**Dr. Eric Schmidt, chair of the Board of Advisors, and Robert Work, member of the Board of Advisors, of the Special Competitive Studies Project**

**AI and National Security Report**
**Ylli Bajraktari, CEO of SCSP**

**Cyber Media Forum**
**Project for Media and National Security**
**George Washington School of Media and Public Affairs**

**12 September 2022**

**Moderator:** Good morning everyone and welcome to this Cyber Media Forum with Eric Schmidt and Robert Work who chair the Special Competitive Studies Project. This is their first public discussion with correspondents on their findings and recommendations. The report was just released today on how to strengthen America's long term competitiveness in a future where AI and other cyber technologies reshape our national security.

Two quick words of thanks, if I might. First to Tara Rigler who handles media for SCSP. She's been a fabulous wingman in arranging this session and some of the logistical complications that will become apparent in a moment. And also a most heartfelt thanks to the Howard Baker Forum and DXC Technology for their continued support of our work in the Cyber Media Forum.

The ground rules, as always this is on the record, but there is no rebroadcast of audio or video. A few questioners have already emailed me to get on the list. I'll ask the first question, I'll go through those. If anybody else wants to get on the list of questions send me a note in direct chat, not group chat, but directly. We'll get through as many as we can in the hour.

Mr. Work is on the line right now. Dr. Schmidt, I've been allowed to tell you, is just exiting Ukraine where he has made a private secret trip. He got to a European country and is airborne now and will be dialing in momentarily. So until he joins us, Bob Work, welcome. Thanks so much for your time, sir.

**Mr. Work:** Thank you, Thom. And welcome to everybody who's here today. Thank you for joining us.

**Moderator:** I'd like to open if I could, the report was just

released at 9:30. We've all been pouring over it like the Rosetta Stone, but Bob, if you could help us a little bit. What are the two or three major takeaways from the report for the national security realm? And as soon as Dr. Schmidt logs in, I'll ask him the same question.

**Mr. Work:** The main battle ground on the global playing field has been defined. Bill Burns said, "Technology is the main arena for competition and rivalry with China", and President Xi Jinping agrees with him. He recently declared, "Technological innovation has become the main battle ground of the global playing field, and competition for tech dominance will grow unprecedentedly fierce."

Now the United States has essentially assumed that we have been the dominant global technological power since the end of World War II. It is kind of a fundamental premise in all of our national security strategies and our national defense strategies. What this report does, and it is a follow-on to the National Security Commission on AI which came to the very same conclusion, is that we are in this competition and we must win it. It is going to be the defining feature of global politics for the rest of our lives and it is going to determine who is the greatest economic power in the 21st century. It's going to determine who is the greatest military power. It is a competition that we simply must win. And up to this point, because of the 20 years we sent in the Middle East, it kind of took our eyes off the ball and as this technological rivalry and competition was really growing in strength, we didn't really respond as we normally have done in the past. So the NSCAI and now the follow-on Special Competitive Studies Project is really to say this is a real technical competition. It is absolutely critical to the future of our country as well as democracies worldwide, and we must win it. This starts to give recommendations on how we organize ourself for the competition and how we win it.

**Moderator:** Thanks so much, Mr. Work.

I understand that Dr. Schmidt has just joined us.

**Dr. Schmidt:** Hello, I hope you can hear me. I'm an airplane, and I apologize for my poor connection.

**Moderator:** You're coming through loud and clear, sir, and it's

great that you're talking to us both at distance and at altitude today.

Mr. Work just gave us the sort of 30,000 foot view of the report and I'd love to ask you as well, what do you think the public, the government should take as the major themes and findings of this report? And also, sir, if you could share any observations. You've just been on the front lines of a 21st century war that's in many ways an information war in Ukraine. What did you see, and what did you learn?

**Dr. Schmidt:** First, I think the report speaks for itself, and my overall message is that the way our political system works is that everybody assumes we passed the Chips Act and we're done. In other words, like we had two years of arguing and China and leadership and so forth, and by this magical political process we have done something amazing.

In practice, of course, this is just the beginning. Our analysis of what China is doing indicates that they're serious. It's very easy to say that China has also internal problems. My assessment of China's internal problems is that they will spend their time doubling down on solutions to their internal problems which include leadership in AI and quantum, software, semiconductors, and in biosecurity, biosafety, and biology because the solution to the problems that China has is more investment in the areas that are competitive with us.

The point here is, it's easy for Americans to say hey, you know, they're Chinese, they've got their own problems and so forth, but I think that ignores their long-term thinking and their long-term commitment, et cetera. I think Bob and Ylli are probably even better at saying that because they have better connectivity.

