THE BROOKINGS INSTITUTION

WEBINAR

TECHNOLOGY AND THE SECURITY OF DEMOCRATIC SOCIETIES

Washington, D.C.

Monday, September 12, 2022

PARTICIPANTS:

Session I: How to Win an Information Competition: Understanding a Changing Landscape and What to Do About It

JESSICA BRANDT, Moderator
Fellow and Policy Director, Artificial
Intelligence and Emerging Technology Initiative
The Brookings Institution

PAUL ASH
Prime Minister's Special Representative on Cyber
and Digital Christchurch Call and Cyber Coordinator
Government of New Zealand

OLGA BELOGOLOVA
Adjunct Assistant Professor, Center for Security Studies (CSS)
Georgetown University

RENÉE DiRESTA
Research Manager
Stanford Internet Observatory

AUSTIN WANG
Assistant Professor, Political Science
University of Nevada, Las Vegas

Session II: Advanced Military Technologies in the U.S.-China Competition: How Advanced are They Really, and How Much Do they Really Matter?

MELANIE SISSON, Moderator
Fellow, Strobe Talbott Center for Security, Strategy, and Technology
The Brookings Institution

TOM STEFANIK
Visiting Fellow, Strobe Talbott Center for Security, Strategy, and Technology
The Brookings Institution

PARTICIPANTS (CONT'D):

CAITLIN TALMADGE
Nonresident Senior Fellow, Strobe Talbott Center for Security, Strategy, and Technology, The Brookings Institution
Associate Professor of Security Studies, Georgetown University

Session III: Democracy Under Threat: Countering Digital Authoritarianism and Malicious Actors

CHRIS MESEROLE, Moderator
Fellow and Director of Research,
Artificial Intelligence and Emerging Technology Initiative,
The Brookings Institution

SARAH KREPS
Nonresident Senior Fellow, Artificial Intelligence and Emerging Technology Initiative
The Brookings Institution

DAHLIA PETERSON
Research Analyst, Center for Security and Emerging Technology
Georgetown University

ISHAN SHARMA
Fellow and Advisor, Strategic Initiatives
Federation of American Scientists

* * * * *

P R O C E E D I N G S

MS. BRANDT: Hi, everybody. Welcome. Thanks so much for joining us today for the symposium on Technology and the Security of Democratic Societies. This is the third in the year-long series which I think, as many of you know, is part of our Global Forum on Democracy and Technology, which is the institution's signature effort to foster greater policy alignment on core technology policies among the United States and its democratic partners and allies.

We have multiple workstreams as part of this work. It's looking at issues from, you know, surveillance to cybersecurity among many, many others and today we have three panels that are focused on a variety of topics, including state-backed information manipulation, advanced military technologies and digital authoritarianism and malicious actors.

We are going to get started in a moment with our first discussion which is on How to win an information competition: Understanding a changing landscape and what we can do about it. And so I am going to welcome our panelists to the conversation.

I'm really delighted that we have four experts joining us today representing perspectives of government, platforms, researchers, with a variety of different sets of expertise and focus. Paul Ash is the New Zealand Prime Minister's Special Representative on Cyber and Digital and he leads at the Christchurch Call and Cyber Coordinator. Olga Belogolova leads policy for countering influence operations at Facebook, where she coordinates the companies IO disruption effort and she's, of course, also an Adjunct Professor at the Center for Security Studies at Georgetown University. Renee DiResta is the Research Manager at the Stanford Internet Observatory where she investigates the spread of maligned narratives across social networks at the behest of the Senate. Renee led an investigation into the Russian IRAs multi-year effort to manipulate American society. And we also have Austin Wang who is an Assistant Professor of Political Science at UNLV in Las Vegas who is an expert on China's information manipulation activities focusing on

Taiwan.

So, I'm going to kick off the conversation with some questions to the group in a second, but we really want this to be as interactive as possible, so I hope that you'll submit questions. You can do by emailing events@brookings.edu now or whenever the spirit strikes you.

I'm going to start by kicking a question to Renee. You know, you've tracked this for a long time and I'm curious like how are you, from your perspective, seeing authoritarian governments evolve their influence operations in response to recent developments, shifts in politics, government, and industry mitigation efforts and then, of course, technological change?

