kill Chain," which was written by John McCain's, I guess, chief and lead staffer on the House Armed – the Senate Armed Services Committee, that really elaborates on that.

And the point that is made in the book is that, yeah, we did change. We went from a super experimental, highly-centralized culture in the days of Vannevar Bush to a calcified one, you know. And here's where we begin to step on some toes and understand that it's not just a change in culture, it's a change in economic incentives. The toes that we can step on here, of course, well, are many – are many.

And we should be clear, the culture is wrong in Congress. The culture is wrong on the Pentagon generally speaking, although it is getting better. It is not uniform through the IC. But you know, sadly, particularly in the Pentagon – which I – full disclosure, I sit on the Intelligence Committee so my insight into the Pentagon is limited – but you know, was a – was a culture in acquisition and development that evolved from the purchase of highly specialized big non-commodity hardware. You know, if you're really good at buying tanks and aircraft carriers, those are not skills that are good for buying software.

And the reason I say software, and we talk about this in the report, is that software is more and more everything. And we sort of run through the classic article that everybody knows about, how software is eating the world. You know, software does not lend itself to the kind of acquisition that a tank does. And in fact, in many ways it's the opposite, right? It's never done. And we hold up an example. Kessel Run, which most people will be familiar with, you know, an innovative and creative new software development group that came to be, you know, largely because of some really courageous leadership on the part of Dr. Will Roper within the Pentagon, where they are actually writing software the way the private sector does – you know, iteratively, constant contact with the end user, feedback, constant patches, constant updates.

That's the opposite of the way, you know, we buy non-software stuff, and even buy an awful lot of software. So that's just one example of how not just culture but economic incentives need to change. You know, if you're a contractor that is used to living in the hardware world and you really want to get into software,

you know, you're going to have tools at your disposal to turn off the possibility that, you know, 21st century software developers get in and, you know, as they say, eat your lunch. And that's something that we need to be really intentional about addressing.

James Andrew Lewis: Yeah, I know software eats everything. The phrase I prefer is software cures all the ills, because it really is a cure. So, I mean, that's a great part. There's a – (inaudible, technical difficulties) – software development fast. People are beginning to realize that.

Part of what you talked about – and this came up in the discussion of software – is public-private partnership. And the – (inaudible, technical difficulties) – part on now bringing people into the IC would help address some of the skepticism people have. When I read that, I was thinking: When you see a Hollywood movie about spies, there are never lawyers in the room. And in real life, of course, there's lawyers everywhere. But when you think about public-private partnership, is it more than just bringing people in or sending people out? Tell us what you have in mind for that, because it's a very broad phrase.

Rep. Jim Himes: Yeah. So the years in which I have been very active on IC issues – the last eight years, I guess – have been years in which the breach – let's call it a breach; that may be slightly overstated – between the private sector and the IC has been inordinately large. And that's due to a bunch of things, right? Coincidentally I was put on the committee about one month before Edward Snowden released the information he had taken from the NSA. And we all remember the kerfuffle that caused in the American body politic. And of course, you know, Google employees' reaction to the possibility that Maven might be used for counterterrorist purposes, et cetera.

We do have a very meaningful rift between the private sector and the IC. It can be overblown. I mean, make no mistake, you know, executives at many of the companies that we're talking about here are often very, very helpful to the IC. But my point is not whether they should be more or less helpful to the IC. It's that we can really stand to use a much – a much more open and free flow of information between the IC and the private sector. And that can be as simple – and this actually happened – as, you know, Sue Gordon going to Palo Alto and addressing employees of the platform companies, or whatever it might be, just, you know, we're people, right? We understand relationships better than we understand text.

And you know, so one of the things that we actually encourage the IC leadership to do is to actually intentionally spend – don't just show up at the conferences, but actually go and get to know private-sector leaders and private-sector employees. And that leads to, you know, the possibility that we talking here – talk in the report about, about, you know, the possibility of fellowships, of more hiring authorities, of temporary hiring authorities. We didn't go too far down this path, but you know, I'm intrigued by the notion of a digital service. Now, you know, that was sort of talked about and worked on in the Obama administration, but why not a digital service in which you have broad-ranging people going around the IC understanding the challenges of software and data analysis and providing an outside perspective? All of that stuff is enabled, A, by lesser suspicion between the two sectors; and B, by modernizing our clearance process.