Just a quick summary for everybody, I was part of a group that went to Ukraine for 36 hours, and in that course I spent a lot of time looking at the way the war is happening. I think everybody is aware that in the last week or so the Ukraine side has made a lot of military progress. I won't review that, but I think it's all well communicated and well articulated in the press.

What I was interested in is what did the tech industry do to help? Ukraine has been a center for an awful lot of cyber

attacks from Russia. They're probably the early warning system, if you will, for what Russia does. They probably have more experience dealing with Russian information, Russian information tactics, and so forth. So the overall summary is something like this.

The first thing they did is they had a law that prevented government from putting government data in the cloud. In one day they had a meeting of the Parliament, they changed that law, and the second day, in the first week of the war, they moved all their data from government servers in Kyiv to the cloud. They should have done that before, but the point is, the war gave everybody a political excuse to do the right thing. They should have been moving to the cloud anyway and they did it very quickly.

The second thing they did is, and Elon Musk is genuinely a hero here, Elon based on just a verbal statement, was willing to authorize a large number of StarLinks into the country. I won't say their names, but other entrepreneurs, other donors, gave Ukraine a great deal of money that ultimately resulted in what I was told was about 20,000 StarLinks in Ukraine itself. This allowed the strategy of shutting down the internet by the opposition to fail.

So at that point they've got all the data in the cloud and they've got StarLinks up.

The next thing that happened was they had an app called DIIA, and this app was one of the Estonian citizenship apps where you had biometric data, you had your passport, your driver's license, your financials online, and they added something very interesting to this app. What they did is they added the ability to report what was going on in the war by citizen journalists, if you will. So if your house was bombed, which is obviously a terrible thing, you could send pictures of your house that was bombed and that would call the emergency services and report it and inventory it and all that and the military would do [inaudible].

The other thing they did is they put in a service using an application that I was not familiar with called Threema, which is a Swiss competitive signal and telegraph. And that path allowed the user anonymously to report opposition sightings.

As an example, if somebody noticed a Russian tank they could take a picture of it and they could forward it in an anonymous way to the government. The military had then an AI system that would look and see, is this a tank of interest? They got thousands of these reports every day, and then they whittled them down to targets using computer intelligence and human intelligence and eventually go after them.

So if you think about it, here's what they had. They had an internet that stayed up. They have their government data protected. And they had a way in which citizen journalists, reporters, citizens who were reporting what's going on, could report and give them essentially intelligence on land.

They also did a number of other things which I won't go into but you can read about, which included various forms of cyberattack protection. There's some evidence that they engaged in active cyberattacks on the Russian side and there are public reports that they have used biometric databases to identify Russian soldiers who are alleged to have engaged in war crimes using facial recognition.

What they said, and it's all public so I'm not violating anything secret, there is a whole focus around getting an army of drones, and they seem to be very good at using drones in their war tactics. The programmers and so forth have been very good at hacking the drones and using them.

The reason I was interested, obviously, with my own military and computer science background, I think that as a general statement most of the military people I've talked with over the years have talked about this in principle, but we see it in action. I can just report that based on my small amount of data that the Ukrainian tech industry really did make a contribution to the fight.

Thank you.

**Moderator:** Thank you, Dr. Schmidt, thank you, Mr. Work.

Our first question from the floor is Garance Burke of the Associated Press.

Perhaps Garance isn't on.

AFP, Sylvie Lantaume.

**Journalist:** Good morning. Thank you.

I have a two-part question about artificial intelligence. I understand that it can be very useful. I wanted to ask, is there a real risk of the human to lose control of artificial intelligence?

**Dr. Schmidt:** We've all seen the movies of the Terminator robot that is male and that is [inaudible] by the female scientist, and I'm always in favor of those movies. But that is neither what AI is building nor what we should be worried about.

The biggest issue with AI is actually going to be something which we don't talk about very much which is its use in biological conflict. It's going to be possible for bad actors to take the large databases of how biology works and use it to generate things which hurt human beings. That's a very near term [inaudible].

The next use of AI is going to be around cyber, cyberattacks, targeting, that sort of thing.

The third one will be in misinformation.

Those I think are the realistic short term impacts.

In order for the question that you asked to become relevant it has to be the case that the computer system can have its own objective function. In other words, it can choose what it wants to work on. If a computer system which is always on, one day decides on its own volition to work on physics or chemistry or poetry or so forth, we do not today have the technology to allow it to choose its own objective function. There are many people who believe that that will occur within a couple of decades, but right now it's not in the mirror. Right now these systems are conceived of by humans, their direction is set by humans, and their ability to manage information is profound. Look at the large language model, it's incredible hat they can do. They were designed and their objectives were chosen by humans.

