Special Competitive Studies Project
Ylber Bajraktari
Justin Lynch
Peter Mattis
Luke Vannurden

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

26 October 2022

Moderator: We're responding to the overwhelming interest in your work and the attendance for the recent session with Eric Schmidt and Bob Work set a record for our organization, so we are honored to have you back to discuss your next two reports.
The one on Intelligence in an Age of Data Driven Competition; and then, of course, The Future of Conflict and the New Requirements of Defense.

I'd like to thank the Howard Baker Forum and DXE Technology for their support of everything that we do. Also a very special thanks to Tara Rigler, someone I worked with for 20 years and who used to be the gold standard of communications, and it's just great to be working with her again.

I see most of the people around the table. I know Ylber who is the Senior Advisor for Defense and Intelligence; Justin Lynch who's the Senior Director for Defense; Peter Mattis is your Director of Research Analysis for Intelligence; and Luke Vannurden is the Associate Director for Defense at the Special Competitive Studies Project.

While normally we jump right into Q&A, I think it would be valuable since your reports are so thorough and so deep, I've actually read every word but can't say I'm fluent. In fact I'd ask you for just a quick sort of top line/bottom line, what you think the most important points are, and then we'll jump into a discussion.

Mr. Bajraktari: Good morning, everyone. Good morning, Thom. Thank you very much for having us today and for the opportunity to have this discussion, as well as the discussion in-house previously with Dr. Schmidt and Bob Work and our ARCEO and for your many years of excellent reporting at the Pentagon where I

had the privilege of spending 13 years and we're often learning from your writings about what was happening in the building. So I really appreciate the opportunity to have this conversation.

As you noted, Thom, back on September 16th we held our Global Emerging Technologies Summit in DC which was in conjunction with the release of our mid-decade challenges report. That was the executive summary of the totality of the work we were doing and what has followed since then has been the issuance of six substantive chapters that we talk about in the report.

So we're leading with Defense and Intelligence. Those two chapters from that report are now on our web site. We have four more chapters coming up over the next four to six weeks. So today we'll be discussing the Defense and Intelligence report and obviously welcome the questions they may have.

Just a quick highlight by way of substance on the two reports.

On the Defense side what we did was we looked at is the character of war changing and how it may be changing between now and 2030, and our answer to that is yes, and it's changing rapidly. Justin can get through the drivers of change and the manifestations of those changes.

The second issue we looked at is does China have a plausible theory of victory against the U.S. military? The answer to that is yes. For sure.

Thirdly, is what could the U.S. response be, both to the changes in the character of conflict and to China's theory of victory against the U.S. military. We have about ten different recommendations that we come up with under the Rubric of what we called Offset X, a new defense competitive strategy that again, Justin can elaborate on.

So that's on the Defense side, those three are the key themes on the Defense Chapter.

On the Intelligence side, we also looked at a similar issue which is how the strategic context in which the intelligence community operates is changing. And we identified four dynamics that are really changing the strategic context.

One is the geopolitical competition with China. That's

fundamentally changing the intelligence requirements.

Two is the need for technoeconomic intelligence, that's clearly on the rise. No more is it a matter of order of battle, counting military hardware only, or getting that exclusive report from the foreign ministries. Increasingly we have to pay attention to the technoeconomic aspects of the competition.

The third dynamic is the volume and velocity of data as well as the technology that's coming online that allows you to collect and process this data.

Then lastly, is the disinformation aspect of it. The ongoing relentless attack against our very own democracy that are taking place.

And then we offer four recommendations on how the IC should be responding in this new age of data-driven competition.

That's all from me by way of introduction to these two chapters. Again, I appreciate the opportunity. With your permission I'll turn it over to Justin who can get into greater detail on the defense element and to Peter who can speak more on the intelligence aspect of it.

Mr. Lynch: Thanks Thom and Ylber.

To go into a little bit more detail into the four sections that Ylber just described. I'll highlight first a few of the drivers when we talk about changing the character of war, starting at the strategic level and then moving down to the operational.

