THE BROOKINGS INSTITUTION

WEBINAR

TERMINATOR ON THE BATTLEFIELD: EMERGING AND EVOLVING TECH IN THE RUSSIA-UKRAINE WAR

Washington, D.C.

Tuesday, November 1, 2022

PARTICIPANTS:

Introduction:

MICHAEL O'HANLON
Senior Fellow and Director of Research, Foreign Policy
The Brookings Institution

Presenters:

AMY J. NELSON, Moderator
David M. Rubenstein Fellow, The Brookings Institution

SAMUEL BENDETT
Analyst, Russia Studies Program, CNA

JACKIE A. KERR
Senior Research Fellow, Defense and Technology Futures,
Institute for National Strategic Studies

MARGARITA KONAEV
Deputy Director of Analysis and Research Fellow, Georgetown University

TOM STEFANICK
Visiting Fellow, Strobe Talbott Center on Security, Strategy, and Technology,
The Brookings Institution

GAVIN WILDE
Senior Fellow, Carnegie Endowment for International Peace

* * * * *

P R O C E E D I N G S

MR. O'HANLON: Good morning, everyone. I'm Mike O'Hanlon with the Strobe Talbott Center on Security, Strategy, and Technology at The Brookings Institution. We'd like to welcome you today to an event on technology and the Ukraine war, what we're learning, what we're seeing, what we need to take account of as we think about future warfare and the future of American military power, as well as this conflict and its own trajectory.

Amy Nelson will be the moderator. She's a David Rubenstein fellow at Brookings and my esteemed and well-regarded colleague. And I'm delighted that she's put together this amazing event. So in just a minute I will hand off the baton to her and she will moderate a conversation with Rita Konaev, Tom Stefanick, Sam Bendett, Jackie Kerr, and Gavin Wilde from various institutions around Washington and beyond. Their technology expertise ranges from the role of drones on the battlefield, something we've all been watching, to the kinds of sensor technologies that these drones and other platforms carry, to the way in which the data that these sensors manage to obtain is then communicated and shared on the battlefield, as well as dimensions of cyber artificial intelligence and disinformation.

So that's just a sampling of the kinds of topics you're going to hear about today. I think this is going to be a really important conversation. I'm going to sign off here in a second and look forward to listening to it along with the rest of you. We'll go until around 10:15, and if you have questions in the course of the conversation you could email them, please, to events@brookings.edu. One more time that's events@brookings.edu where we'll be monitoring and trying to get as many of those questions into the discussion as we can after Amy begins with a moderated conversation among the panelists and herself.

So without further ado, Amy, over to you and thanks very much for the opportunity to listen to this great event today.

MS. NELSON: Wonderful, Mike. Thank you so much. And thank you to all of our panelists. This is an all-star panel and it's everybody we would have wanted to hear from on this subject. So I couldn't be more pleased.

Just by way of brief introduction I'll just say that the title of this event referred to the film "Terminator," which premiered 40 years ago and predicted what war would look like 40 years in the future. Of course, it was for Hollywood, so it took place on a battlefield that had been ravaged by nuclear war but was replete with cyborgs and laser weapons.

But futurism and defense planning have always gone hand in hand and predictions have never been in short supply. So today we'll tackle the subject of how emerging and evolving technologies have played out on the battlefield in the current ongoing conflict.

With us today is Sam Bendett. I'll keep intros to a minimum because you can find lots of information about these incredibly smart folks online. Sam Bendett is a research analyst with the Center for Naval Analyses International Affairs Group where he's a member of the Russia Studies program. Today he'll discuss the use of drones on the battlefield and how their use has met or failed to meet different predictions.

Rita Konaev joins us today from CSET and CNAS. She is the deputy director of Analysis and a research fellow at CSET -- or at CNAS, and a research fellow at CSET, interested in military applications, FAI, and Russian military innovation. And she'll explore military applications of AI so far in the war, including Ukrainian capabilities.

Our own and NDU's Jackie Kerr joins us today. She's a senior fellow for Defense and Technology Futures at the Institute for National Strategic Studies at National Defense University, as well as an affiliated scholar here at Brookings. And she'll focus on the role that misinformation has played in the conflict so far.

Gavin Wilde is a senior fellow in Technology and International Affairs at Carnegie, where he applies his expertise on Russia and information warfare to examine strategic challenges posed by cyber and influence operations as well as propaganda and emerging technologies, and today he'll unpack the ways in which cyber operations have influenced the ongoing war and how this compares to previous expectations.

And finally, our own Tom Stefanick, who is a visiting fellow in the Foreign Policy Program

at Brookings will discuss the role of sensor data and autonomous sensing and communications in the conflict with a focus on NATO-provided capabilities to Ukraine.

And with that, Sam, I will turn it over to you.

MR. BENDETT: Thank you so much, Amy. Thank you, Michael. And thank you to The Brookings Institution for gathering us together to discuss this very important topic. So much of what we're going to talk about is basically going to be taken from the headlines. And in fact, the headlines every morning and every couple days seem to add more conversation and more topics to what we're basically discussing and that is the use of drones, the use of unmanned systems in general in this war. And I'm sure by the time we're done there will be another news item coming out of that war that would probably support or override some of our assumptions or discussions.

I think what is going to be helpful for you today from me is highlighting some of the main themes and some of the main technologies and some of the main sort of projections on the use of unmanned systems in the war in Ukraine. This is a topic that I study very closely. My CNA Russia studies program, in fact, conducts regular analysis of this topic with published papers which are available on the CNA website that look into the application of unmanned and autonomous systems in the war on Ukraine.

So one thing that I want to mention is when we talk about robotics, when we talk about unmanned and autonomous systems, today in Ukraine the absolute majority of military weapons supplied such as UAVs and other systems are, in fact, remote controlled. So if we use the military methodology, we're talking about a human in the loop approach. And so, for example, while Russian journalists, Russian media, and Russian experts like to use the word "robotics" or "autonomy" as sort of a catchall phrase, it is, in fact, still very much remote-controlled technologies which are on the battlefield today in employment by both Ukraine and Russia.

Going into this war, it is important to know that Russia probably had a better chance at least on paper against the Ukrainian capabilities. Russia fielded something around 2,000 different UAV types. It had very few combat UAVs but a very extension -- excuse me, a very extensive ISR

(intelligence, surveillance, and reconnaissance) roster of different types of unmanned aerial systems. They certainly practiced with these technologies in Syria, at home, and they used them in other conflicts and missions. But obviously, the war did not unfold as Russia intended or perhaps the war unfolded exactly as Ukraine intended as far as Ukrainian capabilities, it's seizure of initiative, and it's really taken the initiative and utilizing some of these technologies in better fashion than the Russians.