**Journalist:** Can you elaborate on the use of artificial intelligence in biological conflict?

**Dr. Schmidt:** There is a general concern that the database of viruses can be expanded greatly by using AI techniques which will generate new chemistry which can generate new viruses. I have been named to a commission of the Congress, called the Commission of Emerging Bioterrorism. However the meetings have not begun yet so I shouldn't elaborate until, but I know the concern is real.

**Moderator:** Mr. Work, if I could follow on Sylvie's question. I was at the Reagan Library some years ago when you were Deputy and you were the first to really lay out the details of the third offset strategy which was going to counter China and Russia with. I was wondering youir thoughts on this, sir.

**Mr. Work:** Sylvie's question is a good one and it goes right to one of the key themes about the National Security Commission on AI and the SCSP. That is these technological platforms that everyone is pursuing reflect the values and principles of the governments that develop and deploy them.

So you can see in the United States and the West more broadly, really thinking about the moral, legal and ethical boundaries that we want to establish on AI in all of its applications. We know how China views AI. They view it as a means to suppress their population, to surveil their population, to suppress minorities, to trample on individual freedoms, and those things just will not pass muster in democracies.

So Sylvie's question gets to the point, and to follow on Eric's point, the United States and the Western militaries see AI primarily as a means to help humans make better decisions. They're not being designed to supplant the human decision-maker. They're designed to help the human make better decisions.

And to pull on the string just a little bit more, for example in the US conception our AI systems will be able to create their own courses of action to complete a task assigned to them by a human and then choose among them. But we are staying far away from any system that could choose its own goals and choose among them. What Eric referred to as being able to set its own objectives.

Now this is going to be central to the competition. We don't know how authoritarian countries will view this. Perhaps they will assign more decision-making authority to machines than the

West would be comfortable doing. And this is going to be something that we will just have to see how the competition unfolds. It might be a fruitful area for discussion among all of the competitors and possibly means of AI arms control to make sure we don't get to the most dangerous systems that I think of and those are systems that might be able to unilaterally order a preemptive or a retaliatory strike. That would be extraordinarily destabilizing and I think it would be in the interest of all competitors to stay away from those type of systems.

**Moderator:** Thank you, sir.

The next question from the floor is David Sanger of the New York Times.

**Journalist:** Thank you, Thom, and thank both of you. I've got a question for each of you following up on what you said.

Eric, if you could go a beat or two more about the Ukrainians. When you were saying the tech sector played a significant role, I'd be interested to know what role you thought that was and how effective.

And for Bob, just following up on what you were just saying, it used to be that the Pentagon would tell us, particularly in relation to target selection, that there had to be a human being in the loop. That led to an interesting discussion which you alluded to which is what do you do if your competitors are not putting a human in the loop and they're making those selections so much faster. In other words, does putting a human in the loop so slow the process that you're condemning yourself to not being able to respond in time?

I noted when I was watching an exercise underway last year conducted in the United States for some of the Chiefs, that the phrase had changed to there's got to be a human on the loop, meaning some kind of supervisory sense of it, but not necessarily getting in the way of the timing. I'm wondering if you could sort of talk us through the differential there.

**Dr. Schmidt:** Real quick David, again, I'm an instant expert as an American there for 36 hours, so hopefully this is correct.

The way it works --

**Journalist:** That's called a reporter in my world. [Laughter].

**Dr. Schmidt:** When President Zelensky ran for office he had a technical team, a digital team, and the head of that digital team was a guy named Federov or something like that. I don't have his name right but you can look it up. He went in as the Digital Minister when the President became the government. He set out on this path of building a digital nation, a more modern country, something I would think would be welcome everywhere and certainly can you imagine if we had these capabilities of a digital ID in America where everything was online, we didn't have to reenter our data all the time. Everyone here is familiar with the inefficiency of the American digital system as a citizen. So they tried to fix that.

It seems to me that what happened was you had a young person with a team that was originally running a political campaign, then running a civilian government campaign who then found themselves thrust into this digital military role. It was to some degree by accident. And what was interesting to me was, I'm used to the slowness of government and government systems in the West, and in the people that I spoke with it was boom, boom, boom, boom. So one of the things that I learned was that in a genuine conflict, everything happens very quickly. I think that will be true in the future as well.

**Mr. Work:** David, good question. A human in the loop suggest that if you're in say an engagement sequence, searching for the target, finding the target, classifying the target, designating it as something to attack, and then all the way to end game, a human in the loop suggests that at every step the human has to say you are authorized to go to the next step. There is no requirement in DoD to do that. That would slow things down to a point that you really wouldn't get any advantage of putting autonomy in weapon systems.

A human on the loop is supervising what is happening. If it sees an AI enabled system acting in a way that is inconsistent with its development and its operational testing and what it was designed for, it can stop the machine from continuing.

