TRANSCRIPT

Defense Writers Group

A Project of the Center for Media & Security
New York and Washington, D.C.

Dr. Jason Matheny
Director, IARPA

March 14, 2018

DWG: Good morning everybody. Thank you for coming in, and thank you most important to our guest this morning, Dr. Jason Matheny, who is the Director of the Intelligence Advanced Research Projects Activity, which is a different slightly acronym than DARPA which is everybody is also familiar with. Sir, we do appreciate your taking time to meet with us this morning.

Jason has degrees from the University of Chicago, Duke, Johns Hopkins and Johns Hopkins again. So when it comes to research and --

Dr. Matheny: Dilettantism.

DWG: Academic preparation, let's put it that way. He's definitely well qualified.

I want to start at the beginning and give you an opportunity to talk for a moment about what you see in the intelligence community right now, what IARPA is working on, and what your priorities are going forward for the next year or so.

Dr. Matheny: Thank you. I appreciate it.

First, I understand that Pete Walker from DARPA was here last week, and maybe the best way to start is by saying we're sometimes called DARPA for spies. We focus on advanced research in support of national intelligence. We fund work at over 500

organizations around the world, mostly universities and colleges, but also businesses, national labs, FRDCs.

The work that we do is diverse. We fund everything from mathematics to computer science, physics, chemistry, biology, cognitive psychology, sociology, linguistics, neuro science, because national intelligence is a multi-disciplinary problem. The goal is to make sense of a complex world, and that world includes physics and chemistry and biology and sociology. Then we have to fund research in all of those disciplines.

Most of the work that we fund is unclassified, which is an advantage for settings like this. That means we get to be relatively open about what we fund and why we fund it. Most of it is openly published. And that work then yields many hundreds of scientific publications each year. We're probably best known for our work in quantum computing for which we're the world's largest funder of academic research, as well as superconducting computing, machine learning. Our work in cognitive psychology, we're probably the country's largest funder of work in cognitive psychology -- human judgment, decision-making -- because ultimately so much national intelligence work comes down to humans making difficult judgments under uncertainty.

We run our research competitively, so unlike say the National Science Foundation or the NIH in which you fund a research project and you wait a year or two for an outcome. We engage our researchers in tournaments, in which multiple research teams compete against one another towards a common set of technical goals that have highly ambitious milestones associated with them. Typically, a ten-fold improvement over the state of the art or more. In some cases a thousand or ten-thousand-fold improvement over the state of the art. And not everybody makes it through the whole program. Not everybody gets funded. In fact typically, per phase, one research team will get cut at a time, and usually there's only one or two teams left at the end of the program. That makes it extremely stressful for our researchers. But the benefit that they get is that they move much faster on a harder set of problems than is typically allowed for in federally funded research.

I think that's probably about enough to start with.

DWG: Okay, thank you.

I do a lot of work with the Air Force, and one of the concerns that the Air Force has had for years, probably ever since the [printer] UAVs came into common use, has been, it's easy to soak up intelligence, to gather the video, the technical information. And then the hard part comes after that. Once you've got this data, once you have this video, what do

you do with it? Who's going to look at it? Who's going to analyze it and assess it? Thousands of hours of video become thousands of hours of people looking at it theoretically.

So what are you working on in that regard, in terms of possibly getting humans out of the processing loop and out of the analysis loop?

Dr. Matheny: Great question. A large part of our research portfolio is focused on machine learning, to automate some aspects of analysis of raw data including raw imagery, raw video, raw text, raw audio. And some of that work has direct applications to Air Force data collection which is why Air Force has been a transition partner for a lot of the work that we've done on say video analytics, for full motion video, say for example, coming from UAVs.

You're absolutely right, there is too much data for human eyeballs to look at. And so we funded a program called Aladdin that summarizes what's happening in a video.

It's interesting, when we first went to Google sort of asking like what's the state of the art in video search several years ago, the state of the art was you look for the key words that users have fat-fingered in to tag a video with. That doesn't work, though, if you're looking at raw data that's coming off of say a UAV, or you're looking for videos that have been posted on say YouTube by a terrorist group of either a martyrdom video or an IED how-to video. Usually the terrorists are not polite enough to tag their own videos.

So finding those videos automatically using machine learning has been an emphasis for us at IARPA. First in the Aladdin program and now in the DIPA program.

DWG: What is DIPA?

Dr. Matheny: It stands for Deep Intermodal Video Analysis. And it automatically detects activities within videos.

