[DAISY THE GREAT](https://www.facebook.com/daisythegreatband/) [BUILT MY HOUSE ON HOLLOW GROUND](https://youtu.be/z-1sC1lkmKw)

CRAIG: 00:07 Hi, this is Craig Smith with a new podcast about artificial intelligence. Weapons and war are facts of life that most people hope humanity can move beyond at some point in the future, and there is some possibility that the decision-making power of AI will eventually help nation states share resources and solve disputes without armed conflict. But for now, every national government has a responsibility to its citizens to maintain a credible defense, and before AI solves the problem of global governance, it will instead be used to hone military capabilities. Any government that neglects to keep up with this trend will leave itself vulnerable in the global balance of power.

So, as much as we all want AI to be used for peaceful purposes, we have to accept that it has obvious military applications. There is an implicit race underway between the world’s great powers, particularly China, Russia and the United States, to enhance their militaries with AI.

CRAIG: 01:09 To understand this, I talk this week with [Trae Stephens](https://www.linkedin.com/in/trae-stephens-485a811/) and [Brian Schimpf](https://www.linkedin.com/in/bschimpf/) from [Anduril Industries](https://www.anduril.com/), an AI defense contractor. We talked about the current state of AI research and deployment for national security, including how the US stacks up against China. We also talked about the resistance among US engineers to work on defense applications and whether that hobbles the US in the global AI arms race.

Because of the difficulty in getting three busy people to sit down in once place, the recording was made over the phone, which resulted in less than desirable audio quality. Nonetheless, I thought it was an important conversation, a fascinating and informative conversation and so this episode is an hour long. I hope you learn as much as I did.

CRAIG: 02:00 Well, I don't know which one of you guys want to go first, but Trae or Brian, if you want to explain who you are, how you got into this particular field, I'd be very interested.

BRIAN: 02:16 Sure. I can go ahead. I'm Brian Schimpf. I am cofounder and CEO of Aduril Industries. I, for the prior 10 years, was that [Palantir Technologies](https://en.wikipedia.org/wiki/Palantir_Technologies) where I ran product and engineering. Prior to that I worked on self-driving cars, while I was at school at Cornell University, I joined the [Darpa Urban Challenge](https://www.darpa.mil/about-us/timeline/darpa-urban-challenge) and [Grand Challenge](https://en.wikipedia.org/wiki/DARPA_Grand_Challenge) days where it was kind of the first set of self-driving cars that were getting built and a lot of that technology was getting created and I was lucky enough to be part of that pretty early on. Very excited to get back into that, to the national security space, with Anduril Industries where we're doing a lot around how do you apply these modern techniques around computer vision, perception, [sensor fusion](https://en.wikipedia.org/wiki/Sensor_fusion), autonomy, all of these things to modern defense applications.

CRAIG: 02:58 Yeah. Yeah. And Trae?

TRAE: 03:00 Yeah. Hi, I'm Trae Stephens. I'm the cofounder and chairman of Anduril Industries. Prior to starting Anduril, I had been serving as a partner at [Founders Fund](https://en.wikipedia.org/wiki/Founders_Fund), which is a venture capital fund focused on the technology space. Prior to that I was at Palantir as well where Brian and I initially met and then I actually started my career working in the US intelligence community. So, I have a long, a long history in national security.

CRAIG: 03:25 That's right. So, you're more from the national security side. Brian's more from the AI side. Is that a fair way to say it?

TRAE: 03:33 Sounds roughly accurate to me.

CRAIG: 03:35 Okay. What I'm interested in, and I'm really glad that you guys could make the time because there's been this debate, this ongoing debate, particularly since [Google pulled out a Project Maven](https://nyti.ms/2LTfXFc) about the gap between Silicon Valley and the national security establishment and it concerns a lot of people. It concerns me because I spent a lot of my career in China and I'm very aware and sensitive to the advantages that China has because of its political structure and economic structure. So, I wanted to hear from you guys, your perspective, first of all, on how disabling or disadvantaging that gap is for the US in its competition in national security AI, and how you solve it. So maybe one or the other could start talking about why the gap exists, whether it exists as widely as it appears from outside, whether there's more cooperation than people actually see and that sort of thing.

BRIAN: 04:36 Sure. I'm happy to take the first stab at it. So, we believe that the best people working on AI are, as everyone kind of agrees, not working in the defense space today, right. You know, the best people working on computer vision algorithms tend to be at the Facebooks and the Googles and Amazons where, you know, they're working on commercially relevant applications, things that aren't necessarily the most impactful for national security. And there's a lot of different reasons for this, but I think one of them is that the commercial space has created a huge amount of opportunity for people who specialize in these things to apply their skills to exciting, interesting problems. It's really been well designed around how do you engage them very, very effectively. But I don't think the solution is going to come in the form of assuming that we're going to have necessarily these dual use technology users, assuming we're going to have the Googles, the Facebooks, you know, solve the problems that are most critical for national security.

BRIAN: 05:27 The problems that have, historically and I think correctly, these have been solved by companies who are focused and dedicated to working on these national security problems. And there are number of people who are very interested in working on those problems. We've had - Anduril was founded to solve these problems - and we've had no issue recruiting. We've been able to scale up very, very quickly, find a lot of people who are interested. So, the way we've done that is to be very transparent about what we are working on. We're working on defense problems. We want to apply these technologies to those problems and we want to do it in a thoughtful way. That message has resonated very, very well. And I think what people have gotten wrong is that somehow, kind of Google with the problems that it needs to solve, which are very relevant for what Google's mission is, you know, you can kind of magically transport those to the national security space. And I don't believe that to be true. I think you have to have groups whose mission is focused on solving these national security issues, but doing it in a way that attracts retains and engages the best talent in the space. And I believe that looks very different than sort of hoping that Silicon Valley will come to the rescue to solve these problems.

