MAJOR GENERAL PRINGLE: We embrace failure, by the way, we often have celebrations on our most brilliant failures, because that is where we learn the limits of technologies. We have to push the edge of what exists to something that does not exist in order to get that to that future technology. So that's a really important task for a research laboratory to think about.

CHRIS: Welcome to *No Turning Back*, a podcast hosted by General Stan McChrystal, and myself, Chris Fussell. Our goal here is simple: to have serious conversations with serious leaders, so we can learn from the best, and navigate these complex times together. Thanks for joining us.

ANNA: How should we think about the future of technology in the military? How will warfighters leverage technoloy, artificial intelligence, and new innovations to best react to the conflicts that await us?

These are the sorts of questions on Major General Heather Pringle's mind, as the Commander of the Air Force Research Laboratory. Major General Pringle serves as the Technology Executive Officer, whose work and research supports the Air Force and Space Force. We were excited to have her on the next episode of the "Future Focused" mini-series of *No Turning Back.*
In this episode, we hear about Major General Pringle's team of 6,000 folks who aim to create an exhaustive portfolio of technology that predicts new fighting environments and challenges for the military. Major General Pringle speaks about the symbiosis between technology and humans, how the basic "to-do" lists for warfighters today are similar to how they've always been (though the technology applied will be different), and the role that ethics plays in her lab. Major General Pringle discusses how her team is pushing to the exciting edge of technology - and we think you'll really enjoy what she has to say.

Thanks to her team for making the time. Now, over to Stan.

STAN: Great. Well, General Pringle, Heather, it's a real honor to have you here and to get to know you. And I appreciated our conversation the other day. I'm going to start with something more from my era than yours, but back in 1983, something happened, which we didn't find out about till much later, which probably saved the world.

Now that may sound like an overstatement, but I think it's probably true and it comes down to a Lieutenant Colonel. And what happened was, there was a Lieutenant Colonel named … or Stanislav Petrov, and he was running an operation center, one of the alerts centers for the Soviet Air Defense system.

And in the middle of one of the shifts, they suddenly got a launch warning, an indication that five Minuteman missiles have been shot from the United States. Now, most of us would think that that would be preposterous, that they would immediately say, no, that's not correct. But this was during the years of Ronald Reagan, a tremendous amount of friction with the Soviet Union, and so it was not out of the realm of the believable, particularly for Soviet Air Defense Forces.

So anyway, Lieutenant Colonel Petrov is in this difficult position. The machine is telling him that five Minuteman Missiles are in route to the Soviet Union. His standing operating procedures are to alert Moscow, who would make the decision on a counterstrike, presumably to launch one, and start nuclear war.

But to the shock of all of the members of his operation center, he doesn't do that. He hesitates. He described it later, like sitting on a griddle and he let time pass because he had doubts. He thought that potentially, this was incorrect. And he calculated for several reasons. One, because he didn't think the United States would launch only five missiles if it was a sudden strike. He also knew that they had a new computer system that was providing early warning and he thought there might be some bugs to it.

Well, after a few minutes, it turned out that he was correct. It was an act of disobedience that was of great risk to him. But in reality, as I said earlier, he might've saved the world.

Now, what we have is a situation of a service member, trying to decide how much to trust the machine. What about that interaction? And now, 40 years in the future, we've got a lot more machines, a lot more interaction on a daily basis, and that's probably going to have a lot to do to define the future of work. And so that's what we want to try to talk to you today about is the future of work. What's it going to be like? And what do you think technology is going to mean for us now going forward? What are future Lieutenant Colonels going to experience?

PRINGLE: Well, first I want to say thank you so much for having me here today. It's an honor to be able to talk on this important topic and represent the Air Force Research Lab that supports both the Air Force and the Space Force. I gotta say that, first and foremost. But technology and the relationship with humans, an important symbiosis that we have to consistently achieve.

And whether it's artificial intelligence, or a missile warning system 40 years ago, there's really no differences. These machines are tools to assist humans. And so, that relationship and the trust and the transparency between them are important, no matter what level the technology achieves.