Most of that's ground-based video. So for example if you have say security cameras that spot somebody who's handing off a bag to somebody else, or dropping a bag which might have an explosive in it, or brandishing a weapon. Right now those videos are used, unfortunately, forensically. Right? So after something happens. So like the Navy Yard shooting. There was video, there were video cameras, but there weren't enough human eyeballs looking at those video cameras in order to provide an alarm bell.

What we're doing is developing systems that automatically detect activities within videos like the ones I described, but also loitering at regular intervals that can suggest recon. And then flag that for a security officer.

DWG: Where do these two programs stand right now? Are they still under your control? Have they been transitioned to the services?

Dr. Matheny: Aladdin has completed and transitioned to the services. DIVA is about a year in.

Some other work that we do in the sort of general area of how to process imagery and video at scale much more quickly, one is a program called Finder that automatically geolocates an image. So if you take a picture with your cell phone, typically your cell phone is going to geotag that image. It will provide a latitude and longitude and if you upload it to a social media site, it will have that GPS lat/long. But again, if you're a terrorist or a foreign military, you'll probably disable the GPS on a camera. The goal of our program Finder was to automatically figure out where on earth a particular picture was taken. And it does that, just by using the features within the image.

So this could be sky lines, it could be geologic features, botanical features, architectural features, that help you pinpoint where on earth the photograph was taken.

And then we have a program called Core 3D which generates 3D models of buildings and cities from overhead imagery. The Air Force is again a major transition partner for this.

When former Director of National Intelligence Jim Clapper was at NGA, in building models of things like the Abbottabad compound for the bin Laden raid. That took weeks of preparation to build a highly detailed, rich, accurate 3D model of just a single dwelling based on overhead imagery. The goal of the Core 3D program is to do that in minutes.

So those are examples of some of the automation that's now possible using machine learning techniques applied to raw data.

DWG: Thank you for being here.

The Defense Department is wrestling right now with trying to get commercial industries industry and involved and working with it on new, innovative things, concepts. It

started under Under Secretary Ash Carter. But one of the walls that he kept hitting was lots of people in the American commercial Silicon Valley world don't want to be in business with generals. They don't want to be in business with spies. He was trying to reach this community. So he stood up the IUX. And he mentioned over and over again that China doesn't have this problem because they have a civil/military fusion and they're attacking artificial intelligence in a way that we are not as a nation.

Can you talk a little bit about that challenge and how you think you can enable being able to reach this commercial industry and get all the things we need out of it, and transitioned into the military before China does in 2025?

DWG: Great question.

We work a lot with industry, particularly small businesses who aren't the usual suspects in say defense of intelligence contracts, to ensure that the best and brightest are able to work on our problems. And we do that in a few different ways.

First is, we avoid to the greatest possible extent, running classified programs. So we try to find an analogy for an intelligence problem that is declassified, can be kept open. And we ensure that the process to identify who a contractor would be for a research project is fair and level and open to the greatest possible extent.

So typically, we use broad agency announcements in which anyone can bid.

For those who don't want to go through the whole federal contracting process, which is itself a war of attrition, then we run public prize challenges in which we just offer prize money for anybody who can solve the problem. They don't have to have a federally approved accounting system. They don't have to have a contracting officer go through all the, you know, a six-month process in order to award money. If they can solve our problem, we award them cash. We'll just show up on their doorstep with a duffel bag, leave it, drive off in our '67 Chevy. [Laughter]. The big check. We chronically preserve Ed McMann who comes back with the big check at your doorstep.

I think for a lot of non-traditional performers, which can include hobbyists who are basically moonlighting off of their full-time job in major technology company, or a combination of small business and entrepreneurs who are interested in like getting some reputation rewards or bragging rights for having solved a hard problem, and beaten out the big defense contractors, this is a great opportunity.

It also turns out that it's a great opportunity to get visibility into what's going on in the technology landscape around the world, because we typically leave these open to anyone in the world who wants to compete.

So that's one way we engage with not only Silicon Valley, but also the pockets of innovation that are present all around us.

I think a third way is, we run these tournaments in which we have many tens of thousands of participants. Probably our forecasting tournaments are the best example of this. We ran a four-year forecasting tournament in which people were asked to generate predictions for world events. In sum we I think collected three million forecasts from around 40,000 people and scored them all for accuracy. A lot of these forecasts actually came from companies rather than people who wanted to get those bragging rights for showing how accurate their particular tool was for assessing geopolitical risks.

And you know, we offered prizes for those who did best. But it was also a great learning experience about what sorts of events we can accurately forecast, and what kinds we really need to remain humble about. As an organization.