At the strategic level the biggest one I'd highlight off the bat is that we're in an era of persistent conflict below outright warfare, but still conflict, not competition. Mac Thornberry spoke at our summit in the fall and I think he said it really well, that Americans think of competition as something that happens on the golf course and we moved past that with things like sabotage of critical infrastructure, massive intellectual property theft, and really aggressive disinformation and misinformation that targets our social cohesion in an area of persistent conflict.

The second thing at a strategic level is what we call the individualization of war. We can go into more detail about that

in the question and answer section, but I think the top line to highlight right now is that previously in earlier conflicts we've seen where targeting whole societies or militaries was a route to achieve strategic effect, and increasingly we're seeing through technology and then some political changes as well, the potential for targeting individuals at scale as a way to achieve strategic effect, and that ranges from integration campaigns, misinformation that targets the individual, all the way to things that are kinetic and tied to network analysis to try and degrade society or militaries' ability to function.

The third highlight is that wars between great powers are more likely than they have been in the recent past, from the combination of geopolitical and technological effects. We think those wars would be unlike anything the United States has experienced in its past. And even different than what we're seeing in Ukraine since we're talking about wars directly between great powers, and they would be unlike anything because of the amount of resources that could be moved into those wars than because of the really extended reach across all domains that we see. So it's something Americans could very easily experience directly on our own soil, in our cyberspace directly and then in actual space.

Another thing to highlight for the strategic level is that that type of conflict -- wars between great powers -- has every potential to move into a protracted conflict rather than being some sort of quick decapitation or quick war that's won in 72 hours or a couple of weeks the way it's often depicted. It could be something that's very prolonged and could turn into a competition between industrial bases and our ability to innovate in our adversaries' national will rather than just bold maneuver and great tactical choices.

The last strategic level thing that I'll highlight is that we are guided I think really well by our ethics and our laws, but we shouldn't expect that our adversaries we're most likely to fight, especially those in authoritarian states, to be guided or constrained by the same ethical frameworks that we are in their development and use of technology.

A few things to highlight at the operational level. One is that emerging technologies are already qualitatively changing the way that we perceive the world, that we understand it, and that we make choices in the sense that we can absorb vastly more types of

information and a vastly larger quantity of information across a much broader part of the world, and then understand it much better than we could even in the recent past, using AI-enabled software. And then make decisions that are better and faster using software as well.

The second thing to highlight is that the proliferation of software and its ability to be very quickly updated and those updates to be fielded and implemented very quickly is accelerating change, along with some other areas of emerging technology. And that all these together are really fundamentally changing the [hider/finder] competition as it's referred to in DD, with forces trying to hide and be able to maneuver without being perceived, and adversaries being able to find them. And then today with proliferation of precision-guided munitions, especially in drones, being able to strike them as well.

To briefly touch on the China section of the defense report, as Ylber mentioned already, they are competitors and rivals and the PLA certainly have a theory of victory for how to defeat the United States. They've studied what we've done for the last couple of decades rather closely and they developed a theory of informatized warfare that describes how the United States fights and then develops systems of structured warfare to be able to match and defeat the U.S. informatized warfare Informatized warfare is what you think of networks of precision-guided munitions engaging each other.

What we're also seeing is they have every intent, and clearly stated, to be able to leapfrog U.S. capabilities by being first movers in what they're calling intelligentized warfare that capitalizes on artificial intelligence, increasingly powerful networks like 5G and quantum computing, and other emerging technologies to attack an enemy's ability to understand the world, perceive the world, and then be able to still outpace decisions in cognitive warfare.

Those are all significant challenges. The ability to apply force to create force is changing, we outlined that in the first part I think rather well. And then we talk about how China has a plan to be able to defeat the United States in warfare. But we still think the United States has very significant advantages that are created by democratic institutions or practices and longstanding organizational biases, things like that that are helpful.

To highlight a couple of those, I'd say that our demonstrated experience in joint operations in combat, combined operations, and working with allies is certainly a strength that it would be difficult for the PLA to replicate quickly.

Similarly, we empower our leaders at the tactical level as well. We have a really robust history of executionary logistics globally that's hard to match. And the one that's very notable, of course, is our really strong network of partners and allies that China would struggle to replicate quickly.