James Andrew Lewis: Just as a – as an advertisement, we'll probably have an event on the idea of a digital service in a month or so, so after the election. It's one that has – it has some merit.

We've gotten a couple questions and they're all more or less on the same topic, which is the report and you have talked about working with our foreign partners. And you know, sometimes that can be difficult in the intelligence world. Everyone knows Five Eyes now, but when you talk about collaboration with people who are outside the U.S., what were you talking about? What did you have in mind – specific mechanisms, agreements? I mean, what's the approach here?

Rep. Jim Himes: Sure, sure. Yeah. It can be difficult, but I think it's less difficult if you think of the wide array of IC activities. Of course it's difficult when you're talking about operations. Of course.

James Andrew Lewis: Yeah.

Rep. Jim Himes: I think it's actually a lot less difficult in the science and technology world, right? The culture of research is an open culture. I've never – other than my education I've never been in academia, but you know, it's an inherently open culture in academia. And you see this in the scientists who work inside the IC or inside the DOD. You know, they're very attuned to keeping up with literature in their field and they attend academic conferences. And I think we can do and should do more of that, you know, particularly in those areas.

We haven't talked about this, Jim, but I think it's important. There are some areas where research is wide open – artificial intelligence, for example. You know, artificial intelligence is being researched everywhere, and there's all sorts of ferment of new ideas and understanding communications. I would contrast that and maybe put it at the other end of the spectrum with quantum research, right? Quantum research, by definition, requires something other than a laptop. And certainly as you start to think about advanced quantum research, it requires, you know, deep, deep, deep investment and, you know, the issues are more binary. Artificial intelligence basically does everything whereas, you know, quantum computing will have a few obvious applications, some of which are actually very, very sensitive in the realm of national security.

But in both of those fields we should – you know, let me give you a specific example. It's very hard for a foreign scientist – a British foreign scientist, an Israeli foreign scientist – to get a birth inside one of our national labs. And I'm not encouraging, you know, imprudent risk-taking –

James Andrew Lewis: Sure.

Rep. Jim Himes: – but, you know, it will not be lost on people who are listening to us today that it would be pretty darn hard to name, you know, non-U.S. people or people of non-U.S. heritage who have been involved in recent breaches. I can – I can think of one. But anyway, my – you get my point, which is that we should be open –

James Andrew Lewis: Right.

Rep. Jim Himes: – to the notion that it would be worth taking some risk – some incremental risk – if we can get access in narrow areas to unique expertise.

James Andrew Lewis: One of the questions we got touched on your comments on the clearance process. So everyone agrees it's slow. It's gotten a little better since a few years ago, but it's still slow. And someone asked, well, how about over-classification? I used to overclassify all the time because it's a good way to avoid risk. Any comments on that? How does over-classification fit into this?

Rep. Jim Himes: Yeah. Yeah, great question, and the answer ranges broadly.

Over-classification exacerbates the natural suspicion that can arise between the public and the IC, you know, particularly when over-classification is done for precisely the reason that you talked about, because it makes, you know, the truth or what is classified makes, you know, some individual or some agency look bad. But it's also a real problem because one of the recommendations in the report is that we need to find a way, as long as security clearances take a long time – I'm very, very intrigued about how that can be accelerated in this technological and digital world – but as long as they take a long time, one of the things we need to do is find ways for people who want to work in the IC to work on an unclassified basis while they get their clearances. And obviously, the more you put into the classified world, the less productive they can be.

You know, we heard story after story, in creating this report, of really dedicated people who were just basically twiddling their thumbs for 18 months, 24 months. And you can't – you simply can't ask people to do that. So this has – and here I'm getting out onto thin ice because I would call myself a sophomore on issues of classification. But I'm very, very interested in them.

You know, it's been a long time – as a member of Congress, I don't actually have to get a security clearance to get the information that I get as a member of the committee. But, you know, this idea that you send a guy in a raincoat and a hat around to talk to your college roommate, you know, it's just so 19th century, right, at a time – and here you get into privacy issues and all sorts of other issues – that at a time where, if I were willing to give you the passwords for my email and some of my other devices, you don't need to ask me questions because you know – (laughs) – you know what Facebook and Google know about me.

You get my point here, right? There are ways to know what somebody has been doing that I suspect we very substantially fail to exploit. And I don't want to come off as too dark there. This would obviously be fully – you know, fully consented.

James Andrew Lewis: Your neighbors certainly look at you funny when they do the background investigation.

