**JASON MATHENY**

**CRAIG:** Hi, I'm Craig Smith, a former New York Times correspondent and host of the podcast, Eye on A.I. I'm also a special government employee at the National Security Commission on Artificial Intelligence. And in this role, I'm serving as the host for NSCAI's podcast series on the commission's work. This is the fifth episode of six, looking at the commission's first quarter recommendations to Congress.

MUSIC

In the 2019 National Defense Authorization Act, the Congress established the National Security Commission on AI to consider the methods and means necessary to integrate artificial intelligence into the national security and defense needs of the United States.

The commission consists of 15 commissioners selected primarily by Congress and is led by former Google Chief Executive Eric Schmidt and former Deputy Defense Secretary Bob Work.

Last month, the commission issued its first recommendations to Congress covering seven lines of effort, six of which are public and one of which is classified. We spoke with the commissioners leading the unclassified groups about their recommendations.

In this week's episode, I talked to Jason Matheny about his line of effort. regarding cooperation on AI with key allies and partners. He spoke about his group's recommendations that the government established a senior national security point of contact for AI and convene a multilateral working group for AI collaboration and interoperability as well as the need for AI war games.

I hope you find the conversation as remarkable as I did.

MUSIC

What I'd like to do is ask you to introduce yourself and talk about your journey to where you are today, where you grew up, what kind of jobs you've held, and how that has sort of culminated in your position as a commissioner. And then we'll get into the questions from there.

**JASON:** Sure. So, I grew up in Louisville, Kentucky. I had planned on being an architect. I went to college in Chicago and I worked in Cabrini green, which is the housing project in Chicago. And it seemed like we could do better in designing public housing that was more humane, more livable. So., I went to architecture school and then about a year and found an orphaned copy of the world bank's world development report, which contained league tables on how many people died of preventable diseases and how cost-effectively you could prevent those diseases. And I was just stunned that, you know, there were on the order of 20 million deaths a year due to infectious diseases, many of which are preventable. I thought that seemed like a really important problem to work on. And then I spent the next 10 years working international health.

I went to school for epidemiology and worked on infectious disease control. About 10 years in, I was working in India and we were evaluating what kinds of treatments and preventive approaches we could try for HIV, tuberculosis, and malaria.

And while I was there, the first virus was synthesized from scratch at a lab in the United States, really as a demonstration that you could chemically synthesize viruses de novo and this was sort of an 'Oh crap' moment for the public health community.

And their reaction to this was, it's going to be a matter of time before some sophisticated misanthrope decides to synthesize smallpox and reintroduce it to the world or synthesize something worse. And so, I moved then to work in national security first at the Center for Biosecurity at Johns Hopkins, also the Applied Physics Laboratory at Hopkins.

I worked on some projects for the Pentagon. And eventually came into the intelligence community and an organization that had just started called IARPA, which is the advanced research organization for the intelligence agencies. So, I spent about 10 years at IARPA developing new technologies that could address emerging threats from biology, but also other technologies. And then I retired from government about two years ago to start a new think tank with Georgetown university that's looking at the intersections of technology, policy and national security.

About that time that we were standing up this new center, the National Security Commission on AI was stood up by Congress and I was privileged enough to be a part of this commission.

I'm really grateful to be here today to be able to tell you about some of the work that we've done.

MUSIC

**CRAIG:** So, on the commission, a couple of things jumped out at me, and the most interesting or the most dramatic was the talk of having AI war games. And I wondered how that would happen, whether that would be virtual or whether you would actually have AI enabled hardware in a war game situation. The report opened with a mention of swarm technology, and of course, I imagine dogfights between drone swarms.

So, can you talk a little bit about what an AI war game would entail.

**JASON:** There are many different formats for war games, but the fundamental goal for all of them is to explore different approaches to addressing some competitive challenge. And whether that challenge is fighting a war, for example, a war that involves drone swarms or deterring the war, managing the consequences of a cyber-attack or contending with a pandemic, war gaming allows planners to learn lessons at a relatively low cost and allows them to test out different strategies that may look good on paper, but once you play them out with intelligent competitors may not survive first contact. And you want to learn those lessons first in a game rather than in a war.

**CRAIG:** Is this virtual that you're talking about or are you talking about having AI enabled hardware in the field?

**JASON:** Well, we didn't specify in part because we didn't want to micromanage a war gaming effort, so we left it general. But I think one thing that the commission did find is that there have been very few wargaming efforts to date, whether those are field exercises, whether they're tabletop exercises or other simulations.

We need to do more testing of strategies through gameplay, and we need those war games to involve our allies and our partners so that the first time we're collaborating together and building strategies and testing them, is not in an actual crisis.