If you look at those asymmetries that are difficult to replicate, that means that even if China were to be able to replicate the technology that we have, we can deploy it and employ it in a way that's difficult for then to match, which if we plan it out effectively, it means that we have capabilities that are difficult to duplicate, that we can use to our advantage. Which is really what Offset X is about, is about having capabilities that can be generated by the 2030 timeframe and fielded at scale that give the United States an asymmetric advantage that the PLA would have trouble to replicate.

I'll highlight three parts of Offset X at the very beginning before moving to the intel section. The first is, we think that the United States needs to become more capable for distributed and network-based operations. A couple of things to highlight about that distributed, we mean geographically, network based, as opposed to hierarchy based. So if you think of your organization as less of a kind of traditional tree of hierarchy and more of a network with nodes on it and that those nodes are properly trained and equipped to be able to operate together, but also with a degree of independence which will make them more resilient and more responsive even in an integrated environment.

The second area is human/machine collaboration, human/machine teaming. The idea that humans and machines have different strengths, and that by working together on the right tasks together they can out-perform either autonomous systems or humans working in isolation and that human/machine collaboration can help on planning and decision-making tasks and that human/machine teaming can help accomplish complex tasks in physical spaces, and together that will lead to a that's much more effective at planning, much more effective at decision-making, both in the quality of the decisions and plans and in the pace of doing so, and then can accomplish tasks and field mass and reduce the risk

to U.S. human life.

The third area to highlight is software advantage, where software is a key component of our ability to sense the world, understand it, and make decisions and that the military that has the better software and can field and update it more quickly, has a marked area of strength.

With that, I'll pass it over to Peter.

Mr. Mattis: Thank you very much, Thom, for having us. It's an honor to see all the names on the page, names that I recognize from print but not necessarily from previous conversations or interactions, so it's a genuine pleasure.

As Ylber mentioned, the intelligence community is facing four big imperatives for change with the emerging geopolitical rivalry with the PRC that has economic, technological, ideological, political, military dimensions in sort of a full spectrum rival, if you will. The need for integrating science and technology and economic data into our system, the emergence of new tools for managing and making use of that data, and then the relentless disinformation attacks and other kinds of influence campaigns that are meant to disrupt the functioning of our democracies.

So broadly speaking, we see this as requiring an effort to build new capacities to manage and use information and transform it into intelligence to support decision-making, to build new capacities for bringing in information to the system.

If you think about, assuming we're all in the Washington, DC area, on some issues of national defense and security most of what you need to know is within a 15-20 mile radius of where we are. But when you think about what the United States knows about technology, the economy, what's going on in the world, this is much bigger than this area and we want to find out where that information is, where it's being held, and how to bring it in.

Third, supporting the employment of new technologies to counter disinformation and other efforts in the information space to disrupt our systems.

The challenge of doing these things comes from the fact that we're going to have to, we're trying to push for a change without the benefit of a Sputnik moment or a Pearl Harbor, something that

vividly captures an imagination, that suggests that there's something wrong.

And in some of our early conversations we had the concern that it wasn't that the IC was performing poorly, it's that it couldn't compete, it's not that it couldn't contribute, but a concern that over time an inability to grapple with these challenges would mean that the IC was unable to meet the needs of the United States government as it moves into this more competitive landscape.

There's a slow drop to irrelevance. You know there's certainly still some room for some strategic failures, but if you think about the way in which Ylber described the competition, at the point that we have a Sputnik moment it may be too late to make the changes that are necessary.

So we've drawn this out in sort of four main areas. The first is digital transformation for the IC. This is an area where the intelligence community is probably the first part of the U.S. government to recognize the value of AI and other data management tools, but all of the strategies and implementation efforts have sort of run aground in sort of the bureaucratic process, and there's uneven implementation despite excellent strategies, excellent plans. This is something that's going to require administration, congressional and IC leadership focus to sort of set the priorities, make clear the standards, and ensure that the system keeps moving along through this process.

The second is the issue of open source. In this case we recommend the creation of a new sort of national center for open source -- an open source center that's serving a national purpose rather than being tied to any specific departments, interests or views. Because we've seen how that has not necessarily met the needs of the U.S. government or of the country as a whole.