MS. DiRESTA: Yeah, thank you for having me. It's such a great and important question. I think first it's important that we not thing of influence operations as solely or even primarily a covert action on social media phenomenon. Authoritarian governments have often had well-resourced vast propaganda apparatuses at their disposal built up over decades targeting both their own citizens as well as citizens of foreign publics. Social media has been additive. It's been particularly useful for targeting citizens of foreign publics and I'll go into a little bit on how. But the, we have to be thinking about these operations across the entirety of the broadcast to social spectrum and the overt to covert spectrum. That's how we -- that's the framework that we use at Stanford. So, as far as what has changed, you know, there was a conceptualization beginning in around 2018 Facebook's terminologies coordinated inauthentic behavior and there was a formulation around that where the kind of inauthenticity was what was emphasized. The idea that the accounts were fake. Over the last four years or so, it's not quite that cut and dry anymore. What we're seeing is something of what you might call a regulatory arbitrage dynamic in which adversaries adapt to policy changes and enforcement actions undertaken by platforms in that covert social space by leveraging non-social channels, like the broadcast media at their disposal, as well as by updating their social strategies to roll to less moderated platforms. There are two updates I'll

point to in the context of Russia specifically. The first is what I just alluded to, rolling to less-strict platforms. Facebook and Twitter and most of the major Western social platforms have arrived at a point where they will actively seek out and disrupt the covert social networks. There are other platforms, however, like Telegram that will not do that. Moreover, not only will they not disrupt the networks, they will not make the effort to see if the network is there. So, we see a lot of channels on Telegram that are ideologically aligned with the propaganda of the Russian government, particularly in the context of the Russia-Ukraine war, but it is very hard as outside observers to say that is a Russian state-influenced operation, right? Because we don't have that collaborative working relationship different entities are trying to sort out who is behind what channel. In addition to this kind of regulatory arbitrage response, the other thing that we've been seeing is actually kind of a rollback to some of the old strategies of propaganda, which is a very kind of quaint, you know, using money, using money and existing influencers to influence the public. And so we started to see indicating that that was happening in the context of Covid. We saw Russia-lined entities appear to engage in outreach to academics, to journalists, to influencers, trying to get them to produce content boosting the Sputnik vaccine and attacking AstraZeneca vaccine. In the context of Ukraine, we see again Telegram channels, who knows who they are attributed to, asking influences to make certain types of, you know, pro-Z, pro-Zed (phonetic) content for TikTok in particular. And, again, this is a very, very old tactic, you know, front media, useful idiots, fellow travelers, agents of influence, there's a whole vast array of rich historical terminologies around that spectrum of participation types. So, in closing I will just say that, you know, the activity that led to the definition of CIB in 2018, the kind of demonstrably false accounts, the bots, the very demonstrably obvious coordinated behavior, seems to have waned a bit, and now what that means is that investigations require a fair bit of extra legwork and collaboration in public-private partnerships to confirm that the actions being taken can reasonably be attributed to a malign actor.

MS. BRANDT: That's great, Renee. Thank you so much. Austin, I'm curious how

this looks from your perspective. I mean, Renee has sort of described this shift away from like large volumes of troll farm content towards using influencers and moving to darker corners of the Web and I'm curious, you know, as you track Chinese influence operations in Taiwan, you know, what are you seeing? Are you seeing similar trends, different ones? I'd love to know your thoughts.

MR. WANG: Yes. Thank you for having me. So, basically my observation is very close as to Renee's observation on Russia. So, recently I can see two important social media strategies that is adopted by China. I think the first is about localization and the second is about algorithm. So, on localization now China can now produce or try to produce the content that close to the culture of the target audience. So, during the Winter Olympics we noticed that China tried to recruit several influencers in the U.S., either TikTok or Instagram, to promote a toxic image of the Winter Olympics and in the past, during the pandemic, we see many fake Chinese Twitter accounts that spread a video which made by the Lego movie to try to spread information that China -- spread misinformation that the virus is originating from the United States. And also on Facebook we can observe there are many Facebook page attackers the Taiwanese (inaudible) and this Facebook page where their managers were located in Macau or in Hong Kong. So, in the past few years, this page only published their content in simplified Chinese. But nowadays their content are all written in traditional Chinese. So, I think it's a big change compared to the past. And the second is about the algorithm. So, a recent study I think conducted by the Stanford University shows that 40 per cent of the trending video (inaudible) is actually published by the Chinese government's deleted account. So, in other words, the Chinese government know deeply what kind of videos can be trendy. And also during the Winter Olympics we found a very interesting phenomena. We did not see a very clear evidence that there are any influencers in the U.S. were actually being recruited by Chinese government. But we also found the phenomenon that there are several college students in the U.S. Whenever they publish anything about the Winter Olympics, then they receive a very huge view count. For

example, what we found there are several college students that post their ten cent (phonetic) and only receive 20 view counts. But when they upload the opening ceremony of the Winter Olympics then that video received one million view counts, which is very different from what they could receive in the past. So, you can imagine that if you're a college student or you are a junior student and you want to be an influencer in the future, then you will observe such a phenomenon then this kind of indirect strategy will deeply influence what kind of content you are going to upload in the future. And so I think these two interesting strategies, one on localization and one on algorithms, is something we should keep an eye on in the future.