And then maybe lastly, as just a final example of attracting innovation, when we provide not only financial incentives and bragging rights, but also the opportunities to win pretty high cache scientific awards. I mean we've had a Nobel Prize for Physics awarded due to IARPA research, the MacArthur Prize, the Bell Prize, London Prize. This attracts people who aren't used to doing work with the defense of intelligence communities. They really want to do world-class science and we give them the resources that they need to do that.

DWG: And a quick follow-up, part of what it takes to get resources from Congress is you have to make sure they understand the threat in terms of national security, that you have to be able to have a narrative. If you start talking to an appropriator about quantum computing, that might not be the beset way to go. But typically what does work is when you tell them here is who is starting to catch up with the United States.

Dr. Matheny: Yeah.

DWG: What nations are starting to catch up with the United States in terms these capabilities, AI in particular. And what would you tell an appropriator from Ohio that he or she should be worried about, why we need to keep getting resources to study this

area.

Dr. Matheny: Right. China has been very thoughtful about how to pursue research and machine learning, or AI. Has an AI development plan which is I think reasonable, sets concrete targets. It's basically a Chinese translation of the U.S. AI plan, which I worked on. There were a lot of familiar passages in the China plan. But they've also introduced an implementation plan for that AI Strategy that includes quantitative milestones in speech recognition and imagery analysis and video analysis that are I think are realistic, but also ambitious.

They also, as you noted, enjoy a tight integration between industry, academia, and government. But that can also be a disadvantage.

So I think they're our strongest competitor globally in machine learning, but I think that the United States has an advantage in its competitive landscape in machine learning. We have the strongest universities by far in machine learning research. We have the strongest start-up culture. And we also have risk-tolerant companies like Google and Microsoft and Amazon and Open AI that are willing to fund very high-risk research that may not pay out for five to ten years, that's beyond the investment horizon I think of most organizations.

And then lastly, you know, we get risk-tolerant federal funders like IARPA and DARPA and NSF that have historically funded most of the early stage development of the tools that are now widely deployed in most of our smart phones. It's kind of like break the smart phone apart. Most of this goes back to federally funded research from decades ago.

So those are advantages. It would be good not to lose those comparative advantages. So one thing that concerns me is that we not suffer brain drain from our universities. Since we are the global strong attractor of talent into our university system, you know, there's the John [Holdrum] line about the best thing we could do for national security is staple a green card onto every degree we award from a U.S. university. There's an argument for that.

When we lose students who go back to their country of origin after receiving a degree in a U.S. university, we hurt ourselves doubly full. First is we lose the talent that we helped to create, often with a federal subsidy; and second, is we've just advantaged our competitors by giving them somebody who's received extraordinary training.

DWG: I wonder if you can explain a little bit more about the [inaudible] programs that [inaudible]. And [inaudible] obviously something that has to [inaudible]. And then [inaudible] which [inaudible] modeling [inaudible]. So within a range of [inaudible], I'm sure there's a huge [inaudible].

And then a follow-up, you mentioned [inaudible] around the world. Are you working with teams from China, Russia? And what is their contribution?

Dr. Matheny: To just answer your last question first, yes, we have funded teams in China and Russia. Not only have we benefited from the work that they've done, but we also now have better insight into the state of research in those countries.

The work that we funded in cognitive psychology has really been along two tracks. First is to diagnose the kinds of problems in human judgment that we all suffer from. Certain kinds of biases and [inaudible] that probably made a whole lot of sense on the African Savannah, but probably don't make a whole lot of sense in a world with thermonuclear weapons or cyber weapons.

So an example is confirmation bias, which is fairly universal, which is the tendency for humans to seek out information that confirms their existing beliefs rather than disconfirms it. And that turns out to be a real problem if you're an analyst.

So we've done work not only in faster diagnosis of instances of confirmation bias but also how do you counter it.

So one program that we had called Serious used various kinds of games to reduce these cognitive biases in analysts, and pretty substantially, including confirmation bias. Just getting analysts to try to disconfirm their beliefs rather than confirm them.

Another program that we had called [Eights] ran forecasting tournaments in which many thousands of participants were measured for different kinds of biases, and we then examined how that affected the accuracy of their geopolitical judgment across a broad range of questions. And it turns out that the people who were most accurate were not the deep domain subject matter experts, but instead were people who had sort of high fluid intelligence, like good pattern recognition ability. They scored very highly on tests of cognitive reflection, which is really a measure of how slowly you think. That is people who are more deliberative, were a little more humble and self-critical, were likely to be more accurate. Then they were extraordinary in their degree of willingness to seek out information that contradicted their deepest held intuitions. In fact that was the

thing that was most outstanding about these people. They were informational omnivores. They would go out and try to find something that would convince them that they're wrong.

So that was interesting. And that then led to --

DWG: What makes those kinds of people?