Both sides today use intelligence, surveillance, and reconnaissance drones very extensively. In fact, this is the main mission for unmanned aerial vehicles in the war. Along with that it's artillery spotting and targeting for the artillery and multiple launch rocket systems, as well as psychological and informational warfare. To date, no social media feed is done without any video from a UAV showing either Ukrainian or Russian attacks.

What became very clear in this war is that despite all the preparation, despite all the writings and discussions in Russia about the use and utility of combat UAVs and warning munitions, Russia in fact had very little of those technologies available on hand in the opening weeks and the opening months of the war and its industry, its policy, its government had to act very quickly and fill a very key capability gap.

The same cannot actually be said about Ukraine which fielded Bayraktar TB2 drones, first in combat capacity and then in intelligence surveillance and reconnaissance capacity. Both sides took some time but both sides eventually fielded better and more capable air defenses and other electronic warfare systems which were some of the capabilities from, for example, for larger UAVs sort of in the background away from frontline combat duties, more to the gathering sort of footage and intelligence about adversarial capabilities and feeding that information to more tactical drones.

Russia, of course, faced a very significant capability gap. And just as before, it turned to an ally. Over a decade ago Russia actually turned to Israel and purchased several types of UAVs which it fields today. When Russia understood that its own loading munitions and combat UAVs are not enough to stop the Ukrainian advance, not enough to put a dent in the Ukrainian capabilities specifically because Russia's loading munitions have a very short range of about 40 kilometers, Russia acquired loading

munitions and kamikaze drones from Iran. And this acquisition was very much in the news and continues to be in the news today.

Russia fields this technology mostly against stationary targets. The Iranian supply Shahed 136 and 131 which are fielded under the Russian name Geran-2 and Geran-1 are actually good at hitting stationary targets, not so much mobile targets that can maneuver quickly away from the original position. But this is also a very capable terror weapon since Russia can send waves of these Shahed 136 and 131 drones against Ukrainian civilian infrastructure targets, such as electrical power stations and heating power stations and other elements of the infrastructure in order to terrorize and force the Ukrainian population and government to come to terms. That is not happening and that is not likely to happen in the near future, but the open question remains, if Russia is capable of acquiring hundreds and perhaps even thousands more of these drones and assemble them in Russia under its own name, how would this war actually change?

This capability gap that Russia is fielding in loading munitions also perhaps exposed significant issues in Russia's own domestic military industry and specifically, defense industrial complex dedicated to manufacturing combat UAVs. It's not like Russia didn't know that it needed this technology. They very much knew that this was going to be an essential part of any warfare going forward, especially after Russia supposedly took some very good notes from the 2020 Nagorno-Karabakh war where combat drones and loading munitions proved absolutely essential to Azerbaijan's victory but its defense industry for a large number of reasons was unable to actually procure enough technologies that would be able to make a capable dent against the Ukrainians. Hence, the entrance of Iranian Shahed drones. Today there is news that Russia may have extended this drone contract. It may actually acquire additional drones from Iran.

And so the question remains, what are going to be Russian capabilities as a newly mobilized force enabled by these hundreds, perhaps even thousands of loading munitions that can fly for hundreds of kilometers against civilian targets and against some of the stationary military targets.

But one of the biggest stars of this war if we look at this objectively is the acquisition of

both sides of commercial drones. In fact, one of the Russian military generals, General Baluyevsky, he actually said that DJI commercial quadcopter is the real star of this war, and it has elevated artillery to the levels of capability not seen since World War I. The DJI quadcopters are absolutely ubiquitous and widespread. They fill, again, a very significant tactical gap in both the Ukrainian and Russian capabilities by providing ISR coverage a few kilometers to a few miles out.

So what's interesting about this is that Ukrainians seized the initiative. They were the first who were very capable in supplying their military and their volunteers on the front with these commercial drones, mostly DJIs simply because DJI as a company really controls a very significant share of the commercial drone market. And eventually, Russia actually caught up with respect to providing this capability and offering this to its military via the official channels but mostly via volunteers.

And this full commercial quadcopter technology isn't going to stop. It is likely to accelerate. And what's important, also, is that both sides are professionalizing the use of commercial technologies amongst their forces with Russian volunteers actually launching initiatives in Russia to train military and volunteers on how to handle and how to become familiar with the commercial drone technology.

So the real questions now facing both the Russian and the Ukrainian militaries are better integration of both commercial and military technology into a single mechanism, into a single network that can analyze data, that can actually function on behalf of the ground forces, artillery, long-range, and short-range forces and other capabilities.

Again, what's important to note if we note the title of our talk is -- these are all remote-control technologies. We see some degree of autonomy discussed and mentioned by the Russians. We see some of those capabilities discussed by other nations and powers building these technologies and providing them to Ukraine. We see Turkey and Iran mentioning autonomy as a capability. But in reality, again, this is going to be very much a human in the loop approach with humans controlling actions and humans controlling these technologies which is why the attack by unmanned surface vehicles and unmanned aerial vehicles in the Russian Black Sea fleet over this weekend is such an interesting

example of how these technologies are evolving with Ukraine once again seizing the initiative and using the technologies long discussed by all major military powers, Russia included, in a combination, in a group, to really strike a very decisive blow against the Russian forces.

This attack has a military as well as psychological significance. It drove home the point that Russian fleet, Russian capabilities aren't really safe even in home harbor they are supposed to be very well protected. And questions remain whether these capabilities can be scaled up and applied elsewhere.

So this brings me to my final point. Both Russians and Ukrainians prior to the war during this conflict and going forward consider the application of unmanned systems, possibly with a much greater degree of autonomy, is absolutely essential to future warfare. Both Russians and recently Ukrainians are stating the new war and the war of the near future is going to be the war of the robots. And the side that is able to scale up the production of these combat drones, whether they be aerial, ground, or maritime, and really mass manufacture them is actually going for the win.

Russia and Ukraine are also using a small number of unmanned ground vehicles, but really, the UAVs and now unmanned surface vehicles and other maritime capabilities are kind of seizing the show going forward. Whether or not both sides would be able to sustain this momentum, whether or not both sides would be able to field a large number of these systems is a good question. It's an open-ended question. Certainly, both sides are committed to using these technologies in the war. And so questions again remain what are the capabilities that these systems can have, how are they going to evolve, and whether each side would be able to well-integrate these technologies into their existing force structure.