CRAIG: 06:31 Oh, that's interesting. That's a fresh perspective that I haven't heard. So, it doesn't concern you - this resistance on the part of the major tech firms, because of the resistance on the part of their employees, to engage with the national security establishment.

BRIAN: 06:48 Trae, I don't know if you want to take this on…

TRAE: 06:50 I, yeah, I think that, you know, it's often overplayed as if there's some majority of people inside of Google and Microsoft and Salesforce or wherever that have these problems. And I don't actually think that's the case. I think that it is a really vocal minority of people. But even so if you are an engineer who accepted a job at Google to work on writing code to optimize ads and then you later find out that that code is being used for other purposes, whether that other purposes are national security or otherwise, it would make sense that you might have qualms with how that's being done. And so, I think going back to Brian's point, I think it's less about being super concerned about whether or not Google is going to participate. And it's more about creating opportunities for companies that are uniquely designed and modeled specifically to serve the national security mission and getting some of those people that are excited about doing this work inside of Google to come and work for the companies where they'll have the ability to do that without having to be, you know, secretive or, you know, not completely transparent about what it is that they're doing with the rest of their organization.

CRAIG: 07:56 Yeah. What about the advantages that China has, or that I perceive China is having, by pursuing this fusion between the military establishment and the industrial artificial-intelligence establishment? Doesn't that give them something of an advantage?

BRIAN: 08:13 I think it absolutely gives them an advantage that they are able to take the best technologies and try to apply them quickly to military problems. And I think in the US, the way we've always done that is working with industry. It has always been through going after these different programs and applying the technology that works there. But there was always sort of an honesty about it in the US. There was always this honesty that this is, you know, we were solving this problem for this defense mission. I think where things have gotten kind of sideways is that lack of transparency around how this technology will be used, why it will be used in what ways will be kind of handled ethically and responsibly. And that's an area where I think if the US [DOD](https://www.defense.gov/) were to push forward and take leadership on this, being very clear around the ethics of AI, how these technologies will be employed and being very honest about their application, both we'll have moral leadership at home where people will be much more interested in engaging in solving these problems and we'll have more leadership abroad where we can lead the way on how you employ these. And I think that will provide both a great advantage to the United States and a great advantage to the world terms of how these technologies are used. I think that will also really drive a lot more engagement with people in the tech community. I think there becomes this disconnect where folks in the DOD talk about things like lethality and you know, have a very sort of aggressive stance on how these technologies will be applied. And it doesn't actually even match with the reality of how they are applied. You know, there's a lot of thoughtfulness, consideration, and legal kind of structure around how, you know, use of force and things like that. But it doesn't come across that way to folks in the valley.

BRIAN: 09:48 And so you get this disconnect where, you know, the DOD wants to talk about just, you know, humanitarian assistance, [disaster relief](https://www.meritalk.com/articles/military-enlisting-ai-to-help-with-disaster-assistance/), almost philanthropic aspects of what it does. But it ends up being fairly dishonest and I think everyone kind of sees through that. So I think by taking a much more straightforward and honest approach of how we'll use these technologies and what participation do we need and selecting for the folks who want to engage on that, I think we'll be able to overcome those limitations in a much more powerful way than simply sort of a - kind of take advantage of the same thing that China has where there's this great industrial base that can actually participate in the mission in a powerful way.

CRAIG: 10:26 Yeah, and you're right, the applications for AI and national security are much, much broader than autonomous weapons systems or semi-autonomous weapon systems, but those nonetheless are what capture the public imagination. Can you give me a sense of what the top AI applications are in defense that the DOD is looking at?

BRIAN: 10:50 So I think a lot, a lot of people focus on, sort of, this doomsday scenario of, kind of, killer autonomous robots running around rampant with no controls or no humans involved. Anyone who has been engaged in the state of AI knows we're not even remotely close to that being technically feasible, nor does anyone even think that's necessarily a good idea. What in reality has a huge impact today is just increasing the quality and integrity of the information that people have for making decisions. So, I think of this mostly in the case of how do we have things like, you know, better intelligence information. If I can get much more information about, you know, where our troop movements or things like that and be able to just present the most relevant pieces to a human. So instead of having banks of humans just staring at a video camera all day, that substantially increases the quality of decision making that the US DOD can do.

BRIAN: 11:46 So most of the problems today that AI is most applicable for are sort of, how do I best take advantage of the huge amounts of information that are available, find the most relevant portions, and present that to humans to make those qualitative decisions that they need to make. It really is about how do I kind of sift through this vast amount of information to make sense of it. And basically, every application that you're going to see in the next five years revolves around that theme. How do I essentially automate the understanding of the world and make it better for humans to do that? There's a number of areas as well where it boils down to, you know, even relatively rudimentary things. You know, how do I have aircraft plan flights? You know, how do I detect kind of maintenance problems in advance? Those are kind of like, you know, lower level things that I think will be impactful. But by and large, the biggest application that has the most interest, the most drive and I think the most near-term applicability but brings real capability to what they're doing in the DOD is this idea of how do I make sense of this huge quantity of information faster. That's going to be the biggest bang for the buck in the near term.

CRAIG: 12:52 Do you have a sense of what the Chinese are working on?