**CRAIG:** Can you talk about specific ways that the US can expand allied cooperative planning and interoperability and some of the other things that you talked about in AI enabled war fighting and intelligence efforts.

**JASON:** Most of the US allies and partners have been making investments in AI, starting to develop doctrine and strategy around AI. But we've been doing so largely in isolation from one another and we need to do this in a way that is more collaborative, more in sync. We need to assess where we are with our allies, where we need to be, and set a path to get there.

And in doing so, we need to cover issues like shared computing resources. What computing environments can we now collaborate on with our allies? What models and datasets can we share? What are the standards that we should building new technologies towards to ensure that they are interoperable or they are agnostic to say, a networker database structure, so that they are by design ones that are going to be operable on multiple networks? And we need to do this together with our allies and partners rather than bolting our allies on at the end.

**CRAIG:** And in the recommendations you say US allies and partners need to enhance and expand interoperable battle networks in order to offset the capabilities of potential adversaries to employ such networks in ways that threatened to defeat US and allied power projection. Can you give an example of an interoperable battle network?

I mean, what are you talking about precisely? Is there a use case that you could give that would clarify that for listeners?

**JASON:** Sure. So, a military example would be for the US allies and partners to maintain networks that provide a shared picture of a battle environment. For example, that your intelligence surveillance and reconnaissance data share raw sensor data and target information, target tracks and share effects reports.

And I should mention, you know, that the need for these kinds of interoperability and shared networks isn't limited to military systems. We also need the same kinds of interoperable and shared networks for early warning of pandemics and natural disasters so that we can address these crises together.

**CRAIG:** In what way can adversaries employ their networks to threaten or defeat US or allied power projection? What are you talking about there? When you talk about them employing their networks, how does that relate to whether or not allied networks are interoperable?

**JASON:** So, you know, one advantage that the United States has is that we have true friends in the world. The friends that China and Russia have are generally transactional friendships that are temporary and based on a specific relationship like an economic one.

Whereas we have allies that share a set of values around democratic principles, that share a set of beliefs about what's needed to restore the rule of law globally and ensure an economy that works for the benefit of all as opposed to the benefit of a few. And I think that the sort of advantage that one gains from having true allies, also presents a challenge, which is if you have allies, which operate a range of different technology standards and use a variety of different network protocols, you're going to have to spend a lot of time thinking about how to allow these technologies to work together.

So, our friendships are not costless. They involve some overhead. Our competitors don't have those kinds of friendships or alliances, which presents some disadvantages to them. Some significant disadvantages in that if a crisis arose that they would largely be on their own. But their networks would be highly integrated because it's simply one country with central command authority that is using that network. Now, the ways in which adversaries can potentially use their networks in ways that are quite challenging to overcome, varies based on the kind of domain and the kind of scenario. But one of the challenges that I think is unique to AI is that right now, most AI systems are very brittle. They're pretty easy to defeat with a low level of sophistication. And if you're interested in taking down an AI classifier that's at the end of an ISR system, for say, image recognition, that doesn't take a whole lot of effort right now.

So, if you're on the offense right now against AI systems, you have an advantage. There simply hasn't been much research on how to prevent spoofing or other kinds of attacks on AI systems. So that I think there's one area where the U S and its allies will need to significantly increase their investments.

**CRAIG:** And to make it even more concrete, if you have a computer vision enabled drone, for example, it would be pretty easy to fool that computer vision system with different kinds of adversarial attacks, right?

**JASON:** That's right. Spoofing imagery is probably the most mature, these kinds of different attack vectors. You can also fool different video classifiers and you can cool audio classifiers. You can fool text classifiers.

So, these kinds of attacks in some cases are pretty robust against a range of different sensory data. And I think the challenge has been the defenses are not as robust or as generalizable. This is an area that the commission has described in its first report, and we're likely to pursue in our future reports: the need for increasing investment in AI security, AI assurance, AI robustness.

So that the systems that we do end up deploying are ones that are much more difficult to spoof.

MUSIC

**CRAIG:** In the report, it says that the Defense Science Board has concluded that the way to offset competitive networks is to inject AI and autonomous systems into our battle networks. What does that mean? Inject AI and autonomous systems into the battle networks?

**JASON:** I think it can vary, again, depending on the domain and the scenario, I think that there'll be very few instances where you would want a completely autonomous system in a battle network. But there are many cases where AI can help a human user interpret data or to flag data for a human user that might otherwise not be detected.