Thank you very much.

MS. NELSON: Thank you, Sam. That was fantastic. And that question about sustaining the momentum and what it will take to do that has already come up in a number of questions and I look forward to returning to that during the Q & A.

Rita, over to you.

MS. KONAEV: Thank you for hosting us this morning.

Sam really set us off for an excellent beginning because I think he gave a really good reality check about the technologies that we have been looking at for a while in talking about the mystic technologies of tomorrow and in essentially kind of understanding the limits of their capabilities in the wars of today.

What I want to do for the few minutes that I have is elaborate a little bit about the use of artificial intelligence, machine learning, and some other autonomous technologies in this war that we're observing and draw some early lessons with the very serious caveat that this war has unfolded in really unpredictable ways in a way that really undermined and contradicted and nullified a lot of expert assessment and expert analysis. And I include myself very freely in that expert group. So all the lessons that we're drawing are done with the real caveat that we are still very much in the midst of this war and equally important, we are contained by the information that is available to us.

So with that in mind, the information that is available to us is also what we have in our hands to assess the use of emerging and new technologies on the battlefield including artificial intelligence. Artificial intelligence is one of those fields where there is a lot of hype. And there's a lot of incentives for all actors involved to kind of sometimes essentially inflate and perhaps even exaggerate a lot of the capabilities, a lot of the autonomy, the freedom of decision and movement, and sophistication of some of the tech that's being employed, including for one way or another some sort of a marketing perspective.

So everything that I say should be taken with a grain of salt given that it's coming from a variety of sources, whether it's official government, media, some of the manufacturers of these technologies that one way or another have an agenda of sorts, not necessarily nefarious by any means, but nonetheless an existent one.

So as Sam started off, we have seen massive use of AUVs, drones, and loitering munitions in this war. And as Sam has correctly pointed out, the absolute majority of these systems are being employed by human, they are remotely operated. Having said that, it's perhaps interesting to point

out that some of the advertised functionalities in these systems are still not fundamentally autonomous in the way that we envision perhaps the killer robot conversation. Even when these systems are advertised as autonomous, we are still talking about functionality such as takeoff, landing, and some navigation which are essentially more akin to an autopilot as opposed to the type of autonomy we have envisioned towards the end of the targeting chain where a system has the ability to identify, track, select, and even engage a target. So this is to say that they're already limited to begin with. Very few of them even have such functionalities, and even when such functionalities, the autonomous functionalities are advertised, they're still quite limited to what they can do.

The second set of technologies which I think is the one that is the real gamechanger if employed at scale and, hint, it's not, but it has one of the biggest potential I think and that is the use of artificial intelligence and machine learning algorithms for the processing of battlefield information. As we know, modern conflict produces massive amounts of data and a lot of it is absolutely crucial for making decisions. And we're at a point where humans are effectively unable to process, analyze, and glean useful information, useful information that's useful for decision making out of that massive sea of data. And that is where essentially, you know, AI and ML algorithms have the most clear potential to help with decision-making, to help with creating a unified situational picture of what's happening around us, and help them gain all of the advantages that are promised by AI, whether that's speed, precision, coordination, or the ability to reach lethality at scale.

Essentially, one of perhaps the best, the most advertised examples of using AI for battlefield information processing has been by an American company called Primer. And it's a company that's reported, again, according to news media and some Primer representatives, been working with Ukrainian forces -- it's unclear which part of the Ukrainian forces -- in order to capture, process, analyze, transcribe, and translate Russian military communications which, believe it or not, have been unencrypted quite often. So that ability to capture that information on the battlefield to really get within the processes of your enemy to know what they're saying, to know where they are when they're saying it, and to then so quickly be able to take that from data to information to usable decision-making, again, it's hard to assess

right now to what extent that capability is being utilized but the fact that it's already being used on the battleground, at least according to these certain reports, is really significant. I think out of all the four ones that I'm going to name it's perhaps the most groundbreaking.

The third set of reported uses of AI fall into the facial recognition category. And here you have a few examples and instances. You have some reports from Ukrainian ministries claiming that they've been using facial recognition technology or experimenting with it to identify people who are not meant to be in the country. So a combination of, you know, border patrol/counterintelligence operations, essentially. Again, the extent to which this has been utilized is unclear. The extent such a capability is actually even possible is also debatable, especially in a country that is in crisis and in conflict and there's massive amounts of displacement.

Another example of facial recognition technology is perhaps equally cryptic and potentially questionable and that is to use the stories that are coming out of a company called Clearview AI which has been supplying the Ukrainian forces with the ability to recognize Russia captured and deceased Russian troops that the Ukrainians then were able to match to let's say those deceased's social media accounts and then were using this information to contact the parents and the relatives of the Russian soldiers. And as part of a broader, essentially information campaign, to report back to those parents about the activities and the demise essentially of their sons.

That is, again, that is an area where I'm personally quite skeptical because facial recognition technology, especially coming out of Clearview that has had some issues of its own, is not sufficiently advanced or reliable to recognize bodies on the battlefield that have died an unpleasant death and to believe that they were then matched to the social media accounts of those individuals at scale is something that I think is perhaps something that could have been used as an example here and there to demonstrate, but the ability to use that reliably at scale I think we should be a little bit skeptical of what's happening.

And finally, there were also a few examples of AI machine learning algorithms being employed for information operations behind production of deep fakes and in authentic and fake social

media accounts that Russia has employed on platforms like Twitter and Facebook and Instagram in its effort to describe the Ukrainian cost, describe the Ukrainian leadership, and promulgate its, you know, misinformation information and disinformation information messages. And that's something that we have seen before. Again, this is unlikely being used at scale and we're also only able to glean what's happening within this capability based on successful takedowns of those accounts. And so on the one hand we're not necessarily aware how widespread it is but we know from a broad understanding of AI for this information operation is that the future is very scary and potentially extremely difficult and bleak to regulate but right now it's still kind of nascent in its early stages.

So with that I think an assessment of AI on the battlefield is it is absolutely employed and to perhaps it's fair to say at an unprecedented scale. But scale is a relative term, and I would personally not say or go as far as saying that AI is used at scale on the Ukrainian battlefields. Simply because something is important and unprecedented doesn't mean that it's everywhere and it's ubiquitous. Nor does it necessarily imply that it's already impactful and that alone determines the pace, you know, the trajectory, and the conduct of the conflict. We're absolutely not at a point where this set of technologies is really making that type of an impact. But again, I think of all of those, the ones that I mentioned, it's the AI for battlefield information processing that has the greatest potential and potentially already an impact.