BRIAN: 12:56 I suspect it's that, but I also suspect there's a fair bit of, you know, there's a lot of sort of potentially true, but you know, kind of unclear articles around usage, kind of [autonomous drones and swarm technologies](https://thediplomat.com/2018/02/chinas-swarms-of-smart-drones-have-enormous-military-potential/) and all these sorts of things that may be true. I suspect their applications of AI end up looking very similar to what's working in the US, which is how you're able to target faster. How are you able to understand what's going on quicker? How do you have smarter systems that do this with less humans? And that's really where the advantage is going to come from. How do you have a more impactful force with less human engagement?

TRAE: 13:31 The scarier aspect of what they're doing is that - what Brian and I are talking about here is using AI to carry out the national security mission for the Department of Defense. What China is doing from a kind of a leadership polling position with AI is they're using this for [domestic surveillance](https://nyti.ms/2NAbGaP). And those are vastly different applications of a similar technology. So instead of talking about situational awareness with overhead imagery, they're actually doing like facial recognition with CCTV cameras in urban environments. And the things that you can do with that slightly different application of technology go from like, you know, a reasonably positive world view of the future to something that's dark and much more dystopian than I think any Americans when I think about.

CRAIG: 14:18 Yeah, no, absolutely. I had a conversation with [Pedro Domingos](https://en.wikipedia.org/wiki/Pedro_Domingos), you know, the author of [The Master Algorithm](https://www.amazon.com/Master-Algorithm-Ultimate-Learning-Machine/dp/1501299387) about this and as he was saying, that kind of application strengthens authoritarianism - and the theory has long been that the [Communist Party](https://en.wikipedia.org/wiki/Communist_Party_of_China) will continue in power until there's a large economic shock when there's a public reaction against them. But if they have in place this intense surveillance, not only in China but elsewhere in the world, that kind of cements them in place. So, [he was saying](https://www.eye-on.ai/podcast-010) that, you know, democracy may be the right way, but authoritarianism may win in the end because once it has its hands on these technologies, it's very, very difficult to dislodge.

TRAE: 15:03 Yeah, it's certainly stickier than our approach. And this is not only in the defense world, but it's also in things like medicine. You know, if you need training sets to develop models to detect tumors, it turns out that a state-owned healthcare system where the government has unfettered access to all of the medical imaging, it's much easier for them to build those repositories of training data. So, there are definitely kind of advantages built into their system. But I think this is why it's so important that we spend time working on this here in, in the US and in the liberal democratic world so that we can take a leadership position in the technologies that we're developing ahead of them. You know, the tricky thing about being a leader is that you can only really lead if people are following you. And China has effectively, through [SenseTime](https://en.wikipedia.org/wiki/SenseTime), been able to export their surveillance regime to other countries, Egypt to Venezuela, Iran. And that's something that is only happening because you know, the US hasn't taken a leadership position in defining what those standards and norms should be for how those technologies are applied and used.

CRAIG: 16:09 Yeah, that's, that's very interesting. On the question of standards and conventions between nations and particularly between China and the West, are you hopeful that we'll be able to work out meaningful conventions that both sides would adhere to? Because one of the difficulties with AI is, it's invisible. You don't know when it's being used and so I personally am not very optimistic. I would guess that China will go as far as it can in development before it sits down to a table. And then, even beyond that, it's a matter of trust, and trust between nations of ideological differences such as between the US and China is not a natural thing.

BRIAN: 16:53 I think that the US is not negotiating from a position of strength right now. If you were to imagine the US trying to negotiate, you know, kind of nuclear test ban treaties without having any nuclear weapons, it wouldn't really work. No one would really listen. And so, I think the part of this has been - the US is not leading the way in what is a thoughtful, controlled and human-rights-centered view of how you employ these technologies. We're not actually taking a leadership role. There're no technologies that are available today to do this in a thoughtful way and apply these technologies in a limited fashion. Instead we've spent more time studying the problem that we've done to actually solve the problem and engage in how we use these things responsibly. And I think as a result, we don't have kind of a position to argue from, nor are we even wrestling with the trades and kind of norms that would be required to adopt these things.

BRIAN: 17:44 So I think you had a great point, which is you don't know when these things are being used, it's not aware, but the US could solve that. The US could apply - create standards around how they kind of communicate where this is used, how it used, how are they doing this in a [bias-free](https://www.research.ibm.com/5-in-5/ai-and-bias/) way. You know, there's a lot of these pieces to it that I think if we actually made progress on the solutions to these problems, we would have a much more - strong position to start kind of outlining the frameworks in a very practical way. But instead we're mostly just discussing this in a vacuum without anything to sort of argue against.

CRAIG: 18:15 Yeah. Although just as you said, we're negotiating or discussing from a position of weakness because we don't have those systems in place. I would argue that - you had said earlier that the most lethal weapons systems that people imagine are not immediately attainable for technological reasons - I would guess that that's what China's focusing on.

BRIAN: 18:38 Yeah, I think that's a fair assumption. We've already seen, you know, [things from the Russians](https://news.vice.com/en_us/article/vbzq8y/russian-weapons-maker-kalashnikov-developing-killer-ai-robots) for example, of autonomous weapons systems that'll fire on things that - with relatively little discrimination. The US is unwilling to go after those things, I think very correctly. You know, that is not a technology that the US wants, should have. And I think by kind of approaching these things in a thoughtful way, I think we'll be able to have create international pressure to stay away from those sorts of technologies, create those as something that's considered very harmful and not - almost like a new Geneva Convention. But a lot of it starts from understanding where those lines really need to be and having the thoughtful applications of these things rather than just sort of pausing before we even engage in how you build these technologies.

CRAIG: 19:25 Yeah. And when you said earlier, and correct me if I misunderstood you, that the applications that DOD is looking at are more in command and control areas than in actual autonomous weapons systems. Why would they not be in autonomous weapon systems? Because the technology it would appear to me is there, it's even commercially available. It's just a matter of putting them together into products.