You know, there's been a lot of uncertainty in the past about whether machines were going to replace humans or take over all our jobs. And there are some interesting statistics about personal computers. That was a fear several, you know, decades ago. And what they've found in the United States for example, is, you know, there were some jobs that went away, typists, primarily about little over 3000 jobs across the United States went away. But so many more were created with this enhanced tool that was provided. And so, 19.2 million jobs were created with personal computers. So, I think it's important to keep in mind that there are a lot of benefits with bringing technology…

And kind of bringing it back to artificial intelligence. This is a tool that we can use in combat operations. As you mentioned with missile warning, we're using it for office administration and even to further our research mission and, to help us better discern what kinds of trends are out there in the data, using autonomy to develop new materials and materials that the human might not even think of.

So, there are a lot of opportunities out there with machines: machine learning, artificial intelligence, but if we get the relationship right with the human, we can avoid the mistakes that you mentioned or potentially save the world like the Lieutenant Colonel did in the Soviet Union.

CHRIS: When… I'd like to dive, dive into an area that I'm assuming you and many of your teams spend a lot of time thinking about the, which is around the, the idea of the new types of threats and vulnerabilities that come with layering in ever-more sophisticated technology into, we can talk about the military and their views more broadly, we can't not go down that road because so many adversaries are, are going to, right, so that will fundamentally change things. So, groups like, like yours continue to advance us technologically, which also opens up all to all new types of threats and vulnerabilities that we have to be prepared for.

So, we'd love to get your thoughts on that generally. Like how do we, how do we make this change and prepare for what I'm assuming is like just an ever-increasing number of new types of threats that are out there? And then more broadly, and we can circle back to this, you know, they're, these seed changes in, in military evolution, right? The invention of gunpowder, the ability to control the airspace above the battlefield, and historically, oftentimes we, we realized that how significant that threat is after mistakes are made, you know, the classic sort of *The Guns of August* approach. And so, we'd love to talk about threats and vulnerabilities, but then also your view on, are we in the middle of another seed change and how do we start to think about getting ready for it?

Or we can look back at this last, you know, World War II, where we are now is one period of conflict and the next multiple generations are going to be massively different, but we can, we can start with, with a threat vulnerability equation.

PRINGLE: Yeah. So, I think what you're asking is are we entering this war of cognition, potentially, and is the character of this type of conflict different than it may have been in the past. And I would say there are a lot of elements that are truly the same. What warfighters have to do is they have to understand the battle space. They have to fuse and integrate that information. Then they make decisions that are risk-based and then they act.

And so, what the technologies of today or tomorrow will bring is an ability to do that faster, to integrate greater volumes of data, to bring more force and lethality in different ways. Networked autonomous collaborative weapons, to leverage artificial intelligence, to fuse and harvest a greater sets of data that are out there.

So, I would say that this… the basic to-do list for the warfighters about the same, but how we apply technology to support those tasks will be unique and different. And what we do in the lab is we try to create as many opportunities for warfighters and technologists to get together and have those scrums because, they don't often speak the same language.

The war fighters are thinking about, you know, what I have to accomplish and getting after the threat and technologists are often thinking about: how can I make this material stronger? How

can I make this aircraft go further? You know, questions like that. And so, bringing them together at the tactical level, as frequently as we can, focused on particular challenges, that's where a lot of magic can happen.

CHRIS: Can I just kind of just quickly follow up if that's okay. What are those moments like? Like I'm sure you've observed a lot of us watching, you know, two different space aliens meet and interact. Where do they find that common ground? What does that look like?

PRINGLE: It's really exciting. You know, they, they get really focused on solving problems and, warfighters want to solve problems, and technologists want to solve problems, and so, it's high energy and the communication can be a challenge because they're thinking of limitations and constraints and opportunities in different ways, but ultimately they're all focused on solving the problem. So, it's, it's a great place to be.

We try to do this in a whole host of opportunities. We try to ground their problem sets that they focus on in near-term problems, for example, or even problems such as today. We've spent some time working on, you know, how do we deal with the challenges of COVID for example, how do we do military operations in a COVID environment? That's a today issue and one that continues to linger on, but we also try to think further out what's a midterm problem set that we need to work on, or a far term, potentially problem set that we need to work on.