With that, I want to say one key thing that I think is a vital lesson that we're learning from this war that hopefully we are able to take into our assessment of the U.S. military, our assessment of the Chinese military, and our assessment of just generally the strategic competition in general. And that is that innovation and the ability to demonstrate and experiment with sophisticated, advanced, groundbreaking systems is fundamentally different from adoption of such systems and the ability to use them in operational conditions to make a real impact on the battlefield. And I think it's critical for us in the think tank space, in the media, and you know, in government wherever we're doing these analyses and assessments, to be really, really clear and precise about where the technology is, the one that we're talking about. Is it at a concept level? Is it at a research and development level? Is it just simply being experimented with and demonstrated? Or are these capabilities already being integrated into systems?

Are they being shared across the board, across, you know, within the units that need them and can use them? And are they being deployed, once again, at scale in operational conditions? And the path from that early nascent concept idea through research or development, all of those points that I've outlined, to use that scale is fraught and full of challenges and full of barriers that are not necessarily the worst of them all, are not necessarily technical or technological. If anything, those barriers are the ones that I think require even more attention from analysts like us and those in our community, is the understanding of what are those barriers to adoption that are not technical or technological? What are the bureaucratic, the organizational, the cultural barriers that keep militaries and other organizations and bureaucracies from moving from these groundbreaking ideas and concepts to at the end the ability to use such systems and operational conditions?

And if there's time later on, I'm more than happy to talk about some innovation versus adoption dynamics both the Ukrainians and the Russians have demonstrated in this war and what we can glean from that. But I think the two main takeaways that I want to leave you with is that, yes, AI and machine learning are absolutely on the battlefield in this war between Ukraine and Russia. They're being employed potentially at an unprecedented level and scale and domains. But having said that, their use is still limited and still circumspect, and we have to be quite careful that we're not confusing examples and demonstrations with widescale use, adoption, and impact.

Thank you, Amy. Over to you.

MS. NELSON: Thank you so much, Rita, that was wonderfully informative and some really important points. You know, what you just said really mirrors a conversation we had about nuclear weapons a lot. What are, for example, the sociological impediments to actually adopting the technology, the nontechnical components? Also, really helpful to know that this is -- we're not at scale; right? That this has a long way to go and there's a lot of room for growth or fundamentally change. And so what we see now isn't necessarily what we're going to get.

Also, really interesting is that tension between, you know, well in advance of this war people talked about how the warfighter was going to experience information overload as a function of all

the multiple streams of data coming in and separately, the prediction was that the pace of warfare was going to become lightning fast. And so, and the role of machine learning and artificial intelligence and kind of moderating that tradeoff is really interesting to see here. So thank you.

And with that I'll turn it over to Jacqueline.

MS. KERR: Thank you, Amy. It's a pleasure to be part of this fascinating panel. Fantastic comments by Sam and Rita to start us off.

So I'll start with the disclaimer that these are my views, not those of NDU or DoD and move on.

So I'm talking to you about information influence operations during the conflict. And three main questions I'll focus on first, what are we seeing and how does it fit with predictions? Second, to what extent are we seeing new things about the relationship between information and influence operations and escalation potential? And third, what lessons or takeaways can we take from that?

So with regard to the first, it's become something of a cliché in Washington and elsewhere these days to talk about Russia losing the information war. It's not performing as expected. That we expected a 20-foot behemoth and in fact, it seems to be owned to some extent sometimes. And this draws in a long history, of course. Russia, going back to the Soviet History, long history of significant capabilities and the simultaneous manipulation of information, psychology, influence operations, things like active measures. And with the new forms of technologies in recent years, we've seen a lot of integration of things like hacking and information and influence operations, use of social media, state media, multiple platforms, and dimensions simultaneously for different sorts of mechanisms ranging from microtargeting to scalable campaigns. So in division, polarization, confusing, promoting narratives, and different combinations. These tool sets used in different instances ranging from going back to Estonia 2007 forward to COVID-19, everything in between. And Ukraine has stood out as a test bed for all of this ranging from very technical cyberoperations to information and influence operations, hybrid warfare, using these psychological information and cyber dynamics and dimensions. And so it raises questions, what's happened? Given this seeming violation of the assumption of democratic vulnerabilities, superior

capability that was being studied so much in the west to try to understand this is an asymmetric tool that seemed to play to the advantage of authoritarian states, and we assumed it would on the battlefield as well.

It's easy to point to ways in which early on since even before the war began, Ukraine and its western supporters have seemed to have superiority in the information space ranging from the releases of intelligence leading up to the war to the seemingly easy debunking of early efforts, fake videos, things like Zelensky videos saying that he is surrendering, news stories saying he's committed suicide or that he's left Ukraine and various things like this. Early narratives around fascists and Nazis seemed somewhat ridiculous at least to western audiences, and stories played out led to more questioning of what Russia was planning. That this seemed to be a false flat operation.

Of course, we have to bear in mind that sometimes it's easy to see things as ridiculous from where you sit and not pay attention to those slivers of populations where they have more residents. Tucker Carlson was endorsing and repeating this narrative over and over. There was a leaked memo that seemed to suggest that Russian state media was being directed to play these clips back to their domestic audience of Tucker Carlson, et cetera, and these sorts of feedback relationships with other national fringe media outlets. And of course, we see some repeat of echoes of some of this with the dirty bomb narratives today. But overall, a seeming superiority of the western solidarity around Ukraine, use of open-source intelligence, fact checking, reporting, the effective use of this David versus Goliath narrative and even sort of spunky, creative uses of things which are symbolic.

So it raises a question as to why Russia failed. And there's been a lot of speculation around this, that this was a deliberate attempt to use these capabilities, but it didn't succeed. That maybe the speculation about superiority was not as correct as we thought going in speaks to maybe some of the things that Rita was discussing about the difference between experimentation versus having a unified capability to use something at scale in real time in battle spaces. But then also questioning of whether Russia chose not to use certain capabilities, concern about escalation or use-to-lose dynamics of certain capabilities. And of course, there's some integration across the cyber capability and the information

capability issue sets, you know, given the extent to which Russia uses these in an integrated fashion quite often.