BRIAN: 19:55 I think the correctly has a very high bar on how accurate and reliable do your systems have to be before they will engage in any sort of, you know, things that put humans at risk. This is a great thing that's kind of misunderstood about the DOD, is they do not rush to kind of field new things without understanding the safety and kind of implications of everything they are fielding. And so when you look at something like self-driving cars, that's an application that not only has to be better than humans, it has to be perfect, right? Like society won't accept that until it's basically perfect. And that will, I would argue that it's not even - everyone talks about how this is going to be a year or two out and it seems completely nonsense at this point. You know, given that it's been a year or two out for the last five years.

BRIAN: 20:35 So I think it's pretty safe to assume it's another five to 10 years out. And that's the sort of level you have to get to before you'd be willing to consider how these systems are employed. You have to have very, very high confidence that they will behave nearly perfectly against the parameters and rules and norms that have been set up. And so that technology I would say does not exist yet. Right. That there's a level of sophistication of these systems that is not there. Most of it is around the ideas of kind of processing that information to get substantially better than humans essentially, but not yet at the point where it is as trustworthy and safe as folks would expect out of a system like this. And I think the US will not overly rushed to deploy things that put people in harm's way until that level is met. I think that is correct, but I think there are many applications today which can provide significant benefit in terms of you know, more precision and more understanding of the activities we are engaged in that are very, very high impact rather than just kind of rushing to this problem of autonomous weapons.

TRAE: 21:36 I think it's also worth mentioning that there are autonomous weapons that are in use and have been deployed that are not related to human targets. Things like, you know, [counter missile](https://www.meritalk.com/articles/ready-fire-aim-navy-ai-missile-guidance/) and counter rocket and things like that. These are places where the technology could very easily be applied in a way that would have less, uh, you know, ethical issues surrounding it that, you know, has already been happening in places like Israel with [Iron Dome](https://en.wikipedia.org/wiki/Iron_Dome) and [David's Sling](https://en.wikipedia.org/wiki/David%27s_Sling) and things like that.

CRAIG: 22:05 Yeah. Knowing China and having watched China, they take a much more [techno-utilitarian approach](https://www.kas.de/documents/288143/4843367/panorama_digital_asia_v5a_Lewis.pdf/fddf1a04-3547-d8a1-0782-d7f249dda990) and on the subject of autonomous vehicles, for example, they're already running [big pilot programs](https://www.scmp.com/magazines/post-magazine/long-reads/article/2142449/chinas-self-driving-vehicles-track-take-global) and I would expect to see real autonomous vehicles in China within a short period of time. Partly because it's more of a top down system, it's less litigious from the public's point of view. The public really doesn't have a lot of the rights that Americans have. And by the same logic, I would think that they would be willing to pursue weapon systems that are not perfect simply to have them as a bargaining chip or to have them in their arsenal. Am I too pessimistic or, or how do you guys feel about that?

BRIAN: 22:56 I think that's right. I mean I think the willingness to deploy things that are, you know, either you know, unsafe for perhaps a little more mature is, is definitely higher. That being said, I think the, you know US approach on the whole is one that I would subscribe to, which is being more cautious when you get to these kinds of more at-risk things and you know, if you look at the last 20 to 30 years of defense technology, it has been how do we increase precision, how do we decrease collateral damage? How do we ensure that these things are applied in a more kind of narrow way? That I think is a direction that we should continue going on. I think it's right. I think part of this is kind of figuring out where we can smartly start to move in the direction of, you know, lower cost systems, smarter systems, being able to take some of those advantages of pushing out some of these earlier technologies well before you get to the stage of kind of weapons systems.

BRIAN: 23:49 I think there's a lot we can learn and refine that would have very big impacts today in terms of how we conduct warfare. That would be mostly around this ability to get better intelligence targeting and awareness of what's going on in the battlefield and that will be the highest impact today. Right now, that is one of the key problems that the US faces is how do we have the best kind of targeting intelligence information? Well before we get to the point of needing to do a strike, that sort of strike capability is quite refined in the US already. I don't think that is where, you know, today the biggest impact is. Really it boils down to this problem of how do we get the best intelligence possible and I think the US will have kind of the moral leadership on that and if we solve that problem very, very effectively, I think we'll actually have one of the best kinds of military advantages possible by going after those problems.

CRAIG: 24:35 Yeah. Are you concerned at all that AI levels the playing field very quickly? I mean a lot of these things are still in the research phase, but once they're deployed they can be deployed at scale pretty inexpensively - that suddenly this huge advantage that the US maintains in defense will largely evaporate.

BRIAN: 24:59 If you look at the [national defense strategy](https://fas.org/sgp/crs/natsec/IN10855.pdf) that was published just a couple of years ago, there's a recognition that the US approach of going after exquisite systems - so you know the highest capabilities, the longest range, essentially at any cost - while that may have been working well for the last 20 years that, you're exactly right, that AI levels this playing field where you can now have relatively low cost systems with no real human lives at risk, be able to operate at a much lower cost with a much higher level of capability. You kind of flip things on their head where instead of needing, you know, one camera that can see hundreds of miles or some [sensor that can see hundreds of miles](https://www.c4isrnet.com/c2-comms/2019/04/02/the-army-targets-systems-to-see-1000-miles/), you can now have thousands of these things for the same amount of overhead and that really changes how you think about your force, how you think about how these capabilities are deployed and what systems do you need to go after.