So in the DoD instruction on autonomy and weapon systems, it refers to human supervised autonomous weapons. That is when you put the autonomous weapon in an automatic mode like the Aegis

Combat Systems. We have 100 missiles screaming in towards you and no human will be able to keep track of everything and to assign priorities to every single missile. The machine is much better at that. So there is an automated mode where you push the button and the machine is deciding which targets it's going to attack. The human in the Combat Information Center monitors what is happening and can stop further automated action if it is clear that the machine is not doing what it should do.

**Journalist:** It sounds like a pilot in the cockpit who's turned on autopilot but it is watching over it.

**Mr. Work:** Exactly.

Again, the way the third offset use this, and I believe that it is still consistent with the DoD is, is the human will always exercise judgment over the use of force. The human will assign tasks on the battlefield to intelligent machines. The intelligent machine will be able to create its own course of action to solve that task and choose among them. The humans just monitors and makes sure that it is still operating in a way consistent with international and humanitarian law, the DoD laws of war, rules of engagement, et cetera. I think that s pretty standard in all Western militaries.

Your point is we're not exactly sure how our authoritarian competitors will view this and whether or not, if they released these strictures on AI enabled autonomous machines, would it give them a decisive battlefield advantage? We have not seen that, we haven't faced it, and it's a hypothetical question so it's impossible for me to forecast how we might respond. My gut sense is we will do everything we can to keep the human on the loop, human assigning battlefield tasks, and working in conjunction with intelligent machines on the battlefield.

**Moderator:** Next question is Newsweek, Shaun Waterman.

Okay, Jonathan Dyer of [Inaudible].

**Journalist:** Thank you so much. Mr. Work, I understand that Project Maven has been held up as perhaps the most successful model of the DoD bringing AI Technologies to the fore, but my understanding is it hasn't been all that widely adopted and it still tends to be held in the sort of algorithmic warfare section of the Pentagon. And despite all the kind of advances

inward and outward, is it being utilized all that much? Can you talk us through how some of those changes might be made going forward?

**Mr. Work:** I'm going to ask the staff of the SCSP if they have any updated information. What has happened, Jonathan, is that the Department of Defense has decided that they are going to transfer the computer vision aspects of Maven, being able to pick out objects in images, and they're going to transfer that to the National Geospatial Agency which is the agency that uses national technical means to create images of the battlefield and then AI will help pick out objects inside the image.

There are other parts of Maven that DoD will retain, and I just haven't been briefed on the exact split. As you know, the CDAO, the Chief Data and Analytics Office, just was set up and they will absorb the non-computer vision aspects of Maven into the CDAO function, and I just haven't heard how Craig Martel, who came from Lyft to take over that organization, has decided how to work that in.

AI is being used for far, far, far more things than just computer vision. It's being used, well, we continue to use the computer vision aspects of AI throughout the department. We have started to experiment with using AI to help with predictive indications and warning, and it has turned out to be extraordinarily good.

In Afghanistan, for example, it would say -- this is the machine. I don't mean to make the machine sound like a human, but the machine says, "Based on all of the data that we see, there's a high probability of an attack on a district center in this province within the next seven to ten days," and it has turned out to be very, very accurate. Now combatant commanders are exploring those ways.

Predictive maintenance is now being used by everyone. AI saying this part is most likely to fail within the next 100 hours and you should consider replacing it.

So there's all sorts of AI activities going on in the Department of Defense right now far beyond just Project Maven. And Ylli, I don't know if you have any updated information on this question.

**Bajraktari:** No, I think you're right. I would just add for

Jonathan that when Project Maven was launched it was rightfully called the Pathfinder Project because the purpose was really to find ways to bring data and algorithm and AI writ large to the building. It was small in scale with a little bit of money just to see how much the building has appetite for AI.

That has grown, as Secretary Work mentioned, over time because then you had JAIC that was established with a bigger portfolio and they started experimenting with predictive maintenance, natural disasters, and all these things. And the latest effort was really to consolidate all these efforts into a single office that reports directly to the Secretary and the Deputy under the CDAO that Mr. Work mentioned that really has a responsibility how to streamline all the AI efforts within the department, and all the initiatives that are happening at the service level, at the COCOM level, and the Office of the Secretary of Defense's level. So that I think just indicates how the AI has grown into importance inside the building.

Now unlike Eric who believes that the government is slow, I think this is still fast considering how slow our government moves. But I think all these efforts really just indicated AI's importance and how it will be central to the future of the warfighting.

**Moderator:** We're at the half hour mark. A reminder, if you want to ask a question you can drop me a note in direct chat or use the raised hand icon on the screen. We'll get to as many as we can.