Rep. Jim Himes: (laughs)

James Andrew Lewis: So that's a drawback.

What's the reaction been in the IC? I mean, how do they react to this? You know, there's – it's hard to figure out how we ask this in a nonpartisan way, but what's – has there been a reaction from the IC? Because you worked closely with them in developing it.

Rep. Jim Himes: Yeah, yeah. So it's hard to answer that question, Jim, for a couple of reasons. One, the report is just out.

James Andrew Lewis: Right.

Rep. Jim Himes: And I will tell you that we created this report in a hugely iterative fashion with the IC. So we went and saw everybody – CIA, NSA, DIA. We went to IARPA and DARPA. I mean, we just sent draft after draft. So I can tell you that I'm pretty sure there's nothing in here that's offensive to the IC, because they saw lots and lots of drafts.

Mitigating my ability to answer your question in a really solid way is the fact that sometimes when I ask a question I don't get the most candid answer. (Laughs.) Nobody has told me that it sucked yet. That's why, by the way, I told you that we are hungry, hungry, hungry, obviously, for criticism.

But, no, look, I think, inasmuch as I've heard informally, I think it's been well received. The risk is that we'll just let it sit and, you know, members of Congress will move on to other things. And, you know, this kind of report is hardly a new idea. There are, you know, a half dozen, at least, current out there. I think CSIS is working on some stuff. The Council on Foreign Relations did some.

The real beauty has to be when we find those leaders inside the Congress who say we're going to make a lot of this happen.

James Andrew Lewis: One of the related questions was that you already have people in the IC who – you've already mentioned them. You have IARPA. You have the various S&T branches and agencies. How are they going to fit into this renewed effort?

Rep. Jim Himes: Well, you know, the good news is that our view of In-Q-Tel, IARPA – you know, you name these places where you see innovation happening or being supported. We didn't stumble on pathologies. I expected to find a lot more stovepiping. And I constantly asked the question – there are some virtues to ignorance, and I constantly asked the question, wait a minute, you're doing this on AI, but how do you know that you're taking advantage of the guy over at the University of California at San Diego?

You know, and so we were actually really pleased with the kind of awareness and lack of stovepiping in these entities. I think our answer is a happy one for them, which is that you should be able to do more and range more freely and take more risk than you currently do. And a lot of what our thinking was with respect to them was actually shouldering some of the blame ourselves. You know, and this comes back to what we were talking about before of trying to create a culture in the Congress which is much more accepting of risk and the inevitable failures.

James Andrew Lewis: I'm tempted to ask you if you think that's generational, but we'll give you a pass on that one. (Laughter.) I sometimes wonder that.

You know, and one of the things you mentioned – we are getting more questions in, so I'll feed them in. But you mentioned something. You talked about how we create incentives for a more risk-tolerant culture, a more agile culture. That's really a hard one when you think of the federal system and its – in the report, you talk about how cumbersome the acquisition process is. You hear that from everyone. What are you thinking on incentives? I mean, in the market, you know, incentives are quick and painful if you get them wrong. In the government, how does it work? How would you – what would be a good way for it to work in the future?

Rep. Jim Himes: Yeah. I'm going to answer that question frankly. There are a lot of things that you can do.

A lot of – a lot of this is about leadership and motivated leadership. You know, the chairman of the defense intelligence unit, Eric Schmidt – not the unit, the Defense Intelligence (sic; Innovation) Board – observed that the military, DOD, is actually a very innovative place. And his language is you don't have an innovation problem; you have an innovation adoption problem.

And again, you see a sort of toggling here between DOD and the IC, but you know, to change the incentives you've got to be ruthlessly results-focused. You know, in the development of AI or the writing of software, failure is not an option anymore, and failure is all too often where we wind up. And I think you hold up successes.

I told – I talked about Kessel Run. I just happened to actually be a few days ago at Al Udeid Air Base and had an opportunity to talk to the commanding general there and ask him about it. And you know, he is just beyond thrilled with what his airmen experience in the CAOC there, where Kessel Run is on a – on a real-time basis developing the software. So you need those stories of success.

That's the happy side of the story. There's probably a less happy side of the story in terms of we have a very highly concentrated contractor population today, much, much more concentrated than it ever has been. And look, I have the highest respect for those contractors so I don't want this to come off as in any way attacking them, but they are not necessarily hotbeds of innovation. And in fact – I don't need to tell you this – but there are many incentives that are structured to sort of preserve the status quo. An awful lot of our senior – retiring senior executives and senior officers go to work pretty quickly in the private sector in ways that maybe, maybe, maybe disincentivize you from what economists call disruption in their activities while they're still on the inside.