BRIAN: 25:46 And the US is just starting to wrestle with this shift. So, there's a recognition that this kind of new technology really changes what the limits of that historically, which is manpower, which is how do we kind of take and consume all this information? How do we actually control it and operate it. AI really shifts that on its head where it becomes incredibly cheap to have high quantities of these systems. People haven't yet figured out how to deploy that effectively, haven't really figured out how to deploy that in a military scenario. But that is where inevitably these things go and it absolutely changes the advantage away from these, sort of, very expensive, very high-end systems that are very hard to compete on, to, you just need smart systems and you just need a lot of them and that is a huge shift that the US will have to contend with.

TRAE: 26:26 More broadly, I also think that this shift is, you know, related to hardware versus software focus. So, you know, during the Cold War it was incredibly difficult for other powers to compete with the United States and the Soviet Union because at the end of the day you needed a manufacturing industrial base. You needed vast access to natural resources to actually manufacture these things. You needed to have human capital. You had to have the talent. There was like all of these different pieces that fit into the puzzle. Whereas, you know, what we're seeing with the increasing importance of software is that a ragtag bunch of teenagers, effectively, in the basement of a government building in, you know, [Pyongyang can actually disrupt the international economy](https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html) or you know, political system. And that's something that's just fundamentally different from a hardware defined past that it has really just been super recent.

CRAIG: 27:21 Yeah, yeah. Oh, that's right. And that's what makes it harrowing, frankly. I guess going back to the gap with Silicon Valley engineers, to whatever extent it exists, there doesn't seem to be a recognition that this is, you know, really a national security issue. It's not big bad warriors wanting to deploy killer robots or something. It's a matter of protecting the homeland as much as anything else. So, I mean you guys are kind of unique - or maybe you're not - in being an AI firm focused on defense, or a defense contractor that is using AI - or is that now a pretty large sector?

TRAE: 28:04 I wish it was large. I have spent a lot of time looking for companies working in this space and it's not large. There are not many companies that are attracting talent and raising capital that are focused on defense.

CRAIG: 28:17 Yeah, yeah. That's the impression I get. Again, isn't that a disadvantage for the US? I mean you have China working with [Baidu, and Tencent and Alibaba](https://www.scmp.com/tech/china-tech/article/2120913/china-recruits-baidu-alibaba-and-tencent-ai-national-team), I mean they're the Amazon and, and Googles of their world. It's seamless. I mean there's no resistance or hesitation in [that industrial-military fusion](https://www.realcleardefense.com/articles/2018/05/10/xi_doubles_down_on_civil-military_fusion_113431.html). So, if there isn't this private sector industry that's focused on defense, on adopting AI technologies for defense purposes, again, doesn't that leave us vulnerable to what's going on in China?

TRAE: 28:52 Sure. I think there are, as we said before, there are definitely advantages to the Chinese system and you know, those advantages are not specific just to authoritarian regimes that happened to be our adversaries. I mean you have some of the same types of behaviors in places like Israel where they have mandatory conscription and you know, everyone in their early twenties is coming out of military service into the private sector and tends to be much more interested in these things and at least aware of the problem space. So, I think that that is challenging. However, the caveat to this that I would offer is that there are a lot of people in the tech community that would be willing and would be interested in, would be passionate about working in national security. And the problem is that there's really not a great path to becoming a successful business doing work in this space.

TRAE: 29:44 In fact, if you look back over the last 30 years since the end of the Cold War, the only two venture backed companies that do the majority of their business with the government that have become worth more than a billion dollars are [Palantir](https://www.palantir.com/) and [SpaceX](https://www.spacex.com/). That's it. There are only two examples and 30 years of this working at like a venture capital scale. And so, I think part of this problem is how do we get the Defense Department, how do we get the culture inside the building at the Pentagon to recognize that the skills that are required to properly execute this mission do not live inside of the [defense primes](https://www.dhs.gov/prime-contractors). They don't live inside of Lockheed, they don't live inside of Boeing. They don't live inside of Raytheon and if they want to actually improve our capabilities, we have incredible access to human capital, but we don't tend to make very good source selection decisions when it comes to writing contracts to build out these capabilities.

CRAIG: 30:37 Yeah.

MUSIC: 30:38

CRAIG: 30:43 hile I'm concerned about the Chinese-US competition, I'm also concerned about this [growing suspicion](https://www.csmonitor.com/World/Asia-Pacific/2019/0503/In-race-to-dominate-AI-US-researchers-debate-collaboration-with-China) among the US national security establishment toward Chinese researchers or Chinese companies working in collaboration with US researchers and US companies. To me that is kind of a dangerous road if we go down it, but are you concerned at all that this anxiety about China's research or advantage and the growing competition between the two in the national security space will bleed into the research space and people will start trying to [pull apart collaboration between US research institutions and Chinese research institutions](https://www.nytimes.com/2018/04/30/us/politics/trump-china-researchers-espionage.html) - or do you think that should happen?

BRIAN: 31:34 The traditional approach to how we've protected defense information has been lock it down, prevent it from getting exported, you know, try to control the hardware. And this has worked in a hardware centric world where you know you kind of built these discrete weapon systems. Things were built specifically for weapons systems and there's a very clear line. So, you had a lot of things like you know, [ITAR controls](https://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations), export restrictions, all these things that were designed around this idea that you can the defense information inside, controlled and locked down. I think the thing with AI is that this will not work. You look at where most of the progress has been. It's in the commercial space. It's been through these research labs, it's been through thousands and thousands of researchers each building on each other's ideas to move through things very quickly. Just the sheer quantity of information in progress that's been made in that space, that is what you have to tap into.