MS. BRANDT: Thanks, Austin. Olga, you have the difficult job of actually trying to counter some of these operations and I'm curious like what do the threat trends look like from your perspective?

MS. BELOGOLOVA: Thank you so much for having me and I would say that from, you know, what we see on the platform side it's not too dissimilar from what, you know, the research community sees. But one distinction that I would make is, you know, we're talking about different government-run or potentially government-run operations, and I would probably sort of separate them into two different categories. Some are sort of new threat actors that are entering the space, domestic-run operations across a number of different countries around the world, and then the more sophisticated threat actors that a lot of us are talking about that we've been tracking for some time. So as part of that distinction we've certainly seen a lot of attempts to return to the platform by the threat actors we've been tracking for some time, including Russian and Chinese threat actors, but then we've also seen, you know, some of the same techniques, early techniques, that we'd seen from them being utilized by government actors from other countries. So, for example, in 2021 alone we took down government-lined CIB networks from Nicaragua, Ethiopia, Uganda, Sudan, Thailand, Azerbaijan and they were using some of these, you know, complex cross-platform troll operation techniques that we'd historically seen from these broader-threat actors

engaging in foreign operations focus largely on their own domestic audiences. But on the other hand, you know, we have seen, you know, the threat actors that we all, you know, know and have tracked for some time now, including Russian and Chinese threat actors, Iranian threat actors, shift and adapt. As Renee described, we've seen a lot of similar adaptation techniques to our enforcement actions. Sometimes that includes, you know, ways that make, you know, their easier venues of attack. Maybe we've made it a little bit more difficult for them to get through when they're trying to sort of create large-scale fake accounts. So, I would say in basically four main areas we've seen a shift and adaptation of threat actor techniques.

One is in the shift from the sort of wholesale large-scale operations as you were describing, Jessica, to more narrow and targeted campaigns. An example of that is in May 2019 we removed an Iranian network that was a very small number of accounts but they were posing as journalists and other fictitious personas but they took a little bit more time to develop and they were trying to reach out to people to get them to amplify their content, rather than some of these broader broadcast operations that we'd seen from Iranian operators before where they were sort of going wholesale trying to reach as many people as possible. They were sort of adapting so that they wouldn't get caught, we expect, and they were trying to reach directly to a particular set of audiences, to policy makers, reporters, academics, dissidents, and others.

Another trend that we've seen is a shift to higher operational security, which is sort of expected. When we're trying to take down these networks, we've improved our detection techniques, so have our colleagues across industry, and the civil society, investigators and researchers that are looking for these operations, we're all sort of working and constantly tracking and trying to identify them. And so, they're trying to do a better job, especially the more sophisticated actors like Russian and Chinese threat actors, to show a little bit more discipline. We're not going to see them coming out of St. Petersburg and posing as Americans, right? But those things, the days of those types of operations are long gone,

but, you know, they periodically do slip up and make some mistakes, like that cyber front C network that we spoke about at our last report where, you know, they periodically will be just as sloppy, or they will sort of repeat the same kind of techniques we've seen before. We've also seen, you know, they're becoming a little bit better at avoiding the language discrepancies that make these operations a little bit easier to identify and sometimes, you know, appropriating authentic content rather than creating their own.

And that's where sort of another trend that we've seen comes into the picture, which is the use of authentic voices and authentic communities. Now, we've always seen a bit of that from some of these threat actors. I'm sure Renee and I can recall days of the Internet Research Agency (inaudible) communities, you know, to try to amplify their campaigns, but we've seen a lot more of that. The shift to sort of more overt networks, more overt influence techniques, that's something that I know Renee had just mentioned. You know, we're seeing more, some of these threat actors more involved in the state-controlled media and overt government channel space because we've put the pressure on them in the covert space.

And then finally another trend that we've seen is shift to use of cross-platform. This is again something that I think all of us have mentioned here, which is, you know, we see these threat actors running operations all across various platforms down to sometimes the Secondary Infection Operation, for example, was across multiple forums online. Sometimes they're using petitions, off platform websites, and then, of course, different social medial channels that may or may not be investigating and disrupting their operations and, you know, for example one of the Nicaragua networks that we took down that was a government-run Nicaraguan troll farm we took down about a year ago, that one was across a number of different platforms, including Telegram, including Facebook, Twitter, Blog Spot, You Tube and so many different types of platforms, some of them that, you know, don't even come to mind very often. So, that's another technique that we've seen. And I'll stop there. Happy to dive into further detail.