And so, every individual has certain skill sets where they might feel more or less comfortable, but, doing those reps is really important.

STAN: Absolutely. You know, humans make mistakes, you know, I'm living proof that you can make a heck of a lot of mistakes in a lifetime. And if you think about it, many of the mistakes you make… when I used to pitch baseball, when I was in high school and every once in a while, I'd make the mistake of hanging a fast ball up about letters high, and some guy would hit one that's probably still in the air, but the reality is when you start to get into a higher risk locations, those mistakes matter.

Chris and I both grew up in special operations units and if a soldier or sailor had an accidental discharge, they were carrying their weapon and they mistakenly shot a live round, we typically released them from the unit. They were sent away from the unit. Now, typically a year later they could apply to potentially come back, but it was, it was a heavy cost and that was with no particular consequences to it, even if the round was harmless.

But you remember some years back, a young officer mistakenly had an accidental discharge with a Patriot missile. And that went off and of course that got a little bit more play and luckily no one was killed in it, but the potential danger, I think of some of the big investment people who can leverage information technology make a bunch of bad investments in a very short amount of time and bring down big investment firms.

So really the question I want to ask is: where do we categorize mistakes in a highly technologically enabled world, where suddenly someone has the ability to do a lot more damage with a mistake. Do we constrain them in their authorities? How do we approach that?

PRINGLE: Okay, I'm going to start with giving you my lab commander perspective. So, we embrace failure, by the way, we often have celebrations on our most brilliant failures, because that is where we learn the limits of technologies. We have to push the edge of what exists to something that does not exist in order to get that to that future technology. So, that's a really important task for a research laboratory to think about.

It's a hard thing to do, but it's something, something that we constantly, we, we push, the exciting edge. Now, when it comes to delivering those technologies, those more complex technologies to the field, part of our job is to burn down the risk that an operator will see. So how do we do that? We run a lot of prototyping, a lot of experiments. We bring operators and warfighters to the lab to get, again, some reps on the equipment and try to mature the technology before it gets to the field. We do, we're starting to explore things like digital twins. How can we better represent a system in the digital world and do some of those tests and extreme measures or applications of extreme environments on them before it ever even gets produced.

So now, let's assume we have done all the brilliant failures in the lab. We've done the burndown of risk, with the warfighters and tests and the technologies now in the field. One of the keys there is to really have the human understand the state of this technology. So let me, better explain that.

Couple decades ago, or when glass cockpits were first introduced to the field, there were a number of tragic accidents where the aircraft would take actions and make controls on the aircraft that the pilot wasn't aware of and couldn't see, and couldn't affect. And so that caused some unfortunate accidents. And what it turned out to be is that the pilot didn't fully understand the actions that the machine had taken.

Now, let's fast forward to an era where artificial intelligence is going to be taking a number of actions that we can't control, that we are trying to…. that, that it will do on its own. And so having that same level of transparency and understanding into the machine's actions, will be, will be important going forward as tech… as the complexity increases, we really need to up the transparency and understand the constraints of the system.

STAN: Let, let me ask a follow-up if I could, because this is a question I'm asked all the time. We talk about keeping a human in the loop. You know, particularly for lethal decisions or other major ones. And yet the speed at which warfare is likely to happen in the future may make that impossible. Think of a hypersonic missile going toward a Navy aircraft carrier or something like that. And the, the problem… one of the challenges of AI is it's a little bit of a black box. It does what it does, and you get information out and you're not quite sure how it did that.

Like when Deep Mind won the game of AlphaGo. Remember, they weren't quite sure how the machine had figured out the strategy to use, but it had. And so I guess the question I'd ask is, are we entering a period where we are going to have to make faith-based decisions or accept

decisions with a confidence in the machine that is not based upon us being able to really check everything?

PRINGLE: We will have to build trust in those AI systems and an AI algorithm, for example, is only as good as the data that it ingests. So, if it gets a bad set of data, it's going to produce a bad set of results. And so, you will have to build that over time. But in addition to having the human understand what the machine is doing, and as you said, we're not going to be able to understand all aspects of it.