BRIAN: 32:20 So the whole problem becomes not one of how do you control, restrict and lock down that information. The US Defense Department is not going to be the foremost AI researcher that will not happen. Instead, what they can become is the best at applying this research, the best at integrating at how they operate. The best at finding applications and developing and building those capabilities very, very quickly. And that's where the advantage can come from. And so, I think the foolish approach is to take some of the Cold War strategy of control, lockdown, restrict the information. That won't work in this space. These things are not purpose built for military use. These things are very general-purpose technologies and approaches that can be applied very thoughtfully to military applications. And that's what the US has to be dominant on. So, I think this approach of how do we kind of isolate the kind of Chinese researchers out, you know, even if you could pull it off effectively, I'm not sure it would matter. I think the information will still get out. And I think instead the US needs to focus on fostering that research environment, bringing all the talent to the US that can possibly get here. And then figuring out the best ways to support companies and new approaches. How do we integrate this technology into the way they operate? That is going to be what the winning strategy is.

CRAIG: 33:34 Yeah, yeah, I agree. Can you talk a little bit about Anduril and its foundation and the research that you're doing and the applications that you're building?

BRIAN: 33:50 Trae, you want to kick it off a little bit with how we came to be?

TRAE: 33:54 Yeah, so when I first joined Founders Fund about five and a half years ago now, I set out to try to find the next Palantir or SpaceX. So, what was that next big national security, government focused business and ended up spending the first two years of my time just kind of running into dead ends. I didn't really find anything that I got excited about, had developed kind of this hypothesis that we were starting to fall behind in autonomous systems and artificial intelligence and a lot of the categories of things that [Ash Carter](https://dod.defense.gov/About/Biographies/Biography-View/Article/602689/ashton-b-carter/) had defined in his [Third Offset](http://www.dodlive.mil/2016/03/30/3rd-offset-strategy-101-what-it-is-what-the-tech-focuses-are/) strategy. And it didn't seem like the tech community was responding to kind of the call for help that was coming from the Pentagon. And so, I started talking to Brian and [Palmer Luckey](https://en.wikipedia.org/wiki/Palmer_Luckey) who is the founder and inventor of [Oculus](https://www.oculus.com/?locale=en_US), that is the founder of Anduril as well, as well as some people from our network, [Matt Grim](https://www.linkedin.com/in/mttgrmm/), [Joe Chen](https://www.linkedin.com/in/chenhaus/) and others.

TRAE: 34:51 And it kind of came up with this idea that if somebody was going to do, they said you should probably just be us. And that the combination of software and hardware together to solve some of these critical third offset style problems really had to happen inside of a new defense prime. So rather than just being like a software widget company that emerges from, you know, Palo Alto, it needed to be something that had a little bit more meat to it and was multiproduct and had a, had a kind of a bigger vision for what they wanted to be. And so that's kinda how it all came together. But then Brian, you can dive in on some of the more specifics.

BRIAN: 35:30 Yeah. So, we wanted to look for a problem that we thought we could solve quickly with modern technology approaches. So, it was the first problem we came, we came up with was, well, we think we could solve kind of the [perimeter security](https://www.wired.com/story/palmer-luckey-anduril-border-wall/) problem very, very effectively. So, we talked to a number of folks in DOD and Customs and Border Protection and this idea basically how could you have awareness of what's going on without needing to have increases in manpower and then provide the best information possible. That had a ton of legs, a ton of interest. It was something we were able to build in about six months, have a working system up and they'd be in production in about 12 months total. Very, very fast timelines for the government space. And since that, we've expanded into a number of different areas, kind of applying the same core software and hardware approach of how do we find the best applications for these smart systems, how do we provide the humans with the best intelligence possible - applying this to counter drone systems, applying this to small group intelligence, UAVs - really trying to find a lot of applications where we can apply these methods of you know, AI autonomy, sensor processing, perception to these problems and have a big impact quickly.

CRAIG: 36:39 Is DOD or Darpa or anyone coming to you with problems to solve or these sort of the at this point, not to disparage them at all, but low hanging fruit that you see that you can immediately roll out?

BRIAN: 36:55 I think the answer is yes, they are coming to us with problems. I think [counter UAS](https://breakingdefense.com/tag/counter-uas/) is a great scenario here. I mean, I wouldn't, you know, I think there's kind of been a better job of communicating with industry about what are the key issues that they're facing today and counter UAS is one that consistently comes up. And it's the sort of thing where we can very, very quickly prototype, build and demonstrate new technologies and how they could change the traditional approaches to these problems. So, there's a lot of scenarios like that where it's, hey, here's an urgent need that we have and here's how we can quickly go after it. Solving those problems is an area where I think we will have the biggest impacts in the shortest period of time. Areas where there's real issues today that they have a real threat with when technology can make a significant difference in saving lives, providing defense, actually having real awareness

CRAIG: 37:38 Yeah. How much weapons development or AI powered weapons development is being undertaken within the Defense Department or is most of it being contracted out?

BRIAN: 37:50 I wouldn't say there's, you know, a significant amount of kind of weapons development per se. I mean, I think most of this is focused on understanding the limits and where those kind of big impact capabilities are. So, I think most of it is focused on two aspects. You know, how do we kind of have better intelligence information? That's been probably the single biggest thrust that's been successful in the DOD with, how do they kind of take modern AI approaches, apply them to the vast quantities of intelligence data that's coming in and try to provide the most usable information possible. That's the single biggest thrust. The second is really how do they have, you know, automate some of the more routine things around making an autopilot system more sophisticated, kind of automating some of the planning of flights and you know, things like that. That's been where a lot of the focus has been to date.