So, for example, one way of embedding AI within the system would be to flag a missile alert based on different kinds of sensory data that individually are ambiguous, but collectively suggests that in fact a missile has been launched. That's important for different scenarios where you may not have a definitive warning from a single sensor, and particularly as sort of missile designs are meant to evade certain classes of missile warning systems, we're going to have to use some form of sensor fusion that's AI enabled in order to alert the human operator that a missile has likely been launched.

**CRAIG:** And the question is, of course, then when the military starts talking about autonomous systems, people get nervous. Has there been any discussion of where lethal autonomous weapon systems fall in the commission's recommendations?

**JASON:** So, the commission is discussed legal, autonomous weapons or LAWS with defense organizations, with civil society organizations, with ethicists, legal scholars. We've had many meetings now on the topic. The commission hasn't yet written any conclusions on LAWS, but it's a topic that we'll take on in our reports before March of 2021.

**CRAIG:** When you talk about networks in general or battle networks, can you give a sense of the scope of what that means?

I mean, you're talking about different sensors and detection systems. For example, as you mentioned, with trying to detect missile launches. You're also talking about troop movements on the ground or assets on the ground. But I would guess, and that would extend to cyber activity or probes into infrastructure networks in the United States.

Is there some way that you can describe the scope of what's considered a battle network?

**JASON:** I think all of the example that you gave are right. are all examples of battle networks? It's any form of network that's helping command and control decisions regarding the conduct of a battle, whether that's in physical space or in cyberspace.

**CRAIG:** One of your recommendations is a national security point of contact. Would that person then presumably, or that office, be the one that would gather this overview to ensure that there's interoperability with allies in all of those various domains?

**JASON:** I think one of the responsibilities for sort of a national security point of contact is to ensure that their activities with the United States and its allies that are building towards a common operational doctrine for the use of AI.

And that includes building towards the same standards, having cooperative research programs that are aimed at interoperability, finding interagency agreements that allow us to share data and share models. All of those issues require not only a single point of contact for the US to help coordinate, but also a single point of contact with our individual allies.

One of the things that we heard repeated by our partners is that when they have a question about what a policy is on a particular point in the United States, they usually don't know where to go, and they usually end up having to ask many people before finding out where the belly button is. So, one of the goals of having a national security point of contact, probably housed within the executive office of the president, is that there would be an obvious counterpart for the allies to raise discussions about AI policy and AI doctrine. Now, below that level, obviously there will need to be delegation to people who are covering either the details of a particular military or non-military use of an AI system that has some relevance to our allies. But right now, we don't have that single point of contact at the EOP level.

**CRAIG:** And presumably that would be in the National Security Council.

**JASON:** Yeah. That's our recommendation, that the point of contact should be at the level of the deputy assistant to the president with sufficient authority to convene departments and agencies at the level of NSC deputies. And that person should have the responsibility of developing assessments of comparative strengths in AI research and applications, and manage a multilateral working group for AI collaboration and interoperability. But the person really does need to be able to convene interagency groups in a way that the NSC has historically had responsibility for.

**CRAIG:** In part of your work, or in developing these recommendations, you have had a lot of discussions with allies. Is that right?

**JASON:** That's right.

**CRAIG:** And is there any, not to single anyone out, but are there some countries that are more advanced and have integrated AI into their national security structures more than others?

**JASON:** Well, I'm actually quite bullish about the United States.

I think we've been a center for innovation globally in AI and in computing generally. But we're also fortunate to have allies who were also in say the top 10 of global talent in AI. The United Kingdom has a number of strong organizations, including the Alan Turing Institute and DeepMind, which is an organization within Alphabet that is located in London and draws on mostly UK and European talent and by most measures among the top two AI labs in the world, the other one probably being OpenAI, which is based in California. And then Canada has historically played a really important role in deep learning due to some kind of historical accidents of some of the early deep learning researchers moving to Canada and attracting the leading talent in that particular area of AI research.

Now you can sort of trace the genealogy of much contemporary AI research to Canadian labs, and they continue to do some of the world's best research. So those are two that are, I would say among the top 10. But you also have really outstanding research in countries like France and Germany. You see excellent work in semiconductor manufacturing equipment in the Netherlands and Japan. Taiwan, of course, is producing most of the world's semiconductors through its TSMC Foundry. So, you've got a substantial amount of relevant work in AI and computing being done by the US and its allies. Collectively, most of the world's AI research, AI talent and AI relevant compute is represented in those countries.

So again, when you combine the US and its allies, we have a really enviable position.

**CRAIG:** Ironically, the reason Canada is such an AI powerhouse is because Geoff Hinton didn't want to take DARPA money at Carnegie Mellon, and CIFAR offered him a position and he moved there and then that genealogy that you're talking about largely descends from him.