So I think – and again, I don't want – I don't want that to come off, you know, incorrectly. We build submarines, F-35s, and all sorts of stuff here in Connecticut. But you do really want to hold any incumbent private-sector operator's feet to the fire, because if you don't the result is Eastman Kodak, just to use a private-sector rather than a public sector example.

James Andrew Lewis: The remarks on the clearance process, which I guess must be painful for everyone, generated a lot of questions. So I'm going to try and summarize them a little bit because a couple of them touched on something that we haven't talked about, and that is the relationship between clearances, privacy, and the skepticism about what the government is actually doing. The report touches on this, that people – you know, if you don't work in the community, you don't necessarily know the limits – and you point this out – the limits on what can be done. So what are you thinking when it comes about privacy and streamlining the clearance process? I mean, how is that going to work?

Rep. Jim Himes: Well, yeah, I noticed one of the questions was pointing at this. There was – there was a question that was premised on a disagreement with privacy.

I wasn't actually making a sort of declarative statement about privacy. The declarative statement I would make would be given the digital dust out there, you know, given what Facebook and Google and Amazon know about me, there are obvious ways to learn a lot more about me than you can sending a guy to talk to my college roommate.

James Andrew Lewis: (laughs.)

Rep. Jim Himes: And so the way privacy comes into this is that you could postulate a system which I don't think exists – again, I'm still a sophomore on clearance issues – but postulate a system where I just turn over the keys and I say, you know, have at my text history, have at my social-media history, have at my email history, and whatever else Google currently has on me, right – I mean, this is – this is the irony, right; this stuff is already out there and not necessarily protected – that we could really streamline that process.

Now, I do think a hand goes up at this point and some people say, well, isn't that a violation of my privacy. Well, no, it's not. It's all – it's all done through a system of consent. You know, the truth is if you're going to work in the most sensitive areas of the United States government, you're – you know, you're going to take polygraphs and you're going to give up a lot of your privacy. So I don't think that's the fundamental issue. I'm just not sure we're taking advantage of stuff that Google and Amazon have been doing for 10 years.

The other area I'm concerned, and, again, I need to be very careful and tell you here that I don't have terribly informed views on this, but I started with some skepticism just because I don't know and I'm not persuaded that we are really good at understanding the correlations that lead to somebody betraying their country or being sloppy with secrets.

My guess is it's a lot better than it used to be. But remember, it wasn't that long ago where, you know, being gay was disqualifying to a security clearance. So, again, I want to be humble about this because I've got work to do.

But I don't start as an overseer from the standpoint that, oh, everything is fine in terms of really looking at the population of those who have done badly by the country and what the motivations and character types, et cetera, that led to those behaviors.

James Andrew Lewis: You know, I was involved in two projects that tried to do that, and you got a lot of false positives. I'll just put it that way. So –

Rep. Jim Himes: I mean, I had an interesting conversation, Jim. Actually, I was up at an NSA facility. I had a really interesting conversation with some senior people where I said, look, you disqualify people who are foreign-born immigrants from some of this stuff because they may be disloyal.

Well, I'm not accepting that. I mean, I know first-generation immigrants who were here all of 10 years who are so much more loyal and so much more in love with this country than anybody else I know. So, again, I – we've got some poking to do there.

James Andrew Lewis: One of the topics you raised that got questions in a different stream is the issue of norms, and norms are difficult to get in such a hostile environment. So why don't we talk a little bit about norms? First, what do you have in mind for norms? You mentioned – I'd point out that the Geneva Convention came after a catastrophic war and that gave it a little bit of impetus. We may not – I hope we don't have that impetus now. What's the first step towards building norms?

Rep. Jim Himes: Yeah. So let me answer your specific question first, which is, you know, the first step is to just continue doing the hard work of working with your adversaries in advancing the process – you know, the government group of experts, which now has been meeting for years on cybersecurity issues in the U.N. context. You know, we just got to keep at it. It is unsexy work. It is, you know, more often than not characterized by disagreement than by agreement.

But we just have to keep at it, and in some cases, I think, we have to formalize it. You know, and by the way, the Department of Defense, you know, really has done great work on norms and ethics around artificial intelligence and so that's a model for that. I worry more about things like biosynthesis where the government doesn't really – you know, the whole biotechnology world the ethics are sort of established inside academia, which may be good or bad.