I think some of you may remember that FBIS and OSC used to disseminate things publicly, get thing through the world news connection, and it was a good update. This gets to the point that we're not concerned with the organizational structure or where exactly it sits, so much as this open source organization should have this public role. It should serve as this gateway between the U.S. government and the outside world as a two-way street. A gateway is not simply a one-way pipe. And that way we can start rebuilding the connection and the conversation between

the rest of the United States and the intelligence community and the national security establishment.

We also think that this center should be connected to the intelligence community, the value of the IC's sort of infrastructure, the way in which it does analysis for the U.S. government makes it too important not to be part of this intake and the conversation.

It also needs to be there to think about how to build expertise and to contextualize information. How do you overcome the bias against open source that people complain about culturally within the intelligence community? And I'm not sure that we've even really hit the culture problem so much as we disseminate intelligence reporting with a lot of context. On an open source, a lot of this gets disseminated with just the translation. And how do we make sure that we have people that can explain its value and assure that that value is actually taken into the system and spread around?

There are a few other characteristics we could go into in the Q&A, but I'll move on to the third part which is an idea of a national technoeconomic intelligence center. How do you capture the knowledge and expertise of the U.S. government and the country as a whole, and be able to make use of it to inform our policy thinking on what does the economic and technological landscape look like? If we're putting down new rules, sanctions, export controls, foreign direct product rules, can we game out what this looks like? What the impact is on who we're trying to target and what the impact is on our own system? Can we inform the tabletop exercises and the wargames that mean an economic component for people to think through? How do we have a sense of the landscape, kind of a net assessment view of the technological competition?

And then lastly, as Justin and Ylber mentioned, the PRC in particular, but not only, has gone after our companies and our technologies, and can we get more effective at providing warning to our companies about the threats that are coming to them, not simply in cyberspace, but as matters of strategic interest to nation states.

Finally, on the issue of countering disinformation, we'd like to see a sort of continuation of the effort that we saw work so well with the run-up to Russia's invasion of Ukraine, trying to pre-

debunk the narratives and inoculate people's awareness against the disinformation that's being fed into the system.

Second is to get better at warning, and not necessarily to leave this as just the government piece, but how do we bring in other parts of academia, think tanks, private sectors to build off of that warning and to see the themes and to encourage the work that would say okay, here are the issues, here are the actors, here are the themes that they're going after.

Third, we do need to get better at figuring out the response to denigration campaign efforts to paralyze the decision-making or the attitude of individual officials to disrupt our decision-making.

Lastly, how do we apply new technologies to keep up with the threats that are there? China and Russia have both applied AI to their disinformation efforts, and those have been able to outpace the capacity of manual efforts to take down those networks of disseminating disinformation. So how do we take advantage of the technologies that are available and use them in an ethical and responsible way to address the challenge that's coming at us that's sort of too big for a human brain or pen and paper kind of approach to deal with.

Moderator: That's an incredibly rich serving. I'd like to unpack a couple of things before I open the floor to questions.

You answered part of my thinking about the what is to be done, but I'm really interested in exploring a little more our asymmetric advantages over China, and China's over us.

It's true that the U.S. has a system of allies and partners whereas China just has clients, and the relationship is so different. Nonetheless, the spread of economic might, China's dominance in the information environment, and in fact Xi's a role model to many emerging countries, is something that we haven't really learned how to counter. What should se do there? And as you look to the lessons of allies in the war with Ukraine, at the risk of cliché, there's no Poland next to Taiwan. So what do we do?

Mr. Bajraktari: Thank you very much, Thom. A great question.

I'll start maybe with one overarching theme that cuts across our

report and then I'll turn it over to Justin who can speak perhaps more to the defense aspect of it.

As far as the overarching theme, and I think you heard Dr. Schmidt and Bob Work and Mac Thornberry talk to you about this in our previous conversation, which is that in China right now what you see that potentially puts them at a slight advantage is a very concerted effort of public/private partnership, rallying the resources and the focus and the determination behind some of the technologies that they're pursuing. So they call it the civ/mil fusion, but in essence I think it captures sort of the public/private partnership that they have. In instances not really a partnership, the state directs the private companies there and what to do.