There's a bi-directional transparency that needs to occur as well, where the machine is going to be able to better understand the human state. I want to, I want to give you a quick little example to clarify that. In an effort called Pilot Training Next, which is being run down in San Antonio at Air Education and Training Command, what they're doing is trying to leverage technology to better train the next generation of pilots. And what they can do through monitoring the pilots, the trainees' state, how stressed they are, how comfortable they are with the material, the system is going to react and up the ante in terms of difficulty, if they're having too easy of a time.

So, they're bringing rolling in weather, how are you going to deal with this complexity and this decision? And, so, so that's the machine better understanding the human, just like the human understands the machine. So, the machine will be able to adapt to all the complexity that the human is dealing with and so I think that bi-directional transparency is something that we need to work on.

STAN: Yeah. My granddaughters do that to me every time that they think I've got them figured out, they just upped the ante.

PRINGLE: Yeah, that's right. My kids do that to me, too.

CHRIS: It only gets better. To represent the Navy and this discussion a little bit… I didn't spend that much time on ships, but you hear the… in some discussions, the future of AI human in the loop. That discussion that references to the… closing weapons system, machine guns on, on ships that have been there for decades. And for listeners, that's… it's basically a very powerful machine gun that will tear apart anything that's approaching a Navy vessel, at too fast of an approach speed.

Is that a fair comparison? The, the way that the … designed was designed to work, versus future taking the human out of the loop? Or is there, is there a significant leap between those? Because you hear, they get, get thrown around a bit and I'm not, I'm not sure of the accuracy of that analogy.

PRINGLE: And I'm not sure I'm tracking your analogy completely, but, let me try to answer it this way. Artificial intelligence can help a lot of different systems and help them operate quicker with larger data sets. I just barely touched on, you know, how, how can we use AI to process a large number of resumes and select the best candidate. At the same time, you can apply it to full

motion video, and identify, label, particular objects more readily, quickly, with greater ease and that allows the human to do kind of those last 10 yards of running the, running the field.

But you know, we're also looking at: can we use it for the alpha dog fights that DARPA sponsored just recently? You know, can an AI actually defeat a fighter pilot and basic maneuvers? So, lots of applications across the board. It just depends on how you pull in the data sets to use it. Is that helpful to the question that you asked?

CHRIS: Yeah, I think it is. I mean, I'm, I'm over my skis on that. I just, you hear it gets thrown out as sort of a buzzy comparison. We've been doing this for a long time, but I think, I think there's differences, right. I, I just think like the, see what system is, I don't know why, but to me it seems fundamentally different and more rudimentary than what you're describing the potential for AI.

But that leads into another topic that we're going to dive into, which is what are the, in your view as a leader or the, the group that you lead, the view on the sort of red lines, what are the parent Pandora's boxes in all of this that we don't want to open? I'll give you an example. I teach a course on the future of special operations, and one of the discussions you have there is like as miniaturization and AI and all these things come together, inevitably we're going to have, you know, small, miniature drones attached to operators in the field, at some point. There's also this red line argument against, in some groups against, sort of facial or DNA recognition. Cause those weapons could get just too deadly, too fast. I can know exactly who I'm looking at and decide. And then I can program… when you see Stan McChrystal, you take the shot.

But if I'm wearing miniature drones and Stan's wearing miniature drones, I want facial recognition because I want his drones to know who I am, right? I don't want to be mistaken for the bad person. So, like, how do you look at… you know, the nuance in those arguments gets really complex and I'm, I'm curious what those conversations look like inside of your world.

PRINGLE: It's a, it's a tough one to answer. And I'll tell you, when you look at history, of course, it's replete with examples of differences and where those decisions have been made right at the tactical all the way up to the strategic level. Where do you draw that line? You know, I, I start with the core values that we have in the Air Force: integrity first, service before self, and excellence in all we do. And we have those for a reason to guide our behavior. You know, we're really focused right now on accelerating change or lose. That's our … mantra. And so, we're trying to go fast, but we're, we're trying to not cut corners or sacrifice our core values in doing so.

I would say that we constantly guard against… constantly guard against, or, or watch the guardrails for ethical decisions, turning into something that might've been a risk-based decision when it should have been truly more aligned with our ethics. We've put in some institutional guardrails as well. We have an ethicist on the staff at the Research Lab, which is a great addition. We have an institutional review board that looks at how do we conduct experiments that may involve human decision-making, humans, human performance. And that's a constant in the research community, academia…. it's a best practice academia as well as AFRL.