I'm not saying that's a bad thing. But it's – it probably is worthy, particularly given the fact that people who are knowledgeable tell me that the Chinese, if anything, are ahead of us on some of the biotechnology issues, it would be really worth us devoting official time and formal time to thinking about the ethics associated with biosynthesis and biotechnology.

But, I mean, it's an aggravating answer, Jim, because it's just a long brutal slog if you're going to avoid the kind of urgency which leads you in retrospect because there's been a catastrophe with the use of mustard gas or whatever it might be that lends urgency to the – to the problem.

You know, and, of course, the criticism is always there; well, why worry about norms if the Russians aren't going to observe them. Well, yeah. Yeah, that's right. You know, all of the conventions that we have and have had for hundreds of years have never been observed in their entirety. Not even close.

But it's better to have them if for no other reason than for predictability and if for no other reason than the Russians and the Iranians and the North Koreans and I all share – I, us – all share a vulnerability to rogue states and non-

detractable actors. So, again, it's just, like, you know, just doing the grinding work of trying to advance the cause.

James Andrew Lewis: That was actually going to be my next question, which I'll skip now that you've answered it, which is, you know, what do we do if the Chinese and the Russians don't want to play ball. But I'll tweak it a little bit and say: Who would you work with? Would you do this domestically? Like, do DOD with the AI guidelines, which are very good? Would you start with like-minded countries? What sort of – this is a little off topic for the report, but what's the approach to building norms?

Rep. Jim Himes: Yeah. Yeah. So, and look, let's be fair here. It's not just a problem where the Russians the Chinese may not observe, acknowledge norms. You know, we're as good as anybody gets on cyber offense, and you know, as you might imagine there are those, given that fact, who are hesitant to take capabilities off the table. So it's not just the Chinese. There's a natural dynamic that makes this really hard for us too. I'd like to begin that, as you – as the premise of your question suggested, that we follow norms more than the Russians and the Chinese do, but we also have equities that can be compromised if we are – you know, if we limit ourselves. You know, it's like the proverbial landmine argument that we have.

But so you ask, you know, is it domestic and international? I think the answer is both. I mean, a lot of the thinking, of course, around how to structure norms in places like – you know, areas like AI and biosynthesis and cybersecurity – a lot of that thinking will come out of institutions like yours, and American academia. At the end of the day, of course, the arena in which, you know, the beast is given fangs is the international arena. It doesn't make a ton of sense to have the very best thinking in Silicon Valley on AI if no one else agrees on it. So you know, I really think that this is a chemistry equation that involves a lot of thinking outside of the government. But ultimately, it being brought to multilateral, multinational organizations for some form of acceptance.

James Andrew Lewis: Yeah. That's a place where actually being a technological leader gives the U.S. an advantage, because either people want to be on the same train as us or they're afraid we might pull ahead and it makes them more amenable to norms. So when you look at the – where we stand, though, where would you say we are in terms of – and this is a very broad question, but it's a very broad report – how are we doing on technology, not only in the government but in the private sector? This is a huge debate and it goes to your point about race. I mean, if we're in a race, how are we doing? I hate the race metaphor too but give us – give us your assessment.

Rep. Jim Himes: Yeah. There's all this – you know, if you look in the chart, in the report of U.S. and Chinese spending, we are about at that point of convergence. Now, that doesn't mean much, but it does indicate that it's a very different world in terms of investment than it was 20 years ago. And there's a lot of sort of sloppy language that I engage in around how, you know, our adversaries are now, quote/unquote, "near peer."

I would tell you that people who follow – and I mentioned this earlier – people who follow biosynthesis and biotechnology closely are already sounding alarm bells that, you know, the U.S. may not just be a near peer but may be behind in

some of the research. Some of that may, of course, be attributable to the fact that, you know, as we saw in the example of that Chinese academician who was messing around with the human stem cell genome, that maybe – it may have to do with ethical constraints.

But you know, I do think that generally speaking there are areas where we are, you know, still pretty well ahead. You know, the West's research into quantum technology is substantial, even as China does a lot of that work as well. AI is really hard to say. I mean, AI the issue is not so much the technology as the application, right? I mean, AI does everything today, but now we start talking about autonomous drone system and swarms of autonomous drones, we really do need to give some thought to that particular application of AI. And then on cybersecurity, which is probably the best known of these areas, just because there is such a dialogue at the United Nations, amongst other places, you know, we're stumbling along.