But it speaks to their determination, their focus, to their desire to resource the technological priorities that they really see as both key to overcoming some of the challenges they're facing economically, demographically and militarily, but also to how they approach the rivalry. So that's the overall I would say theme that we tried to address in our report which is what is that model, what is the U.S. model of public/private partnership? How do we harness the capital, the knowledge, the innovation that now resides primarily outside the government, in contrast to the Cold War where most of the innovation was happening inside the government, most of the R&D was paid for by the government. So how do you harness now this new geometry of innovation where innovation is happening in the private sector, private capital obviously outside the doors of any government budgets. So how do you bring some sort of a model that harnesses this, that's reflective of our ideology as a country, our democratic system of governance but that is responsive to the geopolitical competition?

I'll turn it over to Justin to speak to the symmetries on the defense side.

Mr. Lynch: Thanks Ylber.

For the defense side I think it's very helpful to think about what the United States gets from our allies and partnerships globally, and then what China gets from the relationships it has with other states as well.

If you think about what's the product of the idea that the United

States doesn't go to war alone, speaking in a defense sense. We have greater legitimacy internationally by building a broad coalition of nations that contribute to what we're doing and agree to what we're doing. We can certainly pull together a much larger military mass. The United States is often the greatest contributor but we're never the only contributor to have military power in a conflict that we're involved in, which helps in fielding forces, it helps in logistics as well, and a wide variety of things, especially post-conflict.

We're able to achieve broader, deeper effects across all domains by working with our partners and allies than we'd be able to do otherwise, which is similar to but different from the mass piece to it.

Then we're able to advance on many more axes than we'd be able to otherwise. It creates a much larger number of options for us operationally than it would have otherwise and creates uncertainty and unpredictability for Chinese military planners.

Then one of the biggest pieces of this that really kind underlies all these others is how that affects our global posture and our global access for military operations. We are stationed in such a large number of countries already, the United States, which helps with logistics, it helps with being able to actually maneuver our access, expands where we are even further. All of those are very, very significant advantages for defense, and China struggles to replicate very many of those. It's certainly an area where they're actively working already, but if you look at the scale of advantage that the United States gets from that, it will be a while until China can reach that, if ever. Especially if you look at the relationships they're establishing with countries as they do.

Moderator: Thanks. I'd love to follow up, especially because they do have relationship dominance in the Taiwan theater, to say the least.

I'd love to open this to the floor. Either hit the raise hand button, or just come onto the video and microphone. Who has a question or a comment?

Mr. Bajraktari: Thom, while we're waiting for any potential questions, Peter can also speak on the symmetries when it comes to the intelligence.

Mr. Mattis: I think to build off of some of what Ylber and Justin said, it's worth thinking in the intel context, as you think about where, how the U.S. intelligence community works, how Russia's intelligence community, how China's intelligence community, if you can call their systems communities in the first place. One of our distinct advantages is sort of a devotion to truth and objectivity. Right? When you look at people who get accused of politicization in the system, there's a gut response of I did something wrong, and that there's an ideal that the truth will set you free, as it says on the walls of CIA. Right?

And when you look in their system, the Washington Post's incredible reporting n the intelligence piece running up, you know the FSB had good intelligence about Ukraine's willingness to fight, but they were unwilling to provide it to Putin. They said Ukraine, they chose to reinforce his assumptions about the Ukrainians rather than to say well actually, this might be a little bit harder and maybe we should rethink.

It's worth considering the fact that Stalin at least got intel delivered to him saying that the Germans were attacking. In this case, Putin didn't even get it.

In the Chinese system they have a similar sort of issue where the theory and the doctrine and they have this policy process, the way they see the world comes up with the view of what they would consider to be a scientific view of history and the trends of the times, and if things are running counter to that, it takes a lot of effort to shift and move that off of the system. And in a situation where Xi Jinping has more and more control and is closing off the information environment and less and less can reach him, it's harder and harder to make a shift to that kind of fundamental assessment of the world and how to move things forward.

The second piece is that it may sound a little bit odd to us, but when you look in these systems, one of the key differences is that the U.S. intelligence community serves a national purpose. It's serving a national purpose above administrations. Like all U.S. government officials, intelligence officials make their oath to the Constitution, they serve at the pleasure of the President. It is not a personalized system. It's not devoted to a particular political party. And if you look in the Chinese system, for example, even though they moved some of the

intelligence work into the state, all of the oversight bodies, all of the control mechanisms are in the party. Not on the state side.