There are published standards, as well, in certain areas. So, we could talk about what the Jake has published for their ethical principles for artificial intelligence use. And, even when we talk about, you know, pushing state-of-the-art in space, the DOD has published guidelines for the responsible use of… the responsible actions in space. So, those are, those are important. And ultimately, it comes down to an individual decision, but, for me, sticking to our core values is non-negotiable and, that's where we are, but, we are working to inculcate that throughout the lab from top to bottom.

CHRIRS: Super interesting the comment on the ethicist, being on your team, which makes complete sense. It's great to hear. Can you imagine a future state, actually, Stan, I'd love to hear your thoughts on this. You know, as a senior leader, you had public affairs officer, legal advisor, as this stuff gets way more complex, could you imagine a world where battlefield commander has an ethicist on his or her staff?

STAN: Yeah, I can, in react, you remember Rich Gross on our staff at JSOC. And then I had him in Afghanistan. He was a lawyer, but his nature was such that he was also sort of an ethicist and because he and I were very close, he would often just pull me aside and say, you can do that. It is legal, but you shouldn't do that.

And that was good reminder in many cases. And so, I think, I think having someone who knows they have the responsibility and authority and freedom to do that is a really good addition.

CHRIS: Yeah. Maybe new MOS, for someone out there. It just makes a lot of sense. Cause I think you can imagine these, these types of this…. the decision to give up the decision maybe is the way to frame it, going… happening so fast for senior leadership on a battlefield that they'd want someone that can really frame the, the ethical decisions that are going into it.

PRINGLE: And with the pace of technology changing so quickly and one that we can hardly keep up with. Right. Having those boundaries and understanding it's, it's constantly pushed.

And so, we want to have that sort of external validation of where those boundaries are with new technologies, because these are areas that are unexplored and unimaginable, or haven't been done in the past. That's the nature of the job. And so, it's fun and exciting, but one that takes constant care and attention to do it right.

Plus we're always onboarding new individuals as well, looking for new opportunities. So, we want to get it right. And I think that's, that's what our citizens expect us to do as well. And we want to serve them well.

STAN: Yeah. I kind of like to make a comment on that before last that, the last question and that is, I think you're exactly right, Heather. It is important to understand that there are going to be incredible pressures that pull and push us in technology, particularly senior military leaders. And it is impossible to anticipate every situation you'll find yourself in, in future conflict.

At the same time, if you are not moored to some solid values, if you're not moored to some things that we think are very important to us as a society, as a service, and as individuals, then we are going to be adrift and, and it'll be much easier, I think, to make bad decisions, as opposed to making thoughtful, sometimes difficult choices that, that go forward.

Now I'm going hit you with one that I know is difficult all though people tend to say, well, we'll just innovate. Okay. I say, go over there, stand on that side of the room and innovate for a while or let me know what you got. And of course, we know, we have Chris and I have a mutual friend, Walter Isaacson who has written a lot on innovators, but one of his findings is that innovation works in teams. It actually happens in interactions between people. The single individual off, you know, by themselves, doesn't innovate very often. And yet, you're in a world where innovation is simultaneously necessary, but there are some particular challenges to it.

The differences between military services and civilian contractors in academia, you're trying to intersect all of these different groups together, all of these different PhDs together, in a way that sometimes is classified, is often under high pressure, but has to produce great, great outcomes. And so, how do you do that?

PRINGLE: Well, one of the things that, we like to say here is we have a lot of smart people, but we don't have all the smart people. So, we don't want to keep going to the same wells for innovation. And so, we're constantly looking to expand and broaden our perspectives, challenge our own assumptions, our worldviews, and connect with so many diverse groups and experiences and units and organizations that are out there. This includes academia, industry, even within DOD and even within Air Force Research Lab, we try to create as many opportunities for bouncing these ideas off each other. We work a lot with our allies as well, and we have deployed, if you will, personnel to some of these international locations and try to build bridges so that we can collaborate on the development of research and technology. There are so many areas where we can collaborate and do collaborate to build technology that supports both… the interests of both groups.