Dr. Matheny: Professionally, they're incredibly diverse. I mean there were some, because the pool included so many thousands of people we had some really extraordinary folks like Nobel Laureates and hedge fund managers. We had, I think, the World Poker Champion. So people who understood probabilities pretty well and had a well calibrated sense of their own uncertainty.

But we also had pharmacists and grad students and Uber drivers who also participated. It was diverse.

I think people with a quantitative bent were over-represented probably among the highest performers. But the so-called super forecasters, the people who scored highest in this tournament for the entire four years were people who are distinguished most by their cognitive thinking style rather than by their profession.

By the way, there's a whole book now about this research project written by Phil Tetlock and Dan Gardner called Super Forecasting, which is just about the tournament and the outcome.

Lastly in the area of cognitive psychology, we ran a program called Sharp which was aimed at enhancing human reasoning skills using kind of non-invasive neurotechnology. So things like electrical stimulation using like skull caps that could deliver mild currents or mild magnetic fields; various forms of sleep enhancement and reflection. None of it worked. [Laughter]. It
was so humbling for us.

I think this is one of the important things that we do, is try record all of our failures as rigorously as we brag about our successes. We should be talking about what doesn't work. And this was a program that was such a successful failure because we learned so much about all the things that people had speculated about possibly being able to enhance intelligence with. Or some folks were already selling these kinds of technologies. We were really interested to see how much of that was just creative

marketing. And it turns out, it's really all creative marketing.

To your excellent question about what of this could actually help us understand Kim Jung-un. I don't know that any of it would help us in building a mental model of him individually. What it could help us with though is for the difficult job of intelligence analyst, to try to say predict the outcome of negotiations, one of the important findings from our research is it makes sense not to just ask one intelligence analyst or get a bunch of intelligence analysts in a room to deliberate, but instead ask say 100 or 1,000 and basically take the average. That's likely to be more accurate than getting a deliberating group together or relying on a small number of experts.

DWG: Mark, then Dmitry.

DWG: Thanks for doing this.

Quantum computing has been described as sort of the cornerstone [inaudible] several years. I'm wondering if you might be [inaudible] the landscape, which adversaries are investing in that, [inaudible] effort in quantum computing.

Dr. Matheny: This is an area in which I think the U.S. has a lead in part because of a large investment by the federal government in quantum computing research as distinguished say from other areas of quantum information science like quantum communication, quantum sensing. But quantum computing, we do have a lead. China is investing, but not at the levels that the United States is.

There are many potential applications of quantum computing. The one that makes it a security concern is that quantum computers could factor large numbers very efficiently, and most widely deployed encryption systems such as those that protect our email, that protect banking, that protect e-commerce is based on encryption.

I think we're still 20-plus years away from a quantum computer that's relevant to encryption, so we have enough time to think about what forms of encryption we should be employing that aren't based on the difficulty of factoring. Still, I mean I think we need to be doing more research on quantum resistant encryption. There's some research today. [NIFT] and NSA both have publicly called for proposals on how to do encryption that would be quantum resistant.

The other benefit of quantum computing, or the other application, includes being able to solve really hard problems in chemistry. For example, most of the world's fertilizer, and

therefore most of the world's food, is produced using something called the Haber-Bosch process which is close to a century old, and it's very energy intensive. Something like five percent of the world's energy is applied to producing fertilizer.

If we could instead create a catalyst that fixes nitrogen, we would be able to dramatically reduce energy use, much more efficiently be able to grow crops, and in principle, one could use a quantum computer to design such a catalyst. There are other applications, too, solving very hard optimization problems and machine learning, solving hard scheduling and logistics problems, coming up with simulations of molecules that then could aid in drug discovery and drug development, and probably even more applications that we'll discover once we have quantum computers. But I think it will be some time before we have computers that are relevant to these applications. It's just a very hard physics problem.

DWG: How big of a challenge is it if our adversaries get there before we do? What would that mean for the security environment?

Dr. Matheny: Yeah. It wouldn't be good. [Laughter]. And it would be good not to be surprised. Right? So one of the reasons that we invest is so that we understand where the state of the art is, understand a bit about what the time lines are, so that we can deploy quantum resistant encryption when it's critical.

But given that we want to protect classified data for 20-plus years typically, by policy, does mean that we should probably be pursuing quantum resistant encryption with a lot of energy.

DWG: Doctor, I had a question about peer competitors which was asked by Katrina, and I wanted to view it another [inaudible]. Since you confirmed that you do finance this sort of research in Russia and China as well, could you say in which fields? If you're allowed to do that.

And also, how do the Russians and the Chinese respond to that? Do you have to mask this sort of activity? Or they just don't care?