MS. BRANDT: Really helpful, Olga. Thanks. Paul, we are so grateful that you're joining us at 5:45 in the morning your time. Truly we are. And I'm curious, like, you know, given this threat landscape that our colleagues have laid out, what do you see as the sort of most worthwhile opportunities for Democratic governments, your own, but also maybe others, to disrupt these kinds of operations and if you can give us some lessons. Like where has this worked? And sort of what should we, what takeaways should we draw from recent experience?

MR. ASH: Thanks, Jessica. And thanks for the insights from other panelists. It's great to be here with you today. I guess the starting point for government information operations, and I've seen it all. I've been around since city states and nation states developed and I've probably seen three major transitions throughout that period. First the rise of written language and the ability to transmit. Second, the democratization of print and then it was followed not too far after by the 30 Years War which is probably a subject relating to us all. And last, the development of the internet and large-scale online platforms with an algorithmically driven content, and then a point that I think we've heard well-described this morning, the fracturing of some of that through use of small platforms, regulatory arbitraged to locate their content. That's really changing the game for us at the moment, that transboundary nature of the problem and the ability to detect previous transmission of material across borders and really push that into new environments, is causing us some real challenges. So, I think that's the first thing for governments to acknowledge, that we're actually in a new environment where old wine is in a new bottle, if I can put it that way. And that is causing us some real issues. I think Renee's point is absolutely on the money, and I'll come back to money, because I think that's a key part of this. We have to be thinking about right away across the spectrum, a spectrum of demand and supply side, of actors, of tools that they're using. From a government standpoint, you know, one of the great challenges for Democratic societies is managing the challenge of responding to this without actually causing ourselves harm. And probably about five years ago, maybe a little longer now,

actually, I started to hear some of my colleagues who were a bit longer in the tooth than me that had been in this business for a bit longer, talking about old Soviet doctrines of reflexive control and I started thinking a bit more about that, and I think, you know, that really is in our sites at the moment. How do we avoid responding to this problem in intemperate ways or ways that actually cause just as much damage as perhaps the information itself? That's the conundrum most governments are grappling with right now. I think it's a conundrum also that the private sector and civil society are grappling with in terms of building solutions that are truly multi-stakeholder and I'll come back to that. For governments, I think one of the first problems here is conceptual, and it might actually, we found it increasingly useful to think about information operations in some similar ways to other problems we grapple with and the first of those is cyber security. I think we're starting to see some significant conceptual similarities between the way information operations are used and the way malware has been used. One is operating on people's thinking and behaviors and the other on software and hardware and they are designed to have a similar effect of either destabilizing or taking down parts of the critical infrastructure of a state, they see the Democratic institutions as critical infrastructure, which we do.

The second, based on that, I think some of the analytical tools we use for cybersecurity, greater information sharing, sharing of information about indicators of compromise in the cyber world, I think, has parallels in the information operations world, but if we can find ways to surface this content in a more, these indicators in a more consistent way, will probably serve us all well.

I think similarly some of the tools we are having to grapple with to deal with terrorists and violent extremist content online also have significant overlap. We see some strong similarities of the way adversarial behavior works and in the use of small platforms with some of them described to import information back into mainstream platforms, and we see significant overlap, perhaps not at the apex of the transmission chains but certainly partway down where there is an overlap from (inaudible) between the groups that are often used by

states that are driving information operations and particularly the violent extremists and sometimes terrorist parts of the (inaudible) landscape.

How do we think about disruption? I guess there's a few elements in here that we certainly think about, the first being understanding the problem and being able to attribute by surfacing and understanding the networks that are operating and bringing some sunlight to bear on that. So, if we think about the supply side of the problem, in particular surfacing the transmission chains, and there are some real challenges in that, as we've heard those chains have become much more diffuse, as Renee put it, the range vectors from Useful Idiots through to the folks that are monetizing the content with profiting from it, and sometimes the two are the same, actually makes this much, much more difficult to map, but is probably quite important to be doing, and often that's a process that's not best led by governments but can be best led by society and/or industry.

The second piece in there, I think, is actually the challenge of understanding just how those transmission systems are being exploited. Are they direct and we've seen, certainly seen direct targeting, of a specific instance or piece of information, but we see a much more diffuse approach now, flooding the zone, I think a prominent U.S. citizen described it as a few years back, in the hope that people will pick that up and put for them through our societies. I think one of the biggest issues in here for us is understanding how algorithmic systems work and how they, and I think Austin highlighted that, I think we've all picked up on this, my sense is that some of the threat actors involved actually understand us far better than a number of the governments that are having to respond to it, and that one of the real challenges is looking at the way content proliferates, why user journeys occur and in particular bringing that cross-platform question that Olga was describing earlier to bear on this problem. How is it that material is, or the algorithmic (inaudible) are exploited to shift that material from one platform to another for a user?