The other thing that I like to mention is we don't only look at our current workforce and the workforce that we have. We look at the workforce that we want to get. And so, we back up our innovation and our connections to those folks that we want to bring on in the future. And we even go all the way back to K through 12, STEM education, we have high school internships. We have college internships. We are building new regional hubs so that we can get those interactions at the tactical level. That's really where the magic happens. It’s not at my level, it's the team that makes it all happen. So, we try to plant those people and disperse them out in as many opportunities as we can so that we are constantly refreshing the ideas as they come in and then fuse them and nurture and mature them into technologies for our warfighters.

STAN: Yeah, that's really good to hear we in a recent book, we wrote about Google and Project Maven and the internal rebellion that came when members of Google's larger team felt that Project Maven was something that their corporation shouldn't be involved in and was actually at odds with the “Don't be evil” mantra that was used in Google.

Now, I agree… I disagree with their conclusion that it was evil, but it doesn't matter. There was a group of people in that company that felt it was in violation of their values. So, how does an organization like the Research Lab or more broadly just Department of Defense, how do we make our case to a generation, a percentage of which, does it look doesn't dress like I do doesn't necessarily think like somewhat of my generation, has a different approach to authority and whatnot. How do we make our case that this is a process that they want to be a part of?

PRINGLE: Well, I would say we look for the common interests and the common values. And one thing we share in this nation, no matter what you do and where you are, it's we value freedom. And we value what freedom brings and allows us to do. And so, we want freedom of ideas. We want freedom of collaboration. And so, we are often able to find common ground and science is a great place to nurture it.

Sometimes it's just a misunderstanding or miscommunication. And so, we find that by collaborating or just getting the word out there, we can bridge some of those differences. But oftentimes, it's, you know, that that common denominator is, supporting the cause of freedom that has been, you know, you know, it's, it's undeniable how important that is. And we don't want to lose that with technology harvesting too much of our personal data, restricting our movements, or purchasing opportunities or whatever, transportation opportunities, whatever it is. So, I wouldn't say that's the perfect solution, I guess, but, I think everyone, everyone is common on wanting to support freedom. That wasn't very eloquent. I'm sorry.

STAN: I think it was.

CHRIS: No, I think it's an important message. And one, that's hard to get through the very noisy space these days. So, and I appreciate you taking the time because I think you and your, your team, service, what history may judge is one of the most important things happening in the military right now, which is really thinking through: how does technology in this accelerated state, blend into our approach to national security? And all the way down to the individual members of our armed services.

So, really grateful for you, taking the time to educate all of us on this.

PRINGLE: I appreciate being here and having the conversation. It's… we love being a part of this team and we love what we do for the Air Force and Space Force and for our nation. We think it is a critical juncture, for our nation. And we're very proud to be a part of it. And thanks for what you do, too, and getting the word out.

STAN: Well, I want to add my thanks first to you, Heather, just for your personal time and wisdom you shared with everybody today, it's deeply appreciated.

And then I want to also express my thanks for what the entire team that you lead does. You know that the Japanese Naval code was broken before the second World War started. It was broken at a time when American intelligence was underfunded and the people who worked in small, not

well-ventilated rooms just working month after month, year after year to develop the technology and capabilities was thankless effort by a lot of real professional people.

Now later, when the payoff comes, everybody goes, that's great. But there are so many things that have to be done, like right now, like what you and the team are doing, that may never see the light of day or may become the most famous thing of the next 20 years, who knows.

But the reality is I want to express our thanks to all that you and the team do to help keep us safe.

PRINGLE: Thank you. It's an honor. Every day. Very much is.

STAN: Take care.

CHRIS: So fascinating discussion and, I really appreciated her coming on because that's such a, it's an important, but, relatively unknown part of the military, and the work they're doing there. Have you seen sure, surely you have, how would you describe the improvements you've seen over the, you know, since you graduated West Point in the seventies to where we are now in trying to connect, you know, that sort of group of varied thinkers, into advancing military technology. I guess you've probably seen ups and downs throughout your career.