Next is Heather Mongilio of USNI News.

**Journalist:** Thanks you so much. I was wondering, you mentioned that we need to win this war. I was wondering if you can define in your opinion what winning looks like, and if you can also talk about some of the ethics behind using AI, whether it's in the Army or the Navy or any of our other military forces.

**Dr. Schmidt:** Let me say in general, Bob talked about winning includes winning based on our values as opposed to other values, and I think that's important.

My concern is actually not just conflict, but really winning platform wars. I want to give you two examples.

If you think about Huawei, Huawei got well ahead of the Western competitors and we found ourselves in a situation where we were forced to ban the use of the most advanced communications technology for 5G.

Another example is what is the most popular website or applications in the United States today? The answer is TikTok which is a Chinese owned company run out of Singapore.

You can imagine the issues with having platforms dominated by non-Western firms which we rely on.

Bob, sorry I interrupted you, please go ahead.

**Mr. Work:** There's nobody in my view who talks about what winning looks like more than Ylli Bajraktari, the CEO of the SCSP. He always, in fact every time he speaks he's always talking about mistakes of the competition and what winning looks like. So Ylli, I'd like to ask you to answer the question and then I will chime in after you say something.

**Bajraktari:** So Heather, what we did here as part of SCSP, we looked at what the future or the mid-decade would look like if we move at this pace. And we also looked backwards, and what we call it, what happened to the three battlegrounds -- AI, chips and 5G -- for the last couple of years. And what happened to us as a country that leads in talent, in tech companies, in the market idea when we face a competitor that puts all the resources to get ahead in these three what we call battlegrounds. And the importance to get these three battlegrounds right is really critical, because it says that this is not just about military confrontation. This is about all the benefits that all these three battlegrounds will bring to our economy and our society and ultimately our military can use it too.

But what we argue for is, in 5G we still don't have a good plan how to compete against China. One of our analyses indicates that China already has 70 percent of the African 4G. We all know what they did with Huawei. If it wasn't for a diplomatic effort and export controls in place against Huawei, Huawei would have been the dominant 5G alternative globally today.

On chips, we just saw that happened with the Chips Act, but China for the last couple of years has gone all in in building

there fast, investing hundreds of billions of dollars in that space. And on AI, they clearly indicate publicly they want to be the global AI leader.

So we argue that we've got to get these three battlegrounds right so we're not 5G'd again. This is the bumper sticker of our report. And between now and 2025, we only have one budget cycle. When you think about it, although we live in 2022, we only have one budget cycle to get all these three battlegrounds right. The 2025-2030 timeframe is a really important period for our country and the global geopolitical security. Every plan, every strategy that China has produced calls for their resources and implementation of all these technologies to come to fruition. There's a strategy made in China 2025. We all track with Taiwan, possible contingencies in that timeframe. They want to be the global AI leader by 2030. The global standard-setter by 2035. So if we don't get our act together in these three core battlegrounds, everything that Eric was mentioning in terms of biotech, in terms of next generation computer power, in terms of next generation of inventions, is not going to happen in the countries that are at the forefront of democracy today. Everything will happen in China.

So the stakes of these competitions are beyond the military competition. It's about who's going to enjoy the benefits for all the inventions that will come from this.

Eric mentioned TikTok. We have the Huawei global platform. In our report wed have a global map of the Chinese digital infrastructure. You will see that most of the world is really covered in red because they either are using some kind of Chinese platforms or about to use new Chinese platforms in absence of alternatives.

I'll stop there and I'm happy to answer any questions.

**Mr. Work:** And Heather, one way to think of this question, which is a good one, is to flip it and say what does losing look like? So if we lose this technological competition, China controls the global digital infrastructure. It has a dominant position in tech platforms like 5G; it controls the production of critical tech; and it's harnessing biotech and new energy to transform its own society, economy and military. If that world happens, it's going to be very bleak for democracy. US security is going to be directly threatened, our companies are going to lose

trillions of dollars of future revenues, American workers will suffer, we'll become beholden to China or countries in China's shadow for core technologies like we find ourselves right now in pharmaceuticals, for example.

China's sphere of influence will grow as its technological platforms proliferate throughout the world. They will be able to establish surveillance on a global scale.

That's what losing looks like and it doesn't sound like a very good future to me. So we want the United States to control the global digital infrastructure and have the dominant position in tech platforms. We don't necessarily have to control the production of critical tech, but we want to be able to compete in that area, and we definitely want to be able to harness biotech for the safety and livelihood of our citizens and new energy.

So this is not a competition that anybody on the SCSP wants to lose.