BRIAN: 38:37 I think there's still once - that is the right starting point, right. You know, having a firm foundation of those systems is absolutely key. If you can't actually perceive the world, if you can't actually understand what's going on, if you can't actually safely operate these robotic systems. Talking about weapons seems like, you know, you probably have to solve those two problems first before we can have a real conversation around doing anything that's high risk. So those are sort of the foundational problems that I think you have to start with. And those are the areas where we we're really focused as well is how do you solve these issues of perception? How do you solve these issues of command and control? That is absolutely the foundational piece. Any system that you're going to deploy has to solve those to be truly autonomous and to make good decisions. And so that's where you have to start. And that's where the DOD has really put a lot of the efforts to date.

CRAIG: 39:21 Yeah. And in terms of understanding what's going on, the DOD published its [AI Strategy](https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF), although I think most of it was classified, but within that they established the [Joint Artificial Intelligence Center](https://dodcio.defense.gov/About-DoD-CIO/Organization/JAIC/). Is that the umbrella under which all of this is taking place and to which you speak or are there other entities? Can you talk a little bit about that? Because again, I mean [China published its national AI Strategy](https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/) two or three years ago and there isn't sort of one document that people can point to right now that explains US strategy and doctrine.

TRAE: 40:02 The slightly cynical version of an answer to this question is that, you know, we've probably spent more as a government on sending liberal arts majors to conferences to talk about AI and to write reports on AI than we have on actually doing anything meaningful with AI. You know, that's kind of part of the problem, not the solution. You know, if you look at the types of things that come out of the research organizations like Darpa and things like that, these are not commercial opportunities that I would generally recommend that companies should engage with because there's no, there's not really a path to production usage of whatever is built. They're just research projects for the sake of being a research project. And I think that the unique cut that the JAIC and [Project Maven](https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf) and things like that have is that their goal is to field capabilities to the war fighter. And that's something that is far more interesting from a commercial perspective.

CRAIG: 40:59 Yeah. And you mentioned Project Maven, again, does Project Maven fall under JAIC at this point or are they separate initiatives?

BRIAN: 41:09 The reality of the DOD bureaucracy is that it is extremely complicated. I'm not sure anyone actually falls under anybody. It's a very complex beast to get these things moving when you have an institution that's the size of some countries, right. Instead, I think the reality is there's a lot of folks from research labs through the JAIC, through Maven, through, you know, national security intelligence community things all trying to figure out how can they move the ball forward. Right. I think you're going to have kind of a multipronged approach to this. I think that's right. You know, one of the advantages that the US has here is just the pure scope and scale of the resources that can apply to these problems. I don't think he necessarily want it through one central clearing house. I think you do want to have kind of these multi-pronged approaches and have organizations like the JAIC being able to kind of lead the way show kind of what is possible and figure out how to field things quickly and kind of drive this sort of common thread through the department.

BRIAN: 42:00 But the reality is there's a lot of groups within the DOD looking at these problems, all of them having a different twist, you know, be it one of the services or some other very specific mission about how can they most effectively get capabilities fielded today. That is a very important thrust. I think a lot of them are a little more on the research stage around, kind of more on the lab side of demonstrators and you know, experiments rather than what is a thing that could get fielded in the next 12 months. That's the bias that you really should have and that's where I think a lot of the efforts like the JAIC have really pushed forward on - what are the capabilities we can field in 12 to 18 months. Not things that are a five to 10-year research project.

TRAE: 42:39 One of the important metrics that I think will be worth tracking will be whether or not these innovation organizations within the department are actually able to write contracts into production capabilities. So, if you look at, you know, organizations like the [DIU](https://www.diu.mil/), JAIC, Maven, [AFWERX](https://www.afwerx.af.mil/), [SOFWERX](https://www.sofwerx.org/), [Army Futures Command](https://www.army.mil/futures), I mean the list goes on and on. There's so many examples of these innovation orgs, but their strategy seems to be something like this: So, let's say between all of them, there's like a hypothetical, hundred million dollar budget. What they do is they write 400 and $250,000 checks and then they're surprised when nothing kind of emerges from that into a production capability. This is literally the opposite of how the rest of the world works. Like capital tends to concentrate into winners. And so, I think if they want to see better results, the right approach is probably something more like taking that hypothetical hundred-million-dollar budget and writing four $25 million checks into companies that they think actually have the ability to scale into something in production. And you know, doing that will attract private capital, will make it much easier for those companies to recruit and retain talent and it will allow them to scale something into the hands of the war fighter rather than just being like kind of a pilot research boondoggle.

CRAIG: 44:00 Yeah. Along that train of thought, there is not, uh, or, or maybe I'm wrong and I just haven't identified it as such. There is not a national AI strategy for the United States in the way that there is a national AI strategy for China. I mean there's the [Executive Order](https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/), but do you think that executive order stands as the national strategy for the country or do you think there is a need and a usefulness to articulating a national strategy that the world at large can point to and understand?

BRIAN: 44:35 I think if you asked any of the practitioners in the AI space whether there was a national strategy or an executive order, all of them would be scratching their heads. They would have absolutely no idea. And I think the reality is that those approaches, you know, unless it's coming with like mobilizing resources, programs and you know, real kind of emphasis around a set of problems, it's not going to show a material difference. So, I think the real question is how does the US kind of mobilized through defense budget, through, you know, research grants, the types of problems that need to be solved. Like how do we really fund and drive those things? I think a lot of these strategy documents at best can kind of create alignment around those problems but, in reality, tend to be fairly vacuous statements of commitment to work on these things humanely, and with very little practical use in terms of what does that mean and how are we going to actually solve those problems.