STAN: I, I have. You know, they, there always was a technical part of the of the military that was developing things and trying to move it forward. The Norden bombsight different, you know, it was matched with techniques that were adopted in doctrine, but it really has sped up so much in the last call it 25 years because the technology has enabled it to do that.

And so, the other thing that happened is, in the earlier periods of my career, much of the technology in the United States was developed in the military for the military.

And so, it worked in the military and then it migrated itself from the military and things like the Apollo program out to civilian society. And that's flipped now. Most technology is developed in the commercial world and then the military finds an application or uses a, a version of it, which means that it goes faster because there's so many different avenues in the civilian world that just picks us up. So now the military is not just got to figure out what they'd like and ask somebody to invent it. They've got to look across the waterfront, see what's being invented, and see what impact that's going to have on future war and be able to either use it, or at least be able to react to it.

CHRIS: Do, how do you think… I mean, I never served at the strategic level inside the Pentagon or anything like that, but I've observed it. It seems to me that, at a certain point, our more traditional approach to research, funding, forecasting, all those things that sort of evolved after World War II, and that, not that I know of, has gone through any really significant changes, that it's just, it's inevitably going to move too slow.

It probably already is by a decade. Right. But at a certain point, it seems like we're going to get a wakeup call and realize there has to be at least part of that has to be fundamentally redesigned

because even on a 12 month cycle, you're already by the end of Q1, you're behind some advancing technology around the world. You can't take 10 years from identifying a need, to having something on the battlefield. It's just, there's, it's impossible to compete with advanced nation state actors, not the last 20 years of counterterrorism, but these other more sophisticated actors moving at that cycle, I think.

STAN: Oh no, you nailed it, Chris. And in fact, I think we're actually at great danger right now. A friend of mine who I do some work with quoted a number to me and I haven't independently checked it, but he says it takes the United States 105 months to buy new software, adopt new software within DOD. Well, if you think 105 months, you know, you keep software in your civilian world for about a month, and then there are updates and changes and things like that.

And so, if we compare that to what the Chinese are doing or what other competitors are doing, we're operating with legacy systems and processes that have to be overhauled significantly. Now, part of that has always been you want to push down the risk of failure of acquiring something that doesn't work, right. There's the security aspect for it. There's the contracting mechanics. There are all kinds of things that contribute to giving us this dangerously sluggish system. And so, I would argue that we need to make a complete overhaul of the acquisition process, particularly for things around information technology, because, the speed at which that's happening on the outside is going to drive what what's actually found in the next war.

CHRIS: was, was some of that derivative of… and I'm asking genuinely here, I know you, you know, far better, the… like Eisenhower's effort to control, put structure around the relationship between industry and the military to avoid one side of that, those pitfalls, but maybe the cost of that has been, is now overly structured. And when you have actors that are playing by those rules, then, then the game has fundamentally changed.

STAN: I think there are a number of well-intentioned thing. One is: people want it to field very good equipment and sort of field very good equipment. You spend a lot of time identifying the requirements that you want. The, you know, the actual specifics. Then you go through a design process that tries to design that as well as you can. And then you go through testing and all these things, and it's all designed to drive down the risk that you feel something that doesn't work right. And that soldiers, sailors, airmen, the Marine die because you field flawed equipment. Well, the problem with not getting equipment fielded fast enough is worse than not having flawed equipment because you've got nothing. And so, then you add in the commercial side, now a defense contractor can contest decisions.

There was a decision some years ago to buy a certain kind of tanker for the Air Force, an air refueling tanker. And it became a huge controversy. It was contested. The, the contract was switched, and the reality was in my view, it was a representation of all the things we created that are flawed in our acquisition system.

And so, it delayed it tremendously, it added great cost. It did a number of things and it produces actions on the part of defense contractors and whatnot that are counterproductive. And nowadays, it's very hard for small firms to sell things to the military because that the system is

overweighted to the big defense primes who develop expertise in that. And again, they they've done a natural evolution or adaptation to that situation.

So, us being able to produce what we need fast enough, in my view, will not happen, absent significant change.

CHRIS: Yeah. I was doing some research on this recently for a course. And, I hadn't caught this in the news, but it's contemporary, and I think very approachable example of this that you could offer your thoughts on why this happens.