Certainly, underneath that I think there's also a key question around monetization. How is this, how are people profiting from this because there is certainly no doubt that a

number of areas around information operations, there are significant profits to be made, and I think being able to work more closely on understanding that will perhaps help to break some of those chains of transmission.

And I guess the last piece for governments is understanding and predicting future trends. Just from listening to the conversation today, the reshaping in the last two to three months, a phenomenon we've seen in cyber security as well. Once the tools are out, they become cheaper to use, the cost of taking it to market and the barriers to entry for smaller actors become much fewer and the key for governments and for companies is thinking about ways to lift those barriers to entry and make the cost of information threat actors much higher.

I guess that leads me to a couple of places. That will require deep multi-state (inaudible) engagement and I think there's some things we're learning in, for instance, the Christchurch Call work around just how important that engagement was. Researchers, academics, civil society, companies, and governments is. And about the challenges of making it a safe process for everybody. It's not simple. It's messy. But it's actually probably far more robust than either expecting companies to do all the lifting themselves, expecting because fundamentally their platforms are being exploited too, expecting governments to do that because, not to mention they don't have all the tools they need to do it. We need to find some of those new tools to be able to do that. So that civil society and academia which has come up with some pretty extraordinary insights of on-the-ground impacts, can contribute, so that companies which have the big data sense, and the best insights, can, and so governments can work with them on protecting the institutions.

The last piece I'd say here (inaudible) is research access to data. I want to find safe ways for researchers to work with platforms that work within circles of trust. It's becoming a really crucial pinch point and one where we need to find some smart ways to win that challenge. That's going to take I think sitting down around a table in the multi-stakeholder way and mapping out some of the issues. To be clear, you know, from a government

perspective, we don't see a need to be (inaudible) people's source code, that's not relevant from where we stand. But we do need to understand the outcomes of the algorithmic crisis that that code drives, and to think about ways to make that safer. There's a whole pike of disruption work on the demand side too that I won't go into detail, but indication, making, giving users more control and making them more resilient, but I suspect those are longer run solutions than the ones we're going to need and if we rely entirely on those, we will find that the impacts of information operations have been so significant that we struggle to (inaudible). I'll stop there. But hopefully they consist of a starting point for the discussion.

MS. BRANDT: Thanks so much, Paul. You've laid out a number of things here about sort of finding the appropriate role for government and for civil society actors and the need for multi-stakeholder engagement that I think is really kind of top of the agenda. And I know is, you know, we got a bunch of questions ahead of time from some listeners and viewers and I know it's on people's minds is this question of sort of how do you balance a response that's coherent and effective but also, you know, supportive of Democratic values and, you know, where we're not sort of doing more harm to ourselves over the long run than we are to our adversaries, so I really appreciate you raising that point. Olga, but what are the most worthwhile opportunities for industry in terms of disruption?

MS. BELOGOLOVA: Yeah, I think, you know, Paul really hit the nail on the head in terms of talking about the whole society response and the multi-stakeholder approach that is necessary here. And the other thing that Paul mentioned was how long these types of operations have been in existence and so one of the ways that we can see this problem is that we know that these types of operations have existed, you know, in multiple mediums and over many, many decades, centuries, who knows how long. And so, the best thing that we can do as industry is think about deterrents, right? We're not going to stop these things from happening but we're going to try to deter threat actors from engaging in these activities in the first place. And one of the sort of most common things that everybody thinks about that we talk about all the time is disruption, right? Removal of these networks and take

downs and things like that. And that's sort of the most popular topic, but I also want to spend a little bit of time talking about ways that we can deter threat actors that go beyond just taking things down. Certainly, that's important. And on the taking things down piece is sort of a combination of techniques that we try to use and some of our industry partners are doing the same. That includes sort of combination of having expert investigative teams that are designed to look for these types of operations, that are tracking particular threat actors, and building that knowledge into our further detection system. So, taking what they've learned, the tactics and techniques that they see from these threat actors and trying to build them back into our automated detection systems so that we can find more of those types of operations before they become an operation. And you'll probably notice in some of our findings over the years that we do try to say that which portion of the network that we've removed was actually identified by fake account detection, for example, before it became an operation. That's really nice to see when the enforcement systems that are in place are actually catching some of these operations before they've had a chance to build a more well-developed persona and actually, you know, as we discussed earlier, increase the cost for the threat actor to have to work a little bit harder to not get caught. But beyond disruption and automated detection there's a lot of other avenues that we consider sort of part of our deterrent's toolbox. One of them is also banning organizations. When we find that an organization is designed to engage in this kind of manipulative activity, we will ban it. And that means that anytime they attempt to come back as an entire organization, whether they are engaging in inauthentic activities or not, they are banned because they were designed to do this kind of harmful activity on our platform, so it's just another tool in our toolbox.