The third is, as Justin and Ylber said, we work with allies and partners in fundamentally different ways. There's a lot of creativity, there's a lot of sharing, there's an ability to work with anyone just about anywhere in the world at almost any time to be able to do something that's productive and mutually beneficial.

The liaison partnerships that the U.S. intelligence community has are not because we have political client states or because we forced certain kinds of connections, but that we found a way for people to find benefit and to work together, and it allows creativity.

I think when you take everything that Justin, Ylber and I have said, one of the great strengths of the U.S. system is that we can solve problems that we don't know about because we can bring ideas in, we have real allies, we have real partners, not just internationally but domestically that can bring those to attention. Whereas these systems that are a required direction are really going to solve the problems or work on the problems that they know about. They don't have a mechanism for the unknown unknowns.

Moderator: I have one question in the queue from Brenton Monroe whose microphone is not working.

The question is, how important do you see the Indo-Pacific as a strategic region for China to leverage stronger partnerships that could upset the overall advantage the U.S. currently has?

Mr. Lynch: The Indo-Pacific is an incredibly important region. It's certainly where China's moving early in leveraging some of its, or trying to leverage some of its efforts. If you think about the economic growth that's projected across the next 20, 30, 40, 50 years, the Indo-Pacific is one of the key regions. It's where a huge percentage of the world's population lives as well. It's certainly where a lot of technology powers reside.

So China leveraging its relationships there to try to achieve global advantage is certainly important. And when I say leveraging relationships, I don't mean in the sense that we would

leverage relationships, but leverage power and coercion as well, to try and gain advantage.

It's not the only important region of the world. Our recommendations are fungible outside of the Indo-Pacific, but when we look at who we think of as the greatest threat to the United States, it's certainly China and operating in the Indo-Pacific, in the military sense.

Moderator: Any other questions from the floor?

Mr. Mattis: I guess as someone who's spent most of my professional life focusing on China, I'd point out that Xi Jinping and his predecessors have all made a point that China's ambitions for national rejuvenation are sort of global in scope. They've never really seen themselves as being a regional power or confining themselves to an arbitrary geographic deadline or barrier. Mao Zedong's principal issue with Stalin was that he thought that Beijing should lead international communism and not Moscow. So they've always had a global perspective.

And I think it's important to recognize that they recognize that yes, militarily and economically they have to be focused on their periphery, but they're still sort of constantly looking out beyond that and seeing how these pieces interlock and not just from the PRC outward into the region, but how are they able to do things on a global scale to help shape the region in a conducive way.

Moderator: You used the phrase Offset X, and what's interesting about the first three offsets of the United States, we dominate all of them. The first offset was nuclear weapons to countermand a larger Soviet force. We have done the first and had all the early [inaudible]. The second was precision guided munitions, revolutionized warfare. We led the way. Bob Work at the Reagan Library some years ago talked about the third offset which was in this AI/cyber world.

When you talk about Offset X, how confident are you that the U.S. can maintain its dominance in AI and cyber? Have we already lost it to China? And what are your concerns about the breakout in AI and cyber technologies that could change this calculus in China's favor the way the first two offsets favored the United States?

Mr. Bajraktari: Thank you, Thom. Great question. It really

goes to the heart of why we decided to name it Offset X rather than Offset four, if you will. What we're trying to get at, really, is that whatever advantages you may be able to score b the pursuit of the offset recommendations, that we should not be under the illusion that they will be enduring, that they will be perpetual, but rather these are temporal. The duration is sort of unknown, but you have to constantly go back and reevaluate how do they stack? How do the new initiatives you pursue stack against the evolving Chinese military thinking and the Chinese approach to the rivalry with the U.S.?

So in addition to being kind of an intellectual continuity of the concepts you really want to apply historically, we also wanted to convey strongly the point that this is not really a destination that you reach and then you can relax and that you can declare victory. But that you have to constantly evaluate these concepts, see how they will perform and whether they will deliver and then what changes need to be made?