But, you know, it is an interactive problem, right? I mean, I irritated folks in the Obama administration, had a number of really interesting arguments with senior folks in the Obama administration because I felt that their response to the Russian hacking of our election was counterproductive. This is just illustrating how you get to a place to negotiate norms. Again, I believe, and I know, based on my job, that we are as good as it gets on cyber offense.

But the Russians didn't get to experience that. You know, instead we PNG-ed a bunch of their people, we shut down one of their facilities. And I think that a better place to have been – and by the way, lots of senior Obama administration people disagreed with me and this is a big argument – but I believe we would in a safer, better place to have a norms discussion on cybersecurity if the Russians had had the right taste of our offensive capabilities. You know, right now the message is, gosh, we PNG-ed a bunch of people. I'm not comfortable with that.

James Andrew Lewis: We need to get back to the report. But let me just say I couldn't agree with you more. And I was in some of those internal conversations where pushing these guys to punch back with all these – you know, and, yes, there's escalates, and risk, and we need to think about it and, you know, how do you involve your allies. But you've touched on – you know, the Russians got the wrong signal. And I have friends in the Russian government who basically said: You know, after 2016 we were waiting to see what you guys would do back. And you didn't do anything. So you've put your finger on a key point.

But we don't want to have this to be a cybersecurity discussion. Easy to talk about. You mentioned biosynthesis. You brought it up a few times. What other technologies do you think we ought to be worried about? Quantum and AI? Hypersonics? What are the technologies you think we need to focus?

Rep. Jim Himes: Yeah. We really – I don't want to oversell what we were doing or what I know. There's lots of technologies – as you mentioned, hypersonics – that in the DOD context you really want to know a lot more about. It just wasn't sort of the purview of the IC. You know, cybersecurity, biosynthesis, AI, quantum – those are really the technologies that are – that are most relevant. In some cases in surprising ways. You know, you say, well, why biotechnology? Well, you know, in some senses the genome is just software, right?

And I think we – I think we give an example in the report that, you know, what if you could move, you know, 10 megabytes of data on a grease stain on your shoulder, right? You know, some sort of alterable genome. What if you could create a – this gets pretty Hollywood-ish – but what if, you know, you could create a – you know, a housefly that was capable of recording an hour of video? So that's why biotechnology is of interest to the IC. I think quantum is fairly obvious. Those are really the areas. There's lots of technological areas that I think the Pentagon would be more focused on, but those are really the areas that we thought had dramatic applications, challenges, threats, and relevance to the IC.

James Andrew Lewis: We did get one question, going back to the discussion we were having on norms, that said: Technology changes so fast, is it even possible to have an international regulatory regime? I have views on that, but what are your views on it?

Rep. Jim Himes: Well, I mean, of course it is, right? You know, you need to unpack that a little bit. You know, of course it is. You know, it's not like chemical weapons have gone away. And so, yes, we – (laughs) – we need to preserve the legacy agreements around the use of chemical weapons and biological weapons actually, which is out there, even as we create new ones. With all the problems that we're aware of, of noncompliance, of our own challenges, of, you know, giving up the right to – you know, for certain behaviors or applications. But no, of course – of course it's important. I mean, you know – (laughs) – some of this stuff – and, you know, when you write a report like this, you want to sort of every once in a while trot out the parade of uglies. But some of this stuff is really, truly ugly in terms of its implications if we are in some wild west scenario.

And remember that norms aren't just about – and I don't need to tell you this, Jim – but norms aren't just about legally constraining behavior. Sometimes they're about understanding what is considered – so, for example, in the cybersecurity realm, what is considered a criminal act versus a – you know, an attack, an act of war? Understanding a little bit about how your opponent thinks about their doctrine and that kind of thing. So there's all sorts of things that are important around having this international norms and conversations that aren't just purely about the legality of how you use a technology.

James Andrew Lewis: I warned you that we would get a boatload of questions in the last 10 minutes. (Laughter.) So I'm having trouble. They get emailed and I'm having trouble keeping up.

Rep. Jim Himes: All right, I got to move faster with my answers then.

James Andrew Lewis: But this one's a good one. They said, could you address workforce issues? What should the U.S. be doing to make sure we get the right workforce, both in the IC but in the larger technology space.