There's also the possibility that these capabilities are not actually the best tool for wartime. And we've thought a lot about them being useful across all levels of escalation from peacetime to gray zone to wartime. But, of course, in wartime there's more a laser focus on what's going on. And so these are tools that operate in the shadows, that operate best with surprise potentially, and that's the less easy, especially if the operations aren't completely, completely covert but then there's also a possibility that they have been operating in shadows and again, to something Rita said, we only know what we do know right now. And there are things which we don't know because they haven't been debunked and there hasn't been attention to them. And so there might be further effectiveness than we've seen, possibly not just in the theater of conflict but outside but in ways that could affect the theater of conflict.

So one thing which I would suggest is important to pay attention to is strategic targeting of different audiences. And we see some evidence of Russia working very creatively with different audiences, targeting different audiences, strategically in the long term. So there's been a lot of attention to what's going on in Ukraine on the battlefield, what's going on domestically in Russia in terms of targeting domestic audiences, what's going on in terms of things that scale to western audiences, to the U.S.

But how about targeted campaigns against particular NATO allies, trying to undermine the coalition? We know that early on there have been efforts to undermine Polish support or to create fractures through sowing narratives with fake accounts and persona of Ukrainian refugees be involved in crime. We know that there is potential for targeting of other NATO allies in similar ways through narratives around the economy, around the risks of large refugee influxes, around -- and beyond NATO, of course, also other narratives such as food insecurity.

I was in Sweden a few weeks ago and one of the things which was noteworthy there was that the right-wing party had gotten more a percentage of the vote than it ever has before. There's a

historic relationship between that political faction and the Russian Nationalist youth movements. And so questions as to what's going on there that we may not be fully aware of yet. And in the global south, of course, there is targeting of narratives around food insecurity, around western unfairness and unequal care about refugees from different parts of the world in different crises, and there's some beginning evidence that potentially some of these narratives have sticking power. And so while we can't have pure certainty as to what the long-term effects of any of these campaigns will be right now, they need attention, and they can't be written off yet.

And so thinking about the long-term effects and what lessons can be learned right now I would suggest two things. First, about operational risks of escalation as a result of information ops during the conflict. Well, there's been a lot of speculation prior to this about the potential role of information influence operations in the current information ecosystem on conflict escalation and crisis instability. I have contributed to some of this discourse, and I think it's too soon to draw complete lessons. Right now we haven't seen evidence of absolute certainty of this playing a role, like fog of war and crisis instability on the battlefield, but we also can't write it off.

What do we make of the Kerch Bridge and the sort of ready emotional victory of that on social media and the media and then the retaliatory response? We don't know what was going on inside decision making for certain and what role that played. And there's a lot more yet to be learned about the potential feedback loop effects of information and influence campaigns on the battlefield. The complexity of playing to different audiences comes with certain risks of inadvertent escalation. And what do we make of the dirty bomb signaling right now? Is it an effort at intimidation? It's a very ambiguous symbol to different audiences and for it to undermine war support. And what effects will it have besides whatever the intentional effects are?

So by way of takeaways and lessons to be learned I'd say that it's extremely important to pay attention to theaters outside of Ukraine and to other audiences that might be being targeted. And in the long term, strategic implications for support and coalition around Ukraine in support of the war effort. And also, second and third order effects of those targeting campaigns on stability in other regions and

globally. Also, it's too soon to make firm conclusions about what effects this is having on the battlefield right now. There's so much that still will be unpacked with time.

I look forward to the discussion. I'll hand off there. Thank you, Amy.

MS. NELSON: Wonderful, Jackie. Thank you so much. That was incredibly helpful and insightful. Especially, I was really taken with the comments, your comments about the conditions under which these tools can successfully be deployed and how little we know about that. And of course, the idea that it is still too soon to draw complete lessons. Of course, we're here today to draw some lessons but a certain measure of patience is going to be required in the analysis of all of this. So, as well as, you know, understanding the complexity that comes with the deployment of these tools and that there will be second and third order effects with which we may not be familiar. We may not be able to anticipate them very well. And so very much a space to watch. So thank you again.

And with that we'll turn it over to Gavin.

MR. WILDE: Hi, there, Amy. Thanks for having me. I found myself nodding hard at each of the previous speakers' points. And it's fitting that I'm following Jackie because I think my broadest point today is that from a cyber perspective, Moscow's long-time focus on the cognitive effects has potentially posed opportunity costs to their technical ones. I'll also caveat my comments similarly to say that there's much unknown and probably unknowable about the cyber dimension of this conflict in particular but I think it's safe to say that it's certainly prompted a reexamination of the prospects and limits of cyber capabilities in a combined arms campaign and has been less decisive in achieving Moscow's strategic aims than perhaps some predicted.

For the Kremlin, Ukraine should certainly prompt a reexamination of the theoretical and doctrinal expectations that it has placed on information warfare, particularly since Ukraine has borne the brunt of Russian information warfare over the last 8 to 10 years, arguably with very little strategic return on that investment from Moscow. Indeed, Moscow's geopolitical tilt away from them now appears a generational certainty.

Contrary to the mythmaking over the last several years, Russian cyber capabilities

appear to be at best adjunct to kinetic warfare and at worst simply unfit for purpose in a combined arms campaign. Their operations simply haven't lent themselves very well to the conventional wartime demands of timing, efficacy, and control, the same kind of dynamics that Rita outlined. And the known operations Moscow has deployed since late February appear to have fallen short in at least one or more of those areas.

This is important not only for tailoring our own expectations, many of which were somewhat outsized but in the context of Moscow's own theory of victory in the information space which equally emphasizes technical and psychological effects. Moscow has assigned doctrinally a massive burden to information warfare that now falls under question.

Timothy Thomas of the U.S. Foreign Studies Office once called information weapons Russia's "nonnuclear strategic weapon of choice." And he concluded, as do I today, that that notion was probably always due to collide with reality and friction.

For example, a 2011 document released by the Russian Defense Ministry set very lofty goals for information war including to fully degrade transmission networks and critical infrastructure, to undermine political and economic and social cohesion, to undertake mass psychological campaigns, all with this goal of eroding confidence in the target state's government and inducing the states by their leadership. However, the onslaught of disruptive cyberattacks, propaganda, and disinformation notwithstanding, Ukrainian sociopolitical cohesion has arguably not only been solidified but garnered unprecedented external support and has been galvanized against Russia at a historically high rate. So in short, Moscow essentially bet on information warfare providing decisive in interstate conflict but has largely had to settle for proving nearly disruptive.