The other area is product-driven intervention. One of the things my team likes to talk about is, you know, using military terminology, but, you know, on the battlefield it's useful to control the terrain, and we have the opportunity in some ways to control that terrain. And that means changing the way in which the product functions when we see that someone is exploiting a particular piece of it to run these type of operations. We're making it

more expensive for the threat actors to do it and making it easier hopefully for the research community to (inaudible). Things like that include, you know, information in the page transparency tools so people can see where individuals are coming from but then another thing, another program that my team leads in countering influence operations is in the overt influence space. And that's our work in state-controlled media. Some of the things you might have seen around our work related to Russian state-controlled media following the start of Russia's second invasion of Ukraine was our work to not only label the state media outlets themselves but also warn users when they're attempting to share links to those domains so that they know where they're sharing their information from and sort of building a little bit more friction into that process so that it becomes more, so people become more thoughtful not only about what information they are consuming but what information they're sharing as well and where it's coming from. So that's just an example of a couple different product-driven interventions and the way we sort of think about this idea of adversarial design, which is building back what we learned into our systems, trying to red team what we expect threat actors to do ahead of a particular civic event or in a particular region of the world.

And then finally, you know, getting back to the whole society piece, disclosure, notification, sharing, you know, a lot of the public announcements that we do around these operations are not just public announcements to share the work that we've done but they're really part of a deterrent strategy which is exposing these operations, sharing what we know about them, sharing them with the research community so people can better understand how these operations are run, and imposing, you know, another type of cost on the threat actor where they are being sort of named and shamed and exposed out there. And we found that of course sharing information with our industry partners and our partners in civil society and research community really helps us connect the dots. You know, if you take a look at some of the reporting we credit journalists, researchers from academic institutions, but also from civil society groups, who often tip us off to some of these activities and we do

the same in response. And the same with governments, where we can hopefully share information that can lead to further action. An example I mentioned early was the Nicaraguan troll farm and then after you know our enforcement action, we did see the Treasury Department in the United States you know put out sanctions (inaudible). We've seen the same related to some of Pregosian's (phonetic)properties in Francophone, Africa and that exposure sort of hand-in-hand governments and platforms doing what they can respectively do based on the information that we see.

MS. BRANDT: That's great. Thank you so much. I want to encourage our audience to continue to submit live questions. Again that email is events@brookings.edu and if you send them in, they'll somehow magically make their way to me live and we will inform our discussion. So please feel free to send in your thoughts and questions.

You know, I want to ask each of you actually just to sort of look ahead and from your perspective, like what are the key drivers that we all should be watching? I know, Paul, that you're going to have to leave us at 2:15 and so let me give you the opportunity to go first.

MR. ASH: Thanks, Jess. I'm sorry I've got to drop off. I have to go into a Christchurch call steering group. So, you know, I think Olga's actually highlighted one of the key things that we're seeing here in New Zealand and that is just a huge proliferation on informational crisis that has risen over the past probably two years here. We were probably a little bit behind the curve in terms of volume of material that we were seeing in New Zealand out of those operations, but with Covid-19 in particular we saw a real lift in those, and we've seen a subsequent lift coinciding with really the lead-up to and the development of Russia's assault on the Ukraine. And that's been quite interesting to us. We've seen that in our international environment and a number of domestic researchers have been pointing to it. It was really interesting to see the results of the initial survey that Microsoft released back in June on consumption of Russian material in New Zealand and mapping some of that and again I think that pointed for us to the value of working closely between research, industry, and government on some of these issues because it gave signal from the noise, if I

could put it that way, that was really important. That consumption material out of Russia both in New Zealand and elsewhere is something that we've been quite concerned about when we've seen it mentioned that way and, you know, I think it's probably the sharpest trend that we're watching at the moment of material being pumped into an environment in a way that might be different from what we expected previously. It's actually more about that diffuse flooding design and seeing what sticks through their diffuse channels that Renee was describing. And that is helping to inform much better thinking about this. I think you all can see from us a consistent response that focuses on multi-state coder solutions. This is a whole of society problem and if I think about the linkages with industry, actually it's a serious enough problem not just in New Zealand but we saw with some of the activities at the beginning of this year coincidentally at around the same time as the Russian build-up was occurring. If we look at what's happened in some of the more, previously more resilient Democratic societies we can see, I think, quite a significant amount of material flooding into places like New Zealand and other vibrant democracies that have tended to sit at the top of the democracies index. You know, that is now well-observed by our partners across academia and research, it's well-observed by our governments and we have a very, very common shared interest. Fundamentally, we can't grapple with this well in our societies. The very companies that depend on liberal democracies for their existence are going to struggle to operate in them because those democracies will also be struggling. Similarly, academics and researchers the ability to do open research really depends on open tolerant societies. And that's where this challenge of (inaudible) across the democracies and the organizations in them is going to be critically important which is what this practice looks like. If anyone tries to do this on their own, I think we're really going to struggle, and I don't think that being big or small actually is the determinant in that. We've seen large democracies affected by this problem, we've seen small ones. It's actually about the quality of working together and trying to see what works best, knowing we'll make some mistakes along the way, but that we're facing the challenge of quite extraordinary proportions. And it certainly