It was about the, I think it was just US Army wanted to look at the next generation of pistol for the soldier. And the teams came back and said, okay, it's going to take two years of research and $17 million and General Milley said, you know, give me a credit card with $17 million and I'll just call Cabela's and get everybody a pistol. Like what… how does that… that's a bunch of, bunch of good people trying to do the right thing, but it's also crazy.

I mean, in the history of warfare, how many people have actually shot a pistol, right? It's just a pistol. Can you kind of walk through how we get there?

STAN: Yeah. I, I laugh at that one because I watched that one very closely and you're exactly right. You get all these people at big opinions on what kind of pistol you needed and you're right. Pistols aren't fired very much in combat and almost nobody hits anybody when they do fire it. They're just hard. What, what happens is… that's a, that's a very emotional one because people care about boots and pistols. For some reason, there there's great emotion and those two when you acquire them.

But again, there are great boots sold on Cabela's, great pistols sold. So, what happens is you start this process and you get all these good ideas. And when the good ideas come in, after a while, the pistol gets huge. And it, because people wanted to do 97 different things and on certain things you just need, good enough. You just need something that shoots and generally, you know, works, that sort of thing. And yet, because that process wants to go through this incredible rigor, it sometimes over engineer's things and it creates capabilities you don't need. And of course, you could do much faster if you did otherwise.

I want to bounce into another aspect of this too. It's: should you develop things that don't seem like they are right? And I talk here a little bit on the ethics question. So, for an example, at the beginning of World War II, every nation swore that they wouldn't bomb civilians. That was just outside every nation's stated way of operating. But very quickly in the second World War, every nation was bombing civilians and the United States took it to an art form with the firebombing of Dresden and Tokyo, and then the atomic weapons.

And so, we did by the end of the Second World War things that we would have considered unthinkable, you know, four or five years earlier. So that gets to the question of developing capabilities. Do you develop capabilities that you won't use now, but you might use if the rules

change? And then the question is: if you develop that capability, does that increase the likelihood that you'll use it, because you've now moved the goalpost a little bit. What do you think?

CHRIS: Well, and, and it also connected to that line of thinking is are you doing it so that you don't have to use it like a nuclear arms race? Which was horrifying, but in many ways, simpler than what's happening, we're on the precipice of now, which was, you know, how many big nukes do you have, how they distributed around the world, and what's their payload?

Right. And at a certain point, the whole world is destroyed anyway, but there's a, there's a weird sort of balance you find in there. Now, it's going in so many different directions. That… for example… is there a red line about how small a remote vehicle can get and what its capabilities are? Like hould we have, mosquito sized drones that can fly in your window, look like a mosquito, test your DNA, identify this is Stan McChrystal, and then have the ability to, inject something so that you die two days later. Is that any different than, than, than a firebombing your city to kill you? I mean, where 40,000 people might die as a result?

Now would you say we want to do that, but never use it potentially, but if you, if you have it on the shelf and your adversary has in the shelf, does it deter the likelihood that either one of you use it, because now you can meet the negotiating table and say, look, we both, we've both got this horrible capability. Let's never use it. So it opens up this whole new can of, I mean, it's, it's, it's old, but new again, because we haven't had to think like that since the Cold War.

STAN: Right. And what brings it close to home: would it be helpful to know where every American is 24 hours a day, seven days a week? Well, for some law enforcement, it would be helpful. For some marketing people, it would be helpful. For… there are times when you say what I would like to know that! And then we step back and go, well, we shouldn't know that, but if we can know that through biometrics, isn't there sort of an inexorable pull toward at least having that capability. And so, well, now my wheels are turning.

CHRIS: Well, I do think, you know, General Pringle and her team, represent what I hope there's continues to be more of… not just for…. I think people assume groups like that they're coming up with the next crazy weapons. If you listen to her, they're actually trying to solve for, how, how do we look at this? What are the ethics? What are, you know, how do we interact with our allies around these issues? How do we connect civilian thought leaders with military folks? So I, I, I applaud the work they're doing.

STAN: I do too. And talk about having a lot of talent and putting it in the right direction.

CHRIS: For sure, great discussion. And we appreciate her being here.