Dr. Matheny: AS far as I know, they don't care. I mean these are publicly announced awards. And the areas in which China and Russia researchers have done especially competitive has been in data analytics, machine learning.

Russia in particular, which has many outstanding mathematicians and computer

scientists, we've seen a lot of sort of moonlighting activity of Russian mathematicians associated with universities who want to compete on many of our prizes.

DWG: Could you also say what other countries that you do most of your research with, you know, just --

Dr. Matheny: If we looked at sort of a map and kind of, a heat map of where --

DWG: Yes.

Dr. Matheny: So the United States by far leads, and then probably second would be the UK. Third might be Canada or Germany. And by the way, I'm happy to look these numbers up. It's been a while since we have. We spend a lot of research in Scandinavia countries, a fair amount in the Netherlands, a lot in France. A lot of physics research tends to be fairly widely distributed, because a lot of countries have decided to specialize in a particular kind of instrument or infrastructure which then is unique in the world, and so any research on that particular problem will end up involving that instrument.

And then for machine learning research and data analytics and things like linguistics which we also invest a lot in, that tends to be so widely distributed. I mean we fund work in South Africa, we fund work in Brazil, we fund work in Australia. So we've got most of the continents covered. We're still looking for our Antarctic research project.

DWG: Yes, sir. When you're talking about programs like Aladdin that have to do with, you know, head of these large gobs of data, a lot of times you're talking about pulling data from systems even within the same service that themselves aren't interoperable.

Dr. Matheny: Yeah.

DWG: How do you overcome, how do you create an AI that can sort of reach into all these disparate systems? That must be a major challenge for you.

Dr. Matheny: Yeah. It's less of a technological challenge than a bureaucratic challenge. Unfortunately, we don't have the technology to solve that problem because we're bound by the laws of physics, and most bureaucratic problems exceed the laws of physics.

It's a real challenge to get data in the right place, and one of, so in the case of the intelligence community, you not only have policy challenges, you've got human

intelligence and imagery intelligence and signals intelligence and they come from different agencies with different authorities. And having those datasets collocated in the same place, a real challenge.

But then there's another problem which is the volumes of data, the rates at which the data are coming in. It means that you have to either sample from the data, and then how are you sampling? Are you doing random sampling? Are you doing over sampling?

I'd say one thing that has been transformative for the way that we fund research since we're doing it mostly unclassified is cloud computing. So commercial cloud computing, whether it's Amazon or Microsoft or Oracle or Google or whoever, has created an infrastructure that allows academics and hobbyists and startups to have essentially supercomputers at their disposal for short periods of time.

So they're now able to simulate what it's like to be in an intelligence environment in which you do have very large data sets. In some ways, though, they have the ability to collocate data in a way that no intelligence agency has.

The difficulty for us often has been translating their tools into one in which now we have to operate across 17 agencies.

DWG: Just switching gears a little bit.

Could you sort of elaborate on how you deal with the issue of intellectual property when you run these competitions?

Dr. Matheny: Great question.

So we leave it to the inventor. We do not, we don't ask the inventor to give up their intellectual property. For a couple of reasons. One is, we think ultimately the technology market benefits from ventures holding their own IT. Second, we find that when we ask for the IT it has a chilling effect on participation rates, particularly for the people who we really want to attract, who are the entrepreneurs and small startups.

DWG: Gopal.

DWG: Thank you. I was going to ask a question, but he asked it. But I want to ask a different version of the question.

You said you do attract a lot of companies that are from Russia and China. How do you vet them? How do you know they're not a front for those countries buying and selling things?

Dr. Matheny: We do vet them. We look through the various State Department lists that are managed to try to spot fronts, to make sure that they're not on that list.

DWG: When you fund research in other countries, what's the next step of, I understand that most of it's in the unclassified commercial world. That's the kind of research you're funding. How does the intelligence community in the United States tap into that particular [inaudible]?

Dr. Matheny: It varies by the research project and the sort of state of maturity of the technology. But in cases like machine learning. To give an example, we had a program called [Fable] that did automated speech recognition in any language on earth. So if you take a tool like Siri or Amazon Echo, those are tools that benefited from years of development and are tightly focused on a small number of languages that are of certain commercial interest because they have large numbers of wealthy consumers, a lot of web advertising, et cetera. Most of the languages that we have to work with are ones that have relatively small numbers of speakers, that aren't very attractive to large companies, and we don't have years of development time. I mean if there's a crisis in a region of the world in which we don't have speech recognition systems, we then have to develop that very quickly.