Meanwhile, the portion of Russia's aggregate cyber power that gets dedicated to psychological operations like the ones Jackie outlined is significantly higher than that of the U.S. and other western countries. This emphasis on the cognitive aspect is reflected organizationally, suggesting that Russia has perhaps over indexed on impacting hearts and minds about Ukraine at the expense of impacting networks and infrastructure in Ukraine. We need only look as far as GRU Unit 54777 or SVR

Director at MS or FSB Center 18, the so-called internet research agency, to get a sense of the amount of cyber resourcing and capacity that Moscow puts on the assumption that societies are largely manipulable by a cyber means.

While the disruptive potential of these types of operations is certainly unquestioned, their utility in achieving strategic goals, particularly amidst a conventional conflict is far from clear. If anything, as I said, Ukrainian society and the trans-Atlantic community at large has done a very good job at prebunking or debunking, exposing and deplatforming these efforts so the question now becomes whether Russia's best days in the online manipulation game may now be well behind them with regard to Ukraine.

Similar to the dynamics that Rita, Sam, and others have highlighted regarding conventional armed forces, all of the sophisticated capacity in the world can't compensate for a lack of organizational coherence, doctrinal adherence, and logistical efficiency. That applies on the cyber front as well. It's all too easy to conclude that Russia's vast, disruptive cyber capacity can somehow be harness and channeled towards a unified goal. However, bureaucratic rivalries between the intelligence and security services like the FSB and the GRU and Russian military commands over cyber and information portfolios run very deep and very long. And the only entity likely capable of arbitrating such disputes is probably the Russian Security Council. And this would potentially make coordinated broader offensive campaigns as much a political matter as a military one.

Now, you'll note that these disputes are not unique to Russia. We've seen similar bureaucratic wrangling in the U.S. with regard to purview over offensive cyberoperations and those dynamics are certainly in play in force, if not vastly more so in Moscow.

Meanwhile, Moscow has attempted establishing a military cybercommand, kind of an analogue to Cybercom, the so-called information operations troops remains in its infancy. It was only formally stood up sometime in 2014 or 2015 with an apparent initial emphasis on information assurance, counterpropaganda, and psychological operations, much less on technical effects that I've been able to find. Unverified leaks since then, however, do call into question the degree to which there's any real

meaningful distinction between the information operations troops and those units of the GRU that engage in technical and psychological operations. For instance, according to some of these leaks, the leadership of the troops reportedly hails from GRU unit 26165, also known as Fancy Bear, and his deputy from Unit 54777, which was sanctioned by the U.S. for running info-Rus (phonetic) and other disinformation outlets and which reportedly oversees cy-ops planning for the entire military. In other words, it remains to be seen how much Russia's military cyber capabilities are merely subordinated or repackaged GRU capabilities.

Cyber scholar Max Smeets recently wrote a book which I'd highly recommend on the difficulties that states encounter in establishing military cybercommands, one of those being the familiarity of adversary networks that is the daily purview of intelligence agencies like the GRU or the FSB that are simply not very easily transferrable to other entities like a military unit for actioning. Russia's cyber forces appear to have been largely designed for perpetual confrontation and subversion and probably lack the kind of surge capacity that's necessary during conventional wartime. And it's precisely that deficiency that I think underpins U.S. notions of the need for "persistent engagement by its military command cyber forces."

Now, the landscape could radically shift tomorrow. Obviously, the prospects for escalation I think are certainly likely more acute in the kinetic realm but still remain in the cyber domain. The types of destructive malware, like Triton and Industroyer and Pipe Dream which target industrial control and infrastructure critical systems may still be at Moscow's disposal. But the good news is that the allied and commercial capacity that's thus far been brought to bear to kind of preempt and mitigate those types of attacks have made both Ukraine and the rest of us much more resilient. And it's worth considering at least whether some of the most lethal arrows in Russia's cyber quiver have already been fired or neutralized. And in light of the exodus of both foreign technology and domestic brain power out of the Russian market whether the Russian forces will ever be able to make up for that lost capacity.

As for what that all means for U.S. capabilities, I think I would echo national cyber director Chris Inglis that it does appear that the defense is ascendant. The coalition of states and private

sector and civil society actors that have swarmed to aid and Ukraine's already Herculean resilience project has set a high watermark for both resilience and reconstitution against some of these attacks and it's certainly validated the defend forward concept that cybercommand has practiced and underscored how coalitions and partnerships can gain the upper hand against even the most sophisticated of attackers.

So with that I'll turn it over to you, Amy.

MS. NELSON: Fantastic, Gavin. That was really great. I'm particularly struck by your comments about how effective we've become at pre-bunking disinformation efforts. We already have some questions coming in from the audience about to what extent Russia's failure at large-scale information operations is an indication that they're less capable than we thought as opposed to just the fact that widescale information operations in this environment are harder than we thought and perhaps less useful. So hopefully we can come back to that in the Q & A.

Also really striking are your comments about how Moscow has overplayed its hand on cyber operations, and I really liked your phrasing about how Moscow has overemphasized hearts and minds relative to networks and infrastructure. And of course now we're seeing kinetic attacks on infrastructure, perhaps suggesting that, you know, cyberattacks were not effective.

I don't want to take up too much time with that. We'll move on to last but not even remotely least, Tom Stefanik.

Tom, over to you.

MR. STEFANICK: Thank you, Amy. And this has been really a terrific discussion. And I don't really have anything that I can add to this on the specifics.

I would like to turn a bit to the future very briefly and bring the focus, I think, in to much more the sort of battlefield use of information and artificial intelligence which is sort of the subject of our discussion today or so-called artificial intelligence. And by battlefield, I mean sort of what's on the ground. Now, the war in Ukraine has shifted in some significant ways from the initial attacks and warfare in the northern part of the country, a much more urban, wooded area. And now it's settled in we see to a

more static, not completely, but it's an infantry focused war. And while technology is still very important there, it's sort of tragically turned into this infantry versus infantry conflict. There's just a reminder that ground warfare has these sort of enduring principles. It requires human beings to take and hold territory.

Now, that is to contrast very much with a potential conflict with China or a crisis with China. This is largely a maritime, you know, there's islands of importance. I'm not going to go into that but it's largely a maritime region in which the use of battlefield information is very different.