As far as the ethics go, the United States from 2012 on has really said what are the ethical restrictions of AI? We're the only country in the world I think that has a policy on autonomy and weapon systems. We have established AI principle. We have called responsible AI a key aspect of our future. So essentially on the ethical side we are going to keep the human central. AI is going to help the human become a better decision-maker, to become a better pilot, to become a better warrior or a better entrepreneur. So AI will help the human, but in our view the human is central.

The second thing is, everything we do will be consistent with international humanitarian law. We will continue to push principles around the world to make sure that AI is conducive to democratic values everywhere.

I guess the only answer I have for you, Heather, is I know of no other country that is spending the time and effort to really get the ethical, moral, and legal boundaries or guardrails for AI than the United States and our allies.

**Dr. Schmidt:** Can I add to Bob's excellent statement? And he's really the expert here.

When I think of this as a computer scientist, I agree with everything Bob said, and then I come up with all sorts of corner cases. So for example the human supervises something, but what is the limit of what I'm willing to authorize? I say I want to destroy a city as a human, and then the computer destroys it in some horrific way. Well, that's clearly not okay.

So the details here matter a lot. The Defense Department has an AI Ethics Principle which I was part of drafting and was adopted, and that's an example. But I would suggest that this is something which is of a massive scale because it requires coordination with many, many different countries which are all going to disagree.

One of the things that I learned in the AI Commission working with Ylli and Bob was that for example the doctrine around human control of nuclear weapons, which is a core part of the American system, is not the same rules in other countries. This was a surprise to me.

So speaking as your local computer scientist, I think there are going to be all sort of corners and problems where we're going to say this is okay and that is not okay.

I'll give you my favorite, which is a bad example. Let's say that you built a rifle and the rifle could only kill people that were of a different race than yours. Now I'm not endorsing that. I think it's a terrible idea. But as a matter of technology, such a rifle would be possible. So how do we make the decision? I think Bob and Ylli and I would say well, that's a terrible idea. Right?

So that's a simple example and I can think of many more complicated ones involving decisions in conflict where the decision is in a split second, where it's faster than human decision time.

So AI makes great sense in this nice thoughtful way that Bob has articulated, but the real issue is the compression of time. These systems are going to have to make decisions faster than human decision-making time and that's I think where the boundary's going to be. We have to have a serious about that as a society, in my opinion.

**Mr. Work:** We've already identified several use cases where the

time compression is beyond human capacity to operate. One is in cyberattacks. There's no way when we are under a broad cyberattack, especially if the cyberattack is being controlled by an AI system. Humans just won't be able to keep up with attacks in microseconds. We will have to delegate to the machine. Machine, it is up to you to defend against these cyberattacks. And we've already made the decision that we will do that.

I already brought up the Aegis Combat System. In raids where you're facing hundreds or scores of in-bound missiles, we have already said we are comfortable delegating authority to the machine to make the decision on how to stop those missiles.

Now there is an example that we also have already said is okay. Imagine that we have detected a group of 50 enemy tanks at 150 miles. The human commander says I want to destroy those 50 tanks. We have developed weapons that I will refer to as a two-stage AI-enabled guided weapon. The first stage is a guided weapon that puts a bus over the 50 targets and then it release 100 guided submunitions and the guided submunitions make all the choices of which exact target they're going to kill, and then they go do it. It happens in seconds. There's no way that a human operator would be able to look through a camera, for example, and say okay, we've just released 100 guided submunitions -- no, you can't go hit that one. No, no, no, no.

We've already said it's okay, and it is consistent with international humanitarian law because a human has said I want to destroy those 50 tanks. The human doesn't care the order in which they're killed. He just wants to blow up those tanks. So we have already said that is consistent with our ethics and international humanitarian law and there has been really no pushback on that in any consistent manner.

**Journalist:** A quick follow-up. In terms of the more autonomous vehicles that we're now seeing within the Navy and other military forces, has there been any consideration of ethics? I know this came up with when we started seeing like Teslas and the autonomous cars. What happens when you have to make a traffic law, or in the case of this make a decision about not hitting something or not running into one of your other cruisers or ships out there?

**Dr. Schmidt:** It's interesting that the example that you're

using is the canonical example in AI for self-driving cars. The question was, the car is turning and it has a choice of hitting the grandmother or the baby, which one should it kill? It's phrased in a more artful way but that's the question. The correct answer is neither. In other words, you want to define these problems in such a way that the AI systems makes the system, I'm going to refer to Bob here, Bob's strategy around [precision] has the corresponding benefit of decreasing collateral damage which I think we would all agree is a good idea.

So my answer in general is you want these AI systems to achieve the precise objective with greater precision, and anything that is inconsistent with that is a bad implementation, a bad product, or a bad decision in general.

Bob, do you agree?