for us here we've seen that, to your question, Jess, really (inaudible) to view in the past year or two in a way we hadn't previously. It's the first time, for instance, we are seeing an Embassy in New Zealand pushing out quite extraordinary material into the New Zealand information environment in ways that have attracted a significant amount of public push-back and concern and, you know, our partners have seen that over many, many years. I recall that (inaudible) posters on the London Underground a few years back and on the Washington, D.C. metro I think quite, what's the word, flagrantly pushing back on some of the stuff, very clever ad campaigns, actually, to realize the point about the full spectrum, but, you know, it's the first time we've really begun to experience that in earnest and we're having to respond.

MS. BRANDT: Well, thank you, especially for the several multi-stakeholder efforts that you're leading. It's really important work and we're grateful for that. So, we will let you go to it. But thank you again for joining us and sharing these insights and being part of our conversation for as long as you were able today.

Renee, I mean I would ask you the same question, like, sort of, forecasting out into the future, what are the key, what are the drivers that you sort of tracking in your work?

MS. DiRESTA: So, we are also looking at ways to facilitate multi-stakeholder partnerships. I think, I mean right now, SIO studies use and abuse of current information technology fairly broadly, oftentimes that is, you know, state-sponsored influence and for a very long time we were focused primarily overseas. Most of our election integrity work focused on non-U.S. elections. In 2020 that began to change, you know. We did do some work trying to understand what does, what is, what is domestic influence, or I should say, what are influence operations targeting an American election looks like. And we began the project thinking we would see much more from state-sponsored actors, actually thinking we would see much more from Russia and China and Iran. And that content was present, you know. We put a massive report our EIpartnership.net that's called The Long Fuse, but what we started to see was really this very domestic political propaganda that was driving

narratives and I know sometimes there was an authentic amplification but really it seemed pretty, you know, just sort of that the disinformation campaign cycle had shifted to what we might call coordinated very authentic behavior, and that was an interesting, I think an interesting dynamic and something that we continued to try to think through and it what does it mean when these lines are not so bright anymore, when inauthenticity does not only refer to clusters of fake accounts, again, or even paid influencers, but really ideological alignment.

How do we think about just the lines between political opinion formation, political consensus formation, non-political consensus formation in the context of something like Covid, you know, how do we think about this dynamic and, you know, we've moved to thinking a lot about propaganda and rumors? You know, how do rumors spread? Do we think about rumors as a conceptualization, unofficial information moving through society at a time of great uncertainty? What does that dynamic look like? If you have a system in which ordinary people are participating, you know, want to participate, are exercising their freedom of expression, is there things that we want to preserve? This is supposed to be the value of social media, in fact, that citizen participation. How do we balance that with the sort of small numbers of users that might be trying to create kind of a you know constant outraged dynamics or use very demonstrably false and misleading claims but once they're picked up by real communities they spread across the Internet and the question becomes, you know, where does counter-speech work, where does labeling work, what kind of interventions matter, and then also this remaining question of are there state-sponsored actors that are playing around the edges? So, we think about the spaces being, I would say, fairly dramatically broadened at this point and in response to that we have felt that one of the best solutions is the kind of platform academic partnerships, civil society incorporated into the partnerships, sometimes governments incorporated into the partnerships. Again, this question of how can we have all of the different folks we're looking at certain manifestations of the problem, you know, governments primarily in the U.S. focusing on foreign state actors, not American domestic participation. How do we think about where that collection of signals

can come into play to help us understand the information environment for particular high stakes areas like elections or pandemics? And that's been where a lot of our thinking going forward has been focused.

MS. BRANDT: That's great. I love that phrase 'coordinated very authentic behavior' and you're sort of, your answer went right where I was about to probe you, which is like, what does it mean for the policy response when the picture is, you know, quite murky and I think you laid out a number of sort of useful interventions that focus on like transparency and sort of coordination between different sectors. Austin, same question to you.