I'm going to just talk about the information dynamics. There are so many systems and I just want to kind of raise the level of obstruction a bit to think through the picture. You're seeing a little bit of it now, but I think we're seeing just the very beginnings of the dynamics of battlefield information technology, and it's been mentioned, everyone, it's mentioned and Sam and Margarita mentioned this quite extensively, but battlefield information really is, in a simple sense, it's knowing where things are, how they've been moving, their tracks, and what they are. And that information is the key information for fighting a war.

So you can imagine, if you're going to take away all the various weapons that have been in the newspapers and what weapons we've been sending, it will come down to reducing uncertainty on the battlefield, which is a constant information is the reduction of uncertainty. And the dynamics of dealing with struggling for dominance of battlefield information I think is sort of the future dimension that actually does translate to future conflicts, especially great power -- God forbid a crisis or greater power conflict. We tried it in a maritime scenario.

And by information, to again simplify it, it's sensing what -- getting data from the physical environment into a digital environment, moving that data, communications, interpreting that, and then making decisions. And that's the role of command and control. There are lots of acronyms for command and control. I'm not going to use them. There's C4 and SR and America's GAD-C2. The Chinese have their own version of this. But it's really just those things. It's data from the physical environment and moving. All of these things move information back and forth, largely through the electromagnetic environment, which is simply that part of the environment that we all live in and use -- wi-fi, cameras,

satellite, radios, everything. And that's' the environment which is the primary -- one of the areas of the primary struggles. So, if one can sort of simplify the conflict of information, it's injecting noise or disruptive data or false data into sensors so that simply there might be lots and lots of data which we've heard that there is. There's lots and lots of battlefield data but that data may not contain useful information about what's there, what it is, and where it's going and where it's come from. And that's really the difficulty in Battlefield information. And there's lots of ways to disrupt that. That's where technology is very useful.

Now, what kind of sensor is there? There are too many to describe, but of course, radar has been one of the most fundamental. It has been since World War II in the Battle of Britain. It was essential. And radar, I think it's one of the most, I think consequential weapons that have been engaged in Nagorno-Karabakh and up through the present war in Ukraine is these weapons that try to attack radars.

Now, those weapons I would actually classify as fully autonomous. Israel produces -- a company in Israel produces weapons, and on their website, they specifically say, "This is an autonomous weapon. And I'll take that by face value in the sense that according to the International Commission of the Red Cross, and the U.S. doctrine, full autonomy means the ability to fly to a place, look for a target, collect data, interpret the data, and then make a logical decision whether that data suggests there's a physical thing to attack. That's called selection. The International Mission of the Red Cross uses that as well as U.S. doctrine.

And that selection process is actually a logical process. It's kind of predetermined. And that creates, just follow that thread a little bit or that dynamic a little bit. The radar is essential as Sam mentioned, their defense radars mentioned importance of their defense radars. Well, these antiradiation weapons are designed to destroy the radars that are essential to the long-range detection and then tracking functions of their defense.

Now, there are counters to those. The dynamics are, you're going to have to imagine because I can't spin out all of the possible dynamics but that's purely in the information and data realm. In addition, there's jamming communications from the commanders, so that I think is the future.

Now, I will finish with I think the future of autonomy is going to be driven largely by the fact that the ability to jam and disrupt data and communications is going to force nations to rely more on fully autonomous. That is not a remote control which Sam explained very well. It's the dominant mode of using and collecting data. It's going to drive countries to use autonomy because they basically won't have the remote control.

And that concludes my comments.

MS. NELSON: That was fantastic, Tom. Thank you. That was really great. Really appreciated, first of all exceedingly modest that you had nothing to add. Overly modest. That was really informative. I appreciated your comments about reducing uncertainty on the battlefield. And the roll that these technologies play relative to infantry. Your comments on ground warfare, to take and hold territory, which will bring us to our first audience question.

So Tom, I'll give this one to you. To win a war, one must take and hold ground, although the technology of unmanned systems is tactically a game changer. Strategically ground must be taken and held. Do you see examples of where automation is enabling the holding of ground taken by boots on the ground?

MR. STEFANIK: I actually don't. And the evidence of that is the relatively static nature, and let's talk about, I'm sure other people on this talk are more expert ground warfare than I am. But you know, there's a discussion that now there's this pause, you know, because of the weather and the mud and they're waiting for freezing and, you know, these are things that we would be talking about from the Civil War era or from the 18th Century that would affect. Now, at the same time, weather, of course, does affect autonomous systems and sensing and all of those things but not nearly in the way that it affects ground worker. So if you just take that one shred of evidence, I would say that the change in territorial control in Eastern Ukraine where that is, is still very much dominated by maneuvering troops, maneuvering heavy equipment, and not driven primarily by new information technology.

MS. NELSON; Great. Thanks, Tom.

A question that came in prior to our webinar today, how have counter unmanned aerial

systems been impacted by the Russia-Ukrainian war? Are seeing more jammers and electronic solutions for air defense or is it the more traditional kinetic solutions? Would anybody in particular like that? Sam, I want to turn to you otherwise.

MR. BENDETT: That's a great question. And I do have to actually log off for actually just a few minutes but, actually, both sides are increasingly using different types of counter-UAS systems and electronic warfare systems. After the initial period of several months, Russia especially got its act together with respect to air defense and EW and has been able to impact to a significant extent some of the Ukrainian drone operations, especially smaller commercial drones which are more susceptible to the EW. Of course, the Ukrainian front is very large, and the complete aerial defense and EW coverage is not coverage and so the Ukrainians have been very successful in exploiting the gaps in such defenses amongst the Russian forces, but Russians are also using EW to a significant extent against Ukrainian capabilities. And this also concerns some of the more tactical handheld counter-UAS rifles that both sides are building and fielding in much greater numbers. So as this war is continuing into the winter, expect to see more electronic warfare, more jamming systems, more counter- UAS systems fielded by both sides.

MS. NELSON: Great, Sam. Thank you.

A question here for Rita. A participant really appreciated what you had to say about using AI at scale. One of the things they worried about is getting the end-users to trust AI battlefield conclusions, noting that experimenting on the battlefield might be the best way to get them to trust AI process data and conclusions. What is your take on this? How would you suggest getting end-users to trust AI other than from battlefield environment direct information?