**Mr. Work:** I absolutely agree.

Essentially this is what happened in computer vision in the intelligence community. Up through 2015 a human consistently out-performed algorithms in picking out an image, an object in an image. But in 2015, machines started to out-perform the human. At that point the intelligence community says okay. We are going to do a really broad-based move towards AI computer vision because it works as well or better than a human.

The answer I'd like to give, and it's a very difficult one because of all these corner use cases that Eric talked about, is when we do our operational testing of these AI-enabled autonomous systems, we can actually determine if those systems performed better than humans in executing a task. And if that happens, we would be crazy not to go to an autonomous system. And if it doesn't do better than a human. In other words, if there are worse collateral damage outcomes with the system than if we didn't use the system and the human used it, then we wouldn't employ it.

I hate to suggest that, but I envision a future in which the Staff Judge Advocates on the staffs would say what autonomous weapon are you using? Have you considered whether or not it's appropriate for the use case? How are you going to make sure that it doesn't wind up with an unexpected outcome? And what are you going to do if you observe unexpected outcomes, what are

you going to do to prevent them? That is just going to be an aspect of future operations. Humans are going to have to learn how to work with these machines.

And to the point, if all we're going to do is have humans that do nothing more than do what a machine recommends to them, then get rid of the human. What we need to train our human operators and commanders to do is when should you use an AI? When should you rely upon an AI system? And it's an entirely different way to train our commanders. Again, we want the AI to make the commander, or help the commander make better decisions.

**Moderator:** Secretary Work, a question for you from the floor about the two-step tank busting weapon you described. Is that a real thing? If so, what's it called? And thirdly, have we offered it to the Ukrainians?

**Mr. Work:** Yes. The first weapon we used was the ATACMS missile, the Army's -- it's a surface to surface ballistic missile. It was the bus. It shooted out over a tank column and it would release a guided munition called a sensor-fused weapon or when it was first built it was going to release a thing called the BAT, the Brilliant Anti-Armor Technology which would use acoustics to identify its targets.

We have a thing called the Wind Corrected Munitions Dispenser which is a bomb that releases sensor-fused weapons. And we used it in Operation Iraqi Freedom. The Iraqis knew that if they were moving around the battlefield they were going to be targeted by precision guided munitions. So they tried to move in a sandstorm. The sensor-fused weapon didn't care whether it was a sandstorm or high winds or not, and we employed Wind-Corrected Munition Dispensers in the sandstorm and knocked out a lot of Iraqi tanks. So they learned, hey, we can't move in sandstorms either. We can't move at all. We're going to get targeted.

We do have weapons like that now and we have other weapons on development.

In the Department of Defense if you want to develop a weapon, you can develop an AI-enabled weapon that mimics weapons already in the inventory. But if you're going to develop a weapon that does something different, you have to go through this very rigorous approval process involving the top leadership of the

department.

So yes, we do have the systems. What was the second part of the question, Thom?

**Moderator:** Whether it's been offered to the Ukrainians.

**Mr. Work:** I don't know the answer to that. The MLRS, the Multiple Launch Rocket System, is a precision rocket. It was called the 70 kilometer sniper rifle in Afghanistan. It essentially has a 200 pound warhead and it blows up within four meters of its target. So say about 12 feet. That is definitely close enough for government work.

Now we have a new type of weapon, the MLRS -- and we have said we cannot use bomblets anymore. We used to have these things called Dual Purpose Improved Conventional Munitions. Essentially they were little baseball-sized grenades that the missile would spread out over a battlefield. But because they couldn't discern whether it was a young kid thinking oh, this is a toy I'm going to pick it up, or if it was an enemy or if it was an allied soldier, internationally these weapons have been banned. So what the MLRS does now is it's like a shotgun round. Instead of putting out a grenade that has to be triggered, the MLRS sends out the rocket, blows it up, and a large number of fragments just cover an area. But they are not in and of themselves explosive, so there's no worry about leaving them behind.

I talked too long.

**Moderator:** Thanks very much.

Early on I called on Garance Burke of AP. He had connection problems. Garance, are you on for the final question today?

**Journalist:** Sure. Thanks so much. I appreciate you having this.

I noticed the report's mention of the use of drones in the first phase of war in Ukraine, and I'd like to ask what other autonomous weapons you believe could be appropriately deployed in the Ukrainian context?

**Mr. Work:** As you say, Garance, drones for sure. And drones,

again, are a two-stage weapon. The drones you fly out to a position on the battlefield where the enemy are, and then it drops a guided munition. And generally it drops on human control.

There are a slew of those type of weapons being developed. Missiles and drones. And you will see more and more of them.

I just want to read a Twitter account written by NTC Lead 6 at the National Training Center which is a place where Army units go to train against an operational force, an opposing force, that is trained in the doctrine and tactics of a potential competitor. This is what he posted yesterday.