Rep. Jim Himes: Yeah. Great. I got a quick answer to that question. It's a huge answer but there's a really quick answer. And it's in the report, right? Boy, do we need to do better on STEM education than we're doing in this country. And, you know, there's endless information, but – on how we do that. But we just need to do it.

Secondly, again, just to keep this answer short, boy, have we gone in the wrong direction on immigration; you know, Andy Grove, Sergey Brin. I could go on and on and on and on. You know, we – and I don't mean this to sound partisan or an attack on the president, but it is – you know, telling the smartest people in the world that we don't want you here is a massive national-security risk.

James Andrew Lewis: Yeah. I'm speechless. I won't talk about immigration. (laughs) But clearly, you know, 20 years ago people were telling me, when someone got a STEM Ph.D., it should come with a green card attached to it. And we didn't do it then. We haven't done it now. But it's still a good idea.

Somebody asked, one of the things our adversaries focus on, particularly the Russians, is the psychological side of this, the sort of cognitive side, in their influence campaigns. Where would you see this sort of renewed impetus for innovation addressing those issues? You know, they have a different way of fighting than we do. So what do we do about it?

Rep. Jim Himes: Right before this I was in a HPSCI open hearing on misinformation. And that's what you're asking about. Can technology be used to help us sort and understand information?

James Andrew Lewis: Yeah. They're saying given the disparity in adversaries' use of psychological operations and propaganda, what do we do to keep pace? Where do we innovate to stay up with – the Russians are, I think, the best. The Chinese are trying to learn from them, though.

Rep. Jim Himes: Yeah, yeah. I mean, at one level the answer is kind of obvious, right. And the obvious answer is that, even as technology has put inconceivable information at our fingertips – and by information I also mean the truth. You know, I still marvel at the fact that when I get into an argument with somebody in a restaurant over some obscure fact, it takes me, you know, three seconds to get the answer. With that capability, of course, comes the ability to shape the truth or to deny the truth.

And I – you know, I'm not sure the answer there, Jim, is a technological one. In fact, I was a little shaken by what I saw in that hearing on misinformation. You know, I hate the idea of the government, quote, combating misinformation. That just – maybe it's because I grew up in a continent that was run by military dictators through most of the '60s and the '70s. And when I think about what governments are in the business of, you know, combating misinformation – I mean, that's what the Chinese and the North Koreans and the Iranians do. It's not what we do. And yet we obviously have a problem.

So I tend to look on the, you know, demand side rather than the supply side. What I mean by that is that, you know, please, please, please – and, by the way, you know what we do? You know what Congress does? We outsource those things that we don't want to get into because of First Amendment issues. We tell Mark Zuckerberg, you go do it. (Laughs.) I mean, I don't want Mark Zuckerberg telling me what's true any more than I want, you know, NSA telling me what's true.

So I throw up my hands if we're going to sort of preserve this idea of a liberal society where government – and God help us, the private sector doesn't get to tell us what's true and what's not – and I just say we've got to do better on the demand side. You know, we've got to make Americans better consumers of information, more thoughtful consumers of information. And that's really hard. And it's not a technological problem. It's a cultural problem, right? I mean, today we're in a particularly ugly world because polarization does not lend itself to critical thinking.

James Andrew Lewis: Yeah.

Rep. Jim Himes: But one of the lessons we're going to take away from this is that we need to take seriously our responsibility as citizens to be critical thinkers. And look, Jim, you know this is not a new problem, right. As I pointed out in the hearing earlier, you know, William Randolph Hearst probably got us into the Spanish-American War with a lot of disinformation.

So I don't have the answers on this, and it's way beyond the scope of this report. But I do think that the answer to misinformation is more about how we act as responsible citizens rather than how we better arm the government or the private sector with technology to help us with that problem.

James Andrew Lewis: No, that's a great point. And I think many people don't realize that there is no agency that has the authority to do the kind of information regulation you're talking about. And I –

Rep. Jim Himes: I'll tell you what. The moment there is, is when I – (laughs) – when I climb the dome of the Capitol to scream at top volume.

James Andrew Lewis: We have time for a couple more questions. One of them said, what lessons could you draw from the venture-capital community? How do you see working with them? And they're one of the strengths in Americans' innovation ecosystem. So what would you say about VCs? How do we learn from them? How do we incorporate some of what they do? Small team? Go ahead.