MS. KONAEV: Human AI teams I think is one of the most important and most interesting questions in this whole space. And there's no -- I don't want to say there's no doubt, but it is certainly important on operational experimentation, it is absolutely significant in building that trust, and not only building it but calibrating, determining what is perhaps too much trust in systems that don't merit or the conditions that don't necessarily allow for it and what is, you know, perhaps not enough trust in functional

and viable systems. There are other solutions, and in fact, the majority of countries that are developing military AI are not experimenting in operational conditions because they are not involved in operational settings because they're not at war. There is an emphasis on training. There's an emphasis on simulations, in particular. At the end of the day there's limits to how much even simulations, and the most realistic ones and the most repeated ones can supplement or replace operational testing. So I think it's inherently inevitable. So the more you can get data experimentation to approximate operational settings, especially given what we know about the vulnerabilities and weaknesses of artificial intelligence and how susceptible it is to changes in circumstances and introduction into unfamiliar environments, so the closest you can get to simulating operational conditions both digitally and physically, I think that's the most important.

The other point here that I think is quite fundamental is that we spend a lot of time trying to understand what it takes to build reliable systems and trustworthy systems and how to make the system, the AI, the recommendations or whatever itself, themselves, dwarf the person's trust, but we pay a lot less attention to human approaches to technology and human inclination than human factors. And I think it's quite vital to understand how those human factors and those human dimensions and everything that surrounds us as people, the organizations wherein the culture we're from, how all of that shapes our approaches to technology, not just the parameters of the technology itself.

MS. NELSON: Thanks, Rita.

A question for Gavin. And Gavin, I want to come back to what I had foreshadowed, your comments on the limits of cyber capabilities in a combined operation. And the question from the audience member is, to what extent is Russia's failure at large-scale operations, an indication that they are less capable than we thought as opposed to widescale information operations just being harder than we thought. For example, convincing people that Zelensky is dead or a fascist may prove quite difficult while he's appearing on the news, even for a sophisticated information apparatus. Are we seeing Russian incompetent or a competent Russian information effort failing at an extremely difficult problem?

And Gavin, I want to get your take on this, and then Jackie, yours as well, please.

MR. WILDE: Yeah, boy, that's a tough question. I don't know that any of those are mutually exclusive. I think both are probably true. I think on one hand a lot of the discussion around Russian -- on the cognitive end, let's start there, I think a lot of the discussion and focus on those over the past few years, certainly since 2016 in the United States, has perhaps risked inadvertently kind of backing us into the corner of accepting as truth the idea that certainly the Kremlin has adopted that given enough technological prowess and resources thrown at it that societies and human beings are simply wieldable and moldable. That's a very kind of -- that idea is rooted in Leninist thought certainly but it's a very materialist view of information that all information is just simply waiting to be wielded and is imminently instrumentizable to achieve a certain end. I think as certainly has been said here, humans are just a little bit more complex than that and so certainly some of the identity politics and a lot of the cultural issues that Russia faces in Ukraine I just don't think they factored for and have certainly backfired on them.

On the technical side, again, I don't mean to downplay their capacity. Like, Russia is certainly one of the most formidable and dangerous cyber adversaries that the United States and the West face. I think where sometimes we overestimate the ability to just turn that fire at will. Complex cyberoperations are very difficult. They demand a lot of time, a lot of expertise, and a lot of luck. And that's doable over the long term as you kind of try to degrade, as the Kremlin has, degrade a society's ability to function or a government's ability to do its job but it's tough to do that in a sustained fashion, and it is certainly very difficult to compress down into the timelines that a combined arms campaign demands. And so I think a lot of it has to do with the conditions under which Russia is trying to execute these campaigns. They are just running into a lot more friction and I think both we and then need to do a lot more thinking about, as Rita says, the frictions and the complexities inherent in those types of operations. But Jackie is certainly far better suited than I to speak on a number of those.

MS. NELSON: Terrific, Gavin. Thank you.

Jackie, will you close us out here, please?

MS. KERR: Sure. While I agree with everything Gavin just said and I'll add to it, with the approach to information warfare Russia has taken there has been a lot of mythmaking in D.C. in recent

years I think it's fair to say. I had worked on Russian domestic use of information manipulation against dissidents and activists, civil society, and got into working on the international cyborg information conflict around the time some of this was starting to become a central topic of conversation in D.C. And one of the things that was striking to me was things that I'd seen that were very experimental and had a dynamic of throwing things against the wall and seeing what stuck. And there were failed attempts, unsuccessful attempts. In D.C., the rhetoric turned very quickly to this is the very laser capable surgic ability they have. And I always was a tad skeptical of that narrative because there's a difference. It goes back to a comment Rita made about the difference between experimentation and innovation versus scalability and being able to do something deployed at scale and joint operations. And I think with the information ops there's that piece in terms of just even on the level of organizational maturity, question mark. But beyond that just the tools themselves.

And then there's the question of whether they were ever that effective even when they seemed to succeed. We know about the successes because they spilled out into the open because we became aware of them which for some forms of covert ops would be a spelling of disaster, a sign something hasn't succeeded that effectively. And we were always better at demonstrating what they had done than at demonstrating effect and impact. There's been various efforts at research to understand the impact of various Russian information campaigns from election meddling to efforts in Ukraine and so on. But it's hard. It's a hard problem to actually measure impact.

And here we see this point about does this sort of cognitive stuff actually work? Does it work at the level? We've been quick to point out our own difficulties with achieving the kinds of success even at debunking misinformation when it's important for our own security or health. But we're less quick to point out in these narratives some of the problems with the Russian approach.

And another thing that I think is interesting which speaks to something Gavin said at the end of his comments is the offense-defense balance. So there's been a lot of discussion in cyber and information about the superiority of offense over defense. And in fact, this was used as a justification for strategic shifts in the West because the space that can be conquered is so broad. We can't defend it all.

We need to do something to counteract that. And yet, the preparation for complex operations, whether it's information ops or cyber ops, particularly cyber ops that require really understanding infrastructure and using things like zero-day vulnerabilities, this takes a long time and a lot of expertise to prepare.

So I think during war you need really quick operational tempo and what we've seen with some things like critical infrastructure targeting is just maybe more effective to target things kinetically on the battlefield when it's in real time. And it raises questions long-term about how we think about the offense-defense balance going forward with both of these types of operations.

I'll end there.

MS. NELSON: Fantastic, Jackie. That's a wonderful note to end on because it's incredibly thought provoking. I want to thank all of you. Sam, unfortunately, had to step out of the room but I want to thank all of you for your thoughtful comments here today. I certainly learned a great deal. I hope our audience members did, too. Thank you, everyone, for spending the last hour and a bit with us. Over.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2024