Taiwan has become so dependent on China. It's moved a lot of its manufacturing to China. Is there a concern about that, about being so dependent on foundries in Taiwan for chips that go into U S systems when Taiwan is in such a vulnerable position economically and militarily vis-a-vis China?

**JASON:** There is concern about that. I think that's one of the reasons why, in our last report, we included a recommendation for the United States to increase its ability to do onshore manufacturing in leading edge microelectronics. An area that we see as really fundamental to leadership in AI, is semiconductors. If you look at the leading edge, applications of AI are sort of the hero experiments in AI, they're doubling their demand for compute about every three months.

So, models are getting much, much larger. They're requiring ever larger amounts of compute in order to run those models or train those models. And in order then to lead in AI, you either need to lead in semiconductors or you need to have very close and reliable friends who lead in semiconductors, whose supply chain you're going to be able to be guaranteed to access in ways that are secure. There is a need one to continually advance the frontier of semiconductors. So that's why some of our recommendations focused on investments in new semiconductor research. But there's also a need for the U S to retain its position as one of the leading sellers of semiconductor manufacturing equipment and semiconductor manufacturing design tools.

So, the EDA tools that are used for the design of new chips, it turns out something around 95% of the revenues for those tools is from US companies. So, we again can have a good position in semiconductors, but you're right to point out that Taiwan's position in manufacturing is one that creates a lot of concern.

There is a need then to make sure that domestically we have the ability to produce some of the chips that we might be most reliant on, as well as ensure that some of our other allies, such as Korea and Japan also have the kind of production capacity at the leading edge that they need.

MUSIC

**CRAIG:** I would presume that one of the things that you're talking to allies about is whether or not their battle networks include Huawei hardware.

**JASON:** Yes, ensuring the security of 5G networks as well as other networks is really critical. And regardless of whose network or who has devices on the network, who has routers say on your network, you also need to ensure that you have additional levels of security for encryption.

So even if, for instance, we moved to a 5G network, that includes, say only allied countries that are producing the hardware, you would still want to ensure that you have appropriate levels of encryption in case there are cyber-attacks against that hardware that makes them vulnerable.

**CRAIG:** Yeah, Eric Schmidt a few months ago talked about building trust, his systems out of untrusted components.

I don't quite understand what that means, but I would guess it involves encryption of different sorts. Is that right?

**JASON:** Yeah. Encryption and this sort of notion of zero trust environments in which you make sure that you can use infrastructure that you think in various ways might've been spoiled.

And build systems or plans that are resilient. So that is sort of a general principle that I think US government is exploring through work in the defense innovation board and some of the defense science board studies.

**CRAIG:** In this work with partners and allies, when you talk about partners, are you talking about nation States or are you talking about multinationals who are domiciled outside the United States?

**JASON:** When I say allies and partners, I mean nation states.

**CRAIG:** The US has a long way to go, certainly to get where it wants to be in its AI enabled military capabilities. This is a new field. But do you have a sense of where we are as a group of allies?

Are we 70% there or are we just at the very beginning of knitting this all together?

**JASON:** I think we're closer to the beginning. I think the thing to celebrate is that there's goodwill and positive intent from our allies and partners to collaborate in developing and deploying AI safely in ways that benefit democratic countries.

I think that the challenge has been that we're not all building to the same technology standards. We don't test or evaluate our systems in the same way, and oftentimes that means we're not testing them well enough. One example of that is that our systems right now that use traditional classifiers could be fairly easy to spoof and an actual conflict.

So that's the really significant vulnerability. That's one that's going to take a lot of research and a lot of investment in new methods for testing and evaluation. So, there's a lot of work that needs to be done, and that's on the technology side. Then when it comes to the operational side, we need to figure out what are the ways to deploy AI into systems that are compatible with the rule of law and with our ethical principles.

And what can we do collectively to ensure that those systems are used safely when they're used, say, for intelligence surveillance or reconnaissance, or they're used to defend against cyber-attacks? What do we know about their performance in the real world?

**CRAIG:** Beyond the point of contact to govern these things, is there an anticipation that there will be a series of treaties. I mean, how do you codify all of these things.

**JASON:** We haven't heard from our allies the need for new treaties with our partners about how to govern and manage AI. I think there's sufficient good will that the sort of agreements that we've used, for example, within NATO or the Five Eyes or other alliances is such that it doesn't require new treaties. But the question of whether or not we need new treaties with China or Russia is one that the commission is deliberating on.