BRIAN: 45:29 So, I think the reality is those things don't move the needle. Things that move the needle are real commitments to actually solving these problems, actually moving the ball forward, wrestling with some of these challenges and coming out with clear, practical, thoughtful approaches to how we solve these as well as funding the research and applications to move these capabilities out. That's what's going to move the US ahead. You know, I can't imagine that any sort of document is going to have much of an impact unless it really comes with, you know, a commitment to seeing this grow and develop as real capability.

CRAIG: 46:02 Yeah, that's interesting. I hadn't thought of it that way. And that in China, certainly largely still a centrally planned economy, that kind of document does have an impact because so much of spending is still government spending, so it's a different thing. I'll ask one more question because you mentioned Raytheon and Lockheed and we were saying there is not a very obvious AI powered defense industry at this point. I would think those guys would be investing hand over fist in artificial intelligence because again, AI, it's a pretty easy thing. I mean, it's not a building some complicated piece of aircraft. It's algorithms and computer systems.

BRIAN: 46:46 I think the reality is it's much harder than it looks. I think there's a huge discount placed in the DOD around 'it's just software. How hard could it be? And the reality is look at the massive cost overruns, failures and ineptitude that we've seen on government software programs. They consistently fail for billions of dollars. And if it was that easy, you would think these things would just work. Like it wouldn't be that hard. I think the reality is you have an institution that's been built around 'how do you build, buy, design aircraft and ships and missile systems.’ I mean very large, very expensive, you know, very engineered technologies. No modern software company looks anything like that. Amazon does not look like this. Google does not look like this. They do not have, you know, 10-year technology development cycles. They have one-week, one-month development cycles.

BRIAN: 47:39 There's a very fundamentally different way that you build, design and operate, you know, kind of these software heavy systems. And I think the big mistake is assuming that, you know, because I can make a battleship, that means I can make software. It's just computers. And the reality is it's a wildly different set of skills. So, there's a wildly different approach to managing, designing, building, running these programs. And I think that's the fundamental difference, is the DOD and these defense companies are trying to operate these problems as if they were a battleship. It is not, it is a fundamentally different problem and you have to approach it as such.

CRAIG: 48:20 Is the future then in the defense-industrial establishment going to be more like the startup ecosystem where you have companies like Anduril that are small and nimble and can deploy things quickly? Or do you think that there will be software-focused defense companies that will grow to the size of Raytheon and Lockheed?

BRIAN: 48:42 I think you're going to see a mix of both, right? It's like there's, you know, a number of different systems that the DOD buys. They're all wildly different and I think kind of embracing that, understanding that and then figuring out, you know, how are these different companies going to have different expertise, specialized actually do things. You're going to have a mix of these. So, I think that the mistake that has been made is assuming that it is a one size fits all thing, that they all need to look like the defense primes that kind of came up through the Cold War. I think the future's going to look like more companies like an Anduril where it is, you know, maybe faster, more iterative, more exploratory types of work, rather than just purely the kind of large scale, large systems engineering types of companies that you see. So, I think there's going to be this mix. They're, you know, they're very good at building large aircraft and battleships. I am 100% in favor of companies like that continuing to do that. Where I think you're going to see these new technologies shine, you're also going to see new companies shine where it's just a different approach, a different way of operating and a different type of thing you're building.

BRIAN: 49:42 The other thing that's worth mentioning on this same topic is that, you know, Google, Amazon, Microsoft, these are companies that are in kind of the top, easily the top quartile, if not the absolute top of spending on internal research and development. You know, they're between like 15 and 20 - 25% is spent on IRAD. Whereas the defense primes are on average, like between one and a half and 3% and so they're not really spending money to develop new products internally. They're kind of counting on the government to give them money to do it, you know, under contract.

CRAIG: 50:18 Yeah. Well, and that brings me back to my original question, isn't that then a problem for US national security if Google and Amazon have this huge research advantage, aren't feeding some of that into the national security establishment

TRAE: 50:33 Only if we can't build these software focused defense primes. Because I think if you can, then enough of the technology that's being developed, you know, outside of the doors of the defense industrial base can be used, repurposed, learned from for defense applications. But if we're kind of stuck and we're only giving real contracts to primes, then I would be really concerned. But if we figure out how to allow new entrants to come in and start making a difference then I think that we don't really need Google, Microsoft, Amazon to be there at the table.

CRAIG: 51:07 A lot of the basic research, generally, not only out of these companies, is open source is published on [arxiv](https://arxiv.org/) or various places. Is that an advantage or a disadvantage? Because certainly once it's open source, everybody in the world can use it.

TRAE: 51:23 I go back to the point that, that is the reality of where things are today; that the researchers move so quickly because of that openness and there's no way to change that reality. So instead you have to embrace it and you have to figure out how to use that to your advantage. So, you have this space that is moving incredibly quickly. Your advantage will be how quickly can you take advantage of these new technologies. This isn't a 10 to 15 year cycle. This is a one to six months cycle. And if you can figure that out, then you will win. If you can't, you will absolutely lose.

CRAIG: 51:58 That's it for this week's podcast. I want to thank Trae and Brian for their time. For those of you who want to go into greater depth about the things we talked about today, you can find a transcript of this show in the program notes. If you don't see it there, visit [eye-on.ai](https://www.eye-on.ai/) and you'll find the link for it there. I've inserted links and the transcript to make it easier to follow some of the arcana of defense programs. We've been getting good feedback from listeners and I hope to hear from more of you. I wanted to thank Howard Goldowsky in particular for his valuable advice. Let us know whether you find the podcast interesting or useful and whether you have any suggestions about how we can improve.

The singularity may not be near, but AI is about to change your world. So, best pay attention.