So [Fable] develops the speech recognition systems in days for any new language with a small amount of training data, about ten hours of transcribed data. Which is whatever that is, a thousand-fold improvement on the state of the art. That was a real breakthrough. And those tools went directly to the intelligence agencies. So the technology all went straight out because it was finished, it was ready.

But if you take another example, say our work in neuromorphic computing. We have a program called Microns that aims to reverse engineer how the mammalian brain learns, since it appears to be very different from the way electronic computers learn.

For those of us who have had kids, you know, if you're teaching a kid to recognize what a coffee cup is, the kid doesn't have to see a thousand examples of coffee cups. And yet that's how like most machine learning classifiers work.

So what is it that the kid is able to recognize in the category of coffee cups that makes

the kid much more efficient? And the kid is only using about 10 watts of power, depending on like how much breakfast cereal the kid has had. And usually our computers are consuming a thousand to a million times that amount of energy.

So we have a program called Microns. It's really aimed at understanding how mammalian brains are so efficient. That's a program that's very early stage. The outcome of that program will be an improved understanding of neuroscience that might lead in 10 to 20 years to the next generation of high performance computing. That will not transition in the way that [Fable] did.

So the transition path really depends on the technology and the problem, but in general, about half of what we fund ultimately does make it to an intelligence agency.

DWG: You earlier talked about [inaudible]. I asked this question a couple of weeks ago to the Director of DARPA as well. There seems to be a lot of hand wringing that the United States has done on falling behind on AI, China's going to beat us, we need to do more. And the Director of DARPA said that he would put the United States efforts against anyone else's in the world.

Are we talking just about, just an artificial [inaudible] here? People just getting wound up about someone else doing more? What's your sense of, if you will, rack and stack U.S. efforts with the others. Where do you think the United States stands on that?

Dr. Matheny: I think the United States does have a healthy lead. And I think by most measures, if you look at the most highly cited research, if you look at the fundamental breakthroughs in machine learning say in the last few years, like reinforcement learning, generative adversarial networks. Those have been due to U.S. funded research.

So I guess I'm not a catastrophist when it comes to the race between the U.S. and China. I think there is a tendency to be a little bit of alarmist whenever we see technology advances by another country. I mean Japan in the '80s is another example of this, but we've also got, you know, examples of the bomber gap that didn't exist, the missile gap that didn't exist, the submarine gap that didn't exist.

I do think, though, that because right now we're privileged to have a lead, it doesn't mean that we're guaranteed to have that lead forever, and regardless of policy or investment. This is a lead that was earned through it being a priority within science and technology organizations. It's because federal R&D organizations recognized that machine learning was important and we allocated funding to it. It's because companies

recognized it was important, and U.S. universities recognized it was important, and we need to continue recognizing it's important in order for us to maintain the lead.

DWG: Does AI develop incrementally? Or is it something that could break out? Six months from now could China be ahead of us in some significant way?

Dr. Matheny: The great thing about scientific discovery is that it's surprising. And because it just depends on human ingenuity, and that ingenuity isn't deterministic. You're constantly surprised by some discovery. I don't think anybody predicted the creation of generative adversarial networks as an approach to building very strong levels of play and machine learning.

Or like Alpha Zero, which I thought, by Deep Mind, which I really think is a fundamental breakthrough. I mean just being able to demonstrate that you can have essentially self-play without any prior experience. Simply knowing the rules of the game. And you can take that approach and not only achieve super human levels of Go play, but also chess and backgammon, et cetera. So I think that was a real breakout. It was one that I don't think anybody predicted. And if you looked at kind of performance trends, you wouldn't have predicted it.

The same is true in biology, by the way. I mean I don't think anybody predicted CRISPR-Cas9 as far as I know.

So that kind of technological surprise is probably for intelligence analysts somewhat sobering. The fact that they can't predict these kinds of events.

The main thing, though, is to recognize these breakthroughs when they happen and try to understand the consequences that they'll have for security issues as well as for all the extraordinarily positive applications that these tools will have.

DWG: I was wondering if you could go over some [inaudible]'s work. Biosecurity [inaudible], or where you see that program going.

Dr. Matheny: Oh, yeah. So this is an area where we've invested a lot more recently. So in general, I'm really optimistic about the advances in biotechnologies and their applications to improve human medicine, agriculture, energy, materials. But there are also some downside risks.

Some of the risks are deliberate mis-use of these tools to create novel biological

weapons. But I think probably a greater risk is accidental misuse of these tools. Either laboratory accidents that release pathogens or simply unintended consequences of novel organisms that are released into the environment.