Rep. Jim Himes: Great, great question. Great question. The easy answer, of course, is what we've talked about, which is we need to find ways to get their minds and their experience into government for, you know, brief periods of time, to get government people into their environments. But let me offer what I think is a more interesting answer.

You know, I was a tech banker back when everybody who was a banker was a tech banker, in '99 and 2000, and one of the insights I got into that community is that venture capital is really about the identification of people. Very few venture capitalists are masters of the technologies that they invest in, but they are masters at identifying people who have disruptive ideas and who have the tools to make those things work. And if that's the sort of secret sauce to venture capital, it's a little scary, right, because the federal government is not necessarily in the business of identifying those people. Yes, we promote people hopefully in a meritocratic way. You like to believe that your general officers and your senior executive service are the best of the best. But what do you do about a – about a – you know, a major in the Air Force who is just – you know, who is the Sergey

Brin of his – of his – of his profession? You're constrained in your ability to really – to really give that individual the resources because there is such a lockstep thing in the federal government. So that is – that is me admiring the problem, not offering a solution. (Laughter.) But I think it's challenging.

James Andrew Lewis: It's a hard one.

So coming up on the end. Tell us what you'd like to see the first steps be in moving this forward? What are the things the IC can do? What are – you talk about government in general. What can the government do? What can the Congress do? What are the first steps for – because everyone agrees. You've identified the problem and you've put forward some good solutions. What should we do next?

Rep. Jim Himes: Yeah. Let me – let me answer that with – yeah, because people can read the report and the report has a lot of very specific things, but let me answer that question with an answer that sort of permeates the report but maybe isn't as explicit as it should be.

The Congress, certainly, and much of the government is pretty dumb technologically, and we need to fix that. We really need to fix that, and there's a lot of ways you can fix that. You know, prior to Newt Gingrich, Congress had its sort of in-house technology – you know, the Office of Technology Assessment. And that is a much-mourned organization and we are a lot dumber for it. Look, at the end of the day we're the Article I authority, and if we don't understand – at least basically grasp the technology but also understand the conditions around which technology is developed, like a risk-taking culture, this is going to be a very hard problem to fix.

So we are – so that's my answer to you, even though it's not, you know, page seven here. You know, a lot of this stuff is about making the government a lot smarter on technology. And I don't just mean those senators who were asking about, you know, the intertubes. You know, I really mean everybody in leadership of every branch needs to just be much more conversant, not just with the technology that's out there but how that technology is created, how it succeeds, how it fails, that kind of thing.

James Andrew Lewis: We covered a lot of ground in this conversation. And it was a little bit bouncy, but we talked about clearances, norms, public-private partnerships, international collaboration, and then people and organization. And we could probably talk for another hour, but I want to be respectful of your time. We've come upon the end here. It is an election year. Any final thoughts? What would you want to leave people with when they think about this? It is a great report. We've posted the link on our website. If you don't have it, you can also find it on the HPSI website. But what are your final thoughts here for the group?

Rep. Jim Himes: So I guess I'll maybe close, first of all, with a big thank you to you. But so what's an area that you – you're right, we covered a lot of ground. What's an area where we didn't sort of pull threads enough? We didn't talk a lot about hierarchy and structure versus lack of structure and flat organizations. The federal government is one of those things and not the other. And the reason it's more – there's two reasons why that's super interesting. Number one, being

hierarchical and super structured I think is a liability for innovation inside the federal government, and therefore we should think about changing that. And the question, of course, is how. This gets back to my major – my major in the Air Force problem.

But the other reason that's super interesting is that if hierarchy and structure is a problem, why are we so afraid of the way the Chinese are doing this, right? Because that's how they're doing it. They're doing it in a very hierarchical and structured way. And, you know, what – if we believe that hierarchy and structure is a problem, you know, is that a huge liability for them that opens the doors to our understanding vulnerabilities and their efforts in that regard? So that's probably the subject of a whole other hour or two conversation, but that's an interesting question that I'd love to get some feedback on.

James Andrew Lewis: You know, I thought one of the highlights of the report was that we need to be thinking not only about innovation and technology – whether it's software or hardware – but innovation in organization and innovation in people. So great report. Thank you so much for sharing your time with us. We will post this interview online and on YouTube. So we'll send the link out for that. Thanks, again, for talking with us.

Rep. Jim Himes: Thank you very much. And a big thanks to CSIS.

James Andrew Lewis: Thank you.

(END)