On the one hand, we have the highest hopes that China and Russia will show greater responsibility in their use of AI. But there's a lot that worries us, from China's sales of fully autonomous capable weapons systems to its deployment of surveillance and censorship systems that are meant to crush dissent. Then Russia has fielded autonomous weapons systems in Syria without proper testing, which has led to serious concerns about the safety of civilians. And Russia has historically also pursued autonomy and its nuclear command and control systems, which is deeply worrying.

So, with these concerns, it will be important to find areas of agreement to prevent races to the bottom on AI safety or other issues. And this is an area that the commission is deliberating on.

**CRAIG:** It seems that one of the things that is necessary before negotiating treaties like that is to get the allied side organized and raise the capabilities to a level where you're negotiating from a position of strength.

I'm very interested in Huawei and how we get allies to wait for a different solution. I had a conversation yesterday with Qualcomm, and they're adamant that they're not behind Huawei, that they have solutions that are comparable, but I would guess if that were the case, then we wouldn't be worried about Huawei.

**JASON:** I'll speak to something maybe more general, which is that I think that the United States has a lot of strengths going for it. That gives us some just natural advantages. The first, and I think actually the most important, is our ability to attract talent globally. We historically have benefitted so much from high skilled immigration, and if you think about the number of scientists and engineers who came to the United States during World War II to be part of the wartime effort in science and technology, how much we've benefited from that. But how much historically we benefited from that.

If you look at the number of computer scientists and mathematicians in Silicon Valley, more than half of them are foreign born. More than half of the cofounders of $1 billion plus tech companies are foreign born. That's a great natural advantage. A second natural advantage that we have is our higher education system, which is first rate, leads the world.

A third natural advantage we have is our role in semiconductor design and manufacturing equipment. A fourth advantage that we have is our alliances, the fact that we have true friendships. There is though, a weakness that the United States has, which I think is important in a way that I at least had not paid sufficient attention to.

And that is that we have, I think, been pretty naive about the ways in which the system of international standards can be used as a political tool and a military tool. The way that we have approached international standards for technology is that we leave it to industry to come up with its own tech standards and to promulgate them to the international standards bodies like ISO.

That is not how other countries have approached this. And China in particular, has seen international standards as an environment in which to apply political pressure to, say, Belt and Road Initiative members to pushing for particular standards even against their own financial interests in order to meet some national objective.

So, I think we need to be much more diligent in the United States about the ways in which these international institutions are being abused and ensure that the integrity of international standards is supported by a technical truth as opposed to say, the political objectives of some of our competitors globally. That's, that's an area where I think the United States really has been behind. We've neglected. International standards bodies as an arena of geopolitics.

**CRAIG:** And then finally, I know recruitment is not your area, but presumably among my listeners, there are people that are interested and willing to contribute. How do you see, for your line of inquiry in particular, that people can contribute or should contribute if they have the skills?

**JASON:** So, first people who have AI engineering or software engineering or AI research backgrounds, those people are in high demand, obviously, from lots of places in industry and academia, but they're also in high demand for places in government. So, if they have a strong research background, I think looking at places like IARPA and DARPA and NSF and the DOD labs, the Department of Energy, national labs.

Those are all great destinations for talent, and you can use the intergovernmental personnel act if you're in academia or in a nonprofit research organization to come in. You could also join the Defense Digital Service or some of the other services like the Presidential Innovation Fellowship Program in order to come in and do a stint in government and contribute to an important mission without sort of dedicating yourself to a lifetime of government service. You can still come in for a short-term appointment and get a lot of good work done. A second way to contribute, if you're not on the technology side, but instead are on a policy or strategy side, we need people to think about how AI is likely to be used and misused by various competitors, and we need those people in places like OSD policy and OSD net assessment.

And we need them in the state department. We need a whole new generation of technology diplomats to understand how the geopolitics of these technology competitions are going to be playing out and how to work with our allies. And then we need the think tanks of the world, which includes a lot of the DC research organizations in academia or outside of academia.

We need talent there to be thinking about ,one, how to train the next generation of strategists and policymakers and diplomats and intelligence analysts to deal with this. And we also need talent to be coming in to the federally funded research and development centers and the university affiliated research centers that help provide intellectual support to government. So, there are plenty of opportunities and if anybody is looking for a way to contribute here, please, they should reach out to the commission.

MUSIC

**CRAIG:** That's it for this week's podcast. I want to thank Jason for his time. If you want to learn more about the National Security Commission on AI visit their website at NSCAI.gov.

If you want to share your views on AI and national security, reach out to NSCAI at inquiry@NSCAI.gov. The country needs you.

And remember, the singularity may not be near, but AI is about to change your world. So, pay attention.