To give some examples of that, a couple of months ago the first pox virus was created from scratch. It was horse pox, but it's the same length as smallpox, and the exact same approach that was used to synthesize horse pox can be used to synthesize smallpox. And it was synthesized for $100,000. Which means in principle, that somebody with $100,000 and some technical sophistication could create a pathogen that killed somewhere around 200 million people in the last century, killed around 50 million people per year until it was -- I'm sorry, 5 million people per year until it was eradicated. Because there's no background immunity to smallpox anymore, and most of us have not been vaccinated, it's a real problem. And the fact that somebody can develop something that's as powerful as a hydrogen bomb, more powerful than a hydrogen bomb, for $100,000 using commercially available equipment is I think a real security risk. And that's why we increased our investments in biosecurity in a few different areas.

One is a program called FUNGCAT, which is sort of a biologist [N] joke, GCAT being the basis of DNA. It stands for Functional Genomic and Computational Assessments of Threats. We're not all that great at acronym generation. It's something we've been trying to apply machine learning to. Or at least better human judgment to. And we in that program are aiming to automate the screening of DNA sequences that are intended for synthesis. It turns out that right now most synthesis screening is completely voluntary around the world. And there are big gaps in the way that we screen this.

In the UK actually, there was a, I think it was the Guardian did a sort of like mail order red theme, where they went to a bunch of different DNA vendors and ordered pieces of different pathogens, and all of the orders were filled. It was really terrifying. And I think this is still a problem. So if you either split up your orders for DNA or you make your orders sufficiently small so that they don't get screened at all, you could order some bad pieces of pathogens. The goal of FUNGCAT is to prevent that through improved forms of automated screening.

We also have a program called Felix which is focused on detecting engineering within genomes. Can you tell whether this circulating influenza strain is naturally occurring or whether it's been engineered? And given the kind of research that's going on right now in biology, often in university labs that's focused on so-called gain in function research, trying to enhance the virulents or communicability of influenza strains, which I think many of us believe is foolhardy, but it's intellectually interesting, so a lot of researchers

are doing this. It's really important now to understand whether an influenza strain or some other virus is of natural origin.

DWG: Is this an area that [inaudible]?

Dr. Matheny: I would love to see our competitors invest more in bio-security. This would be a constructive form of competition. Yeah, let's all try to be the world's leader in bio-security. Every country would benefit from enhancing the protections and countermeasures that we have to various kinds of biological threats, natural and otherwise.

We have something called the Cooperative Threat Reduction Program for nuclear security and a small amount for bio-security in which we recognize that there are cooperative gains from, you know, trade and joint investment in nuclear security. Like putting locks on nuclear weapons, ensuring that we all have better early warning systems so that we don't miscalculate. I think bio-security is another place where it would be good for all of us to jointly invest.

DWG: I'd like to go back to [inaudible] data and the program Aladdin that you've already [inaudible]?

Dr. Matheny: Yeah.

DWG: Is reliance large on cloud? Cloud [inaudible]. How is that this arise? Is it secure, the cloud?

Dr. Matheny: Aladdin, the unclassified research part of it, was focused on things like can you identify videos that involve break dancing. Which I'm happy to say you can. And in that research we weren't concerned about securing.

Now those tools have transitioned to intelligence agencies that operate their own cloud, that's completely separate from the public cloud.

DWG: But is cloud securable?

Dr. Matheny: That's a great question. So in the narrow case of the intelligence community it has it own cloud infrastructure that's completely air gapped, in which its own computers are protected, you know, and all that. So that's secure in the sense of being completely cordoned off from the rest of the public cloud.

As to whether the public cloud can be made secure is a really important question, and it's one that we've started investigating. We have, we put out a request for information which we often do when we want somebody else to do our homework for us. And we ask how can you make public cloud computing more secure, to various kinds of attack, to data exfiltration? Also, how can you, how would you ensure that if somebody were misusing the public cloud, for example, running nuclear simulations or using it to break encryption, how could you detect that?

So we've been talking about this sort of idea of classified as a service. Is there a way of creating instances within the public cloud that are just as secure as say the intelligence community's computing but without the costly infrastructure, the guards and gates and guns that are needed to protect that infrastructure?

So stay tuned. I think there are approaches that we'll be exploring soon.

DWG: And what is your annual budget? How much do you --

Dr. Matheny: I wish I could say. It's classified right now. We and others have asked that it be declassified. The top line intelligence budget has been declassified, but they haven't yet declassified the sub-budgets. Sorry.

DWG: How about the amount that you give out in awards? Is that releasable?

Dr. Matheny: That's also classified. Sorry.

DWG: Are there any numbers connected with your budget that are not classified?

Dr. Matheny: That about 85 percent of what we fund I think right now is unclassified. That percent is unclassified.