"At sunrise this morning a swarm of 40 quad copters, all equipped with cameras, MILES" -- which is a system using embedded lasers that tells you whether or not you hit the target i "and lethal munition capable launched in advance of the 11th Armored Cavalry Regiment's attack on a prepared defense by the 1st Armored Division. Drones will be as important in the first battle of the next war as artillery is today."

So we are seeing already how drones are going to be more central to operations for the United States and our allies and we see that happening in real time in Ukraine. So these type of weapons are just going to be ubiquitous throughout the battlefield. And it's going to be important for us when we are developing them. What is the use case? What are the tactics, techniques and procedures that we are going to use to make sure that the weapon will not cause unintended engagements against civilians for example. But Garance, these things are going to be everywhere. They already dominate the battlefield.

**Moderator:** Thanks, Mr. Secretary.

We have time for one more. I'd like to honor one of the people on the call, former Naval Officer who worked at US Cyber Command. He's now a policy advisor at Baker Donelson. Michael McLaughlin, the last question is yours. And thank you for your service to our country.

**Journalist:** Thanks so much, Thom.

Thanks gentlemen for the discussion so far. It's been fantastic.

In your report you describe moving towards a techno industrial strategy. I'd very much like to hear your thoughts on the role of building a global coalition to advance this strategy. And specifically, what are the ways that the US can build a global coalition that's going to limit the types and amount of data collected by adversary technology companies while simultaneously supporting the expansion of American and allied technology as a means to counter Chinese and Russian authoritarian ideologies, censorship, and I think most importantly, AI development.

**Dr. Schmidt:** It's a good question and it's a complicated answer.

The first thing to know is that a lot of the technology in AI is being developed in a way of open source. And open source means that people collaborate and move it very quickly and it also means that your national competitors have access to it. It's well established that China, for example, uses all of that. So that's something that has to be discussed.

I've been telling people that my view is that some of these open source inventions are too dangerous to simply publish them. There needs to be a conversation about slowing down their distribution. There are some people who agree with me and some people who don't. So that's an example I think of your point.

I think in general what I learned in the Ukraine example is you have to start by having security of your own systems. And so the most important thing is that your own system is not being attacked by your adversaries. It always starts with defensive cyberspace, cleanliness, upgrading your software, all of that kind of stuff.

Bob and Ylli would you like to continue my comments?

**Bajraktari:** I think one of the things, Michael, we've been talking with our European and Japanese colleagues is dominating these battlefield platforms as Eric calls it, is we have to combine our competitive advantages together. In 5G, in chips, in AI, in none of these areas maybe we as the United States have a dominant lead. In chips, as you know, we lead because of the Taiwanese CSMC and the [inaudible]. In 5G I think we can potentially come up with an exportable 5G model together with our Scandinavian friends and our Japanese companies. So that's

how we would offer to the swing states, as we call it in our report, an alternative version to the Chinese platforms. But we need to take this lead to bring our allies and partners not maybe all, but there have been many calls to create a G12, we call it, or a democracy technology alliance, in which you bring our competitive advantages, the people, the R&D piece. We harmonize our policies. Because not everybody will have the same policies.

As you know, Europeans are rushing ahead to regular AI. The Japanese are also doing a lot of economic security policies.

So we can create some kind of a joint strategy between our allies in how we're going to dominate this battle of platforms and how we're going to offer to Third World countries.

**Mr. Work:** Michael, you touched upon -- we outline what we call six moves to win the competition. One of them is to build a democracy-led techno-industrial alliance and do exactly what Ylli just said. Cooperate and build secure resilient networks, especially 5G and Future G, cables both terrestrial and undersea, operating systems, data centers, digital apps, software and platforms. It's easier said than done.

We had a very similar recommendation coming out of the National Security Commission on AI. It was well received at the Department of State. They started discussions with our European allies immediately, and I think our Asian allies too, and said how would we go about doing something like this?

So this is more of an aspirational goal now, but as Ylli said, we're focused on the 2025 to 2030 timeframe and with good diplomacy I think we could have the framework for a techno-industrial alliance in that timeframe if we really pursued it.

**Moderator:** To all of our guest speakers today I want to be so respectful of your time. We've actually gone over. This has been a very thoughtful, very thought-provoking discussion about a very important work, your report. So thank you for your time, and safe travels to everyone.

**Mr. Work:** Thom, thank you for moderating. And again, thanks to everyone for joining us today. I can't think of anything more important than the subject of this report and hopefully we'll see some concerted effort behind it as the report is published

and disseminated and considered by our national leadership.

**Moderator:** Thanks again, everybody. Have a great day.