So the recommendation really gets at sort of promoting a competitive strategic thinking on the part of the DoD, and laying the foundation for technological primacy so that it would then allow you to give rise to operational concepts that would perform if and wen the time comes to do that.

Mr. Lynch: I should note that our report, the Decade Challenges to National Competitiveness has a section about leadership and technology. But for the chapter five of that report and the defense IPR, we don't focus on dominance in a particular technology and we don't have a plan that's dependent on any sort of persistent dominance or uncontested dominance in artificial intelligence in the cyber domain or anywhere like that, because very much of what Ylber said where we view these as areas of active competition with the PRC and then possibly other actors as well.

So if you look at human/machine teaming or distributed network based operations, software advantage, what we don't say is you have to be the best in the world at artificial intelligence to be able to perform well here. We'd like to be. That would certainly be helpful. We would like to have uncontested supremacy in the cyber domain. That would be helpful as well.

But the ability to do these things we're describing and do them well doesn't require it.

There are other significant advantages we can gain. It's just outside of the Offset X part that we're describing.

[Fire Alarm sounds and announcement]

Moderator: Good. You can stay in place.

As I was talking to Tara earlier, your project lends a little drama. The last, we had Dr. Schmidt dialing into our Zoom from a plane after a secret trip to Ukraine. You all are dealing with fire alarms. There's always a little added drama.

The next question in the queue comes from Scott Campbell, and it's this:

Individualization in conflict raises a frightening specter for our people. Potentially a new kind of Sputnik moment if widely understood. Do you have case studies or powerful examples of what could be coming?

Mr. Lynch: There's a couple of important trends to note for the individualization of war. One of them is -- once you start with this broader concept that we described in the brief and then we go into quit a bit more detail in the paper. A lot of the data collection activities that we are seeing right now and we've seen over the last several years, start to fit together very neatly and then they start to become a little bit more suspicious.

You look at a broad collection of DNA of American citizens which has been reported by reputable sources as being a [Dolbert] effort. That's something that's happening accidentally. If you look at the collection of in-depth profiles of key individuals, and some seemingly not as key individuals across the United States, the OPM leaks or hacks. And then some of the things we've discovered recently about TikTok both in the sense of tracking and mapping of individuals who use it, their social network, then tracking their locations. All this fits together much more neatly under individualization than I think it did as a broader theme.

The second area that I would tie it to is the emerging literature coming out of the PLA about the intellitization of warfare and cognitive warfare that focuses every much on being able to target individuals' decision-making process, individuals' actions. We

haven't seen a clear operational concept from it that's been published by PLA sources, but we being the defense panel at SCSP, but when we looked at individualization of war as a trend that we're seeing from the technology side, then we looked at it and said okay, this seems to match very, very closely with what we're seeing, how to operationalize cognitive warfare.

Moderator: The next question is again from Brenton Monroe.

It was mentioned that the U.S. is guided by ethics and laws that the CCP is not, the PRC. How much of a disadvantage do you think this currently places the U.S. at? And how can it be overcome vis-à-vis China? Is it realistic to think the U.S. can compete in areas such as AI without compromising these immunological and I would add ethical constraints?

Mr. Lynch: SCSP's Defense Interim Panel Report notes that China and Russia may not be guided by ethical principles or legal conventions in their application of emerging technologies, as demonstrated by Russia's actions in Ukraine and China's actions in Xinjiang. China also has not disclosed any regulations or policy directives. We highlight that this may create tactical and operational advantages for China and Russia in a potential conflict. Nevertheless, we do not recommend the U.S. government and DoD deviate from their current ethical standards and robust internal processes that guide its testing, evaluation, and adoption of new weapon systems.

[Fire alarm sounds again].

Moderator: We'll wait for them to unmute after these alarms.

[Pause].

Moderator: Let's give it another 30 seconds or so. Everyone's time is valuable. If the alarm is still on, we can get a response from Tara and the team to distribute.

[Pause].

Moderator: Okay, out of respect for everyone's schedule, thank you so much for joining us today, and if you could just take that last question and if you want to email the response to me and I'll distribute it to everyone on the call.

So thank you so much, both the participants and the speakers in discussing this very important work. I hope you survive the fire alarms.

Bye everybody. Thanks.

# # # #