It's deeply frustrating, especially for scientists and engineers who in general believe that there are benefits from a high degree of transparency. That is like sort of having other eyeballs on your set of problems will ultimately advance the solutions to those problems. But there's this difficult tradeoff of course that we have with security.

DWG: Sir, you just mentioned something I've never heard before, and that's classified as a service?

Dr. Matheny: Yeah.

DWG: Can you maybe elaborate on that?

Dr. Matheny: Yeah. The whole idea is unclassified.

The question is, so you've got like, let's say you talk about Amazon web services. And right now the financial sector has been reluctant to use cloud computing to a greater degree because they're not sure, really, what its security properties are. How difficult would it be for somebody to rent time on a machine that's right next to yours and possibly do a side-channel attack? And what sorts of security guarantees, kind of like [IFSO] standards can you provide for cloud computing where you're not in charge of the infrastructure.

So classified as a service is looking at a variety of different approaches, sort of data diode approaches, randomized assignment of machines so that you could never know where somebody else's data was being processed, which would prevent side channel attacks, and also being able to provide encrypted containers around data during processing.

There's another approach that we're pursuing in a program called Hector which is focused on homomorphic [inaudible] encryption which is really such an intriguing and powerful idea in cryptolography in which you're able to process encrypted data without ever decrypting it.

So most of the time if you're performing a calculation or like a search on data, you have to decrypt it before you perform that operation or that search, which means then whenever you're doing something useful with data, the data is vulnerable. And virtually all computing systems work this way, which is one of the reasons that people are concerned about say electronic health records or census records or anything else, is that you have this personally identifiable information that at various points in this processing is left sort of undefended.

The intriguing property of homomorphic encryption is that you can keep the data encrypted entirely, from birth to death, while still doing useful things with it. So for example, if CDC were interested in counting the number of flu cases by looking at electronic health records, the health records could be kept encrypted. CDC would simply be able to sum the number of people who had the flu without decrypting all of the other health information within those records.

This has a number of very powerful applications in protecting privacy while still allowing useful computation. So that's another area that we're investing in.

DWG: Where are you with that program?

Dr. Matheny: It's just starting. I think we're still in the middle of contract awards.

DWG: Thank you.

DWG: You mentioned the formal process of requesting [information] [inaudible] and another request for something to identify special [inaudible]?

Dr. Matheny: That's right.

DWG: Can you talk a little bit about that program, also about that process? What happens after you request the information?

Dr. Matheny: Requesting information through these formal RFIs that we release is something that I think we should be doing even more of. The responses that we get back are so thoughtful and so helpful in steering us to the most important technical problems where we need to invest.

What we do is we pose a question that we don't know the answer to in advance, like what new developments in nuclear sensing would allow us to detect nuclear material from longer standoff distances? Because this is a problem that obviously is of high priority, but there hasn't been a whole lot of really great new ideas in a few decades, and we need some great ideas.

So we put the question out there. We spam, basically, as many people as we can with the request, including in places that we think might be overlooked. So academic departments that might have a viewpoint on nuclear sensing, people that focus on different kinds of approaches to this problem that might use standoff magnetometers, or might look for single fault upsets within microelectronics. Lots of different approaches to this problem that aren't conventional.

And then we collate all the answers. We look at where are the places that we're already investing, what's the reasonable degree of skepticism about this new approach that somebody thinks is going to be successful, what would it take to build out a research problem to figure out whether this would work or not?

So that's how we sort of use the results. We often then fund workshops and then the people who sent us responses have some sort of pride of authorship in having laid the groundwork for a future research investment.

DWG: So pride in authorship. Is there any formal relationship that's established at that point? Or is it --

Dr. Matheny: No. Very often the people who respond to our RFIs will later send in a proposal for funding on that problem. And in a way, if they've helped us steer the problem towards the area in which they think the most likely solution exists, then they're sort of, their proposal is going to be more competitive which is probably why there's a certain enlightened self-interest in responding to some of these RFIs. But there's no formal relationship that exists. They don't get funding for responding to the RFI.

DWG: Where do the questions come from? Are they internal questions within IARPA? Or --

Dr. Matheny: Sometimes we get them from other places, that they'll ask us. That's a really good question, we don't know the answer, we'll put out an RFI. But they're questions that we're genuinely interested in answering. We don't use this as like an information operation. This is something that we're sincerely interested in knowing the answer to.

DWG: Thanks.

DWG: We are out of time now, but I want to say thank you. This was really interesting. You guys are working on a lot of fascinating stuff, so I appreciate your time and your insights, and we'd love to have you back.

Dr. Matheny: Great. Thank you so much for all the great questions. I appreciate it.

***