MR. YANG: Yeah, okay. So, in my perspective I think right here I can share one more case study as well as one policy suggestion. So, regarding the case study, I will share a case that I have found during the Winter Olympics. So, during the Winter Olympics, I identified about ten interesting TikTok channels. Thought, oh, these ten TikTok channels were established exactly eight months before the beginning of the Winter Olympics. And these ten channels were all established by Chinese, and they all speak very fluent English, and they are offering to sell some authentic information stories about Chinese. So, this China introduced what is real China, the real force of China, things like that. And so in the past eight months they all introduced something like the history, the culture, the food about China. But on the first day of the Winter Olympics, these ten channels suddenly start to promote all passive image about the Winter Olympics. So, I think, remember it's quite interesting because they set up these channels for at least eight months and they created a lot of original content, so they received one to three million followers before the Winter Olympics. But on the day of the Winter Olympics they started to spread everything about Winter Olympics which is the content is totally different from what they have shared in the past eight months. And after the end of the Winter Olympics these channels go back to their original content. And so I think this co-direct (phonetic) behavior is quite interesting as a very kind of long-term operation (inaudible) information they want to share or they want to control.

And the second is about suggestion. So, my policy on suggestion is that I had recommend we need more transparency on a few accounts and followers and especially donations on this social media. Because we know nowadays these real accounts and followers serve as an indicator of legitimacy and popularity. However, this number can be easily manipulated by the foreign country. And so there are many cases in Taiwan that there is a YouTuber, [Tik]Toker that upload a video and suddenly receive a huge amount of view count, but they are not sure who really watch their video, but they are encouraged to promote, to upload something similar because they know it is something that they can receive more view count. So, you can imagine that if we can be more transparent on who watch their video or who create, who follow them, it could be better for us to understand that whether this information or whether this view count were manipulated other country. So, we know that a Facebook that already show the locations of their page manager. I think it is a good start. So, I believe that a You Tube, Instagram and TikTok should also reveal the location of the view counts or the followers, and, if possible, the donation. Donation is another big issue that can encourage this TikTok or influencer to go to a specific direction. And so I believe that since the Facebook revealed he location of page manager and it's totally legal I believe that other social media platforms should also do like that, at least for the influencer. For example, if your video received more than ten thousand view count, then it will reveal the location of this view count. I think it could be a good way to help general audience to understand whether this video was manipulated by other countries or not.

MS. BRANDT: Thanks. We are moments away from your own sort of thoughts and questions and I've gotten a bunch, so thanks so much for sending those in. Please keep doing so at events@brookings.edu. Olga, let me let you take one last crack at the same question.

MS. BELOGOLOVA: Thank you. Yeah, and I think I'm going to echo a lot of what Renee was saying which is, I think, we've spent a lot of time in our team thinking about that shift to the authentic space and what does that mean. You know, and all of those same

difficult questions around what that means for speech. But also how are we seeing threat actors continuing to and expanding their use of authentic amplifiers and, as Renee mentioned, sometimes that includes, you know, paid influencers, but sometimes that includes, you know, unwitting individuals who sort of become amplifiers for these types of campaigns and how do we think about not only whether they're being used by foreign threat actors but whether, you know, some of those, you know, communities are authentic and where do we draw the lines? And so some of the policy development and thinking that we've been doing is in what we call the emerging harms space, which is how do we, you know, think of new problems that we're starting to encounter? And how do we address these? I don't know if we would ever, the acronym for coordinated very authentic behavior may not be roll off the tongue but we do have other policies that we've shared information around where, for example, about a year ago we took a network down in Germany that was linked to Kardangen (phonetic) and there are some other, you know, groups like that where we see these emerging movements and there's portions of them that are engaging in harmful activity. They have a number of violations on our platform and so we're seeing this coordination of violations that's happening that gives us some indication of, you know, where do we draw those lines around what is, you know, acceptable and unacceptable because, you know, as Renee mentioned, we have to think really hard around, you know, where that begins and ends and how we sort of address authentic, you know, coordination without sort of harming the very real and authentic coordination that happens all the time, whether it's political campaigning or grass roots groups and others that are, you know, using the Internet as it was designed to be used which is to find one another and work together to amplify something. Where is, you know, how do you identify what makes it harmful, what makes it intentional versus unintentional? That's something that we're spending a lot of time thinking about and then, of course, in the sort of other piece of the authentic is the overt influence space. As we're putting pressure on threat actors in the covert space what is the appropriate way to handle, you know, government channels, you know, there's an argument

to be made that a lot of academics and thought leaders have made around this idea of making sure that people are exposed to that information. How do you balance exposing people to what a government's propaganda is with trying to make sure to limit its harms? And so those are some difficult and challenging policy questions that we're spending some time thinking about.

MS. BRANDT: That's great. We have a question here from Kermit Palos from Arlington, Virginia who asks about accountability and anonymity. He says full accountability means zero anonymity and full anonymity means zero accountability. Where is the best trade-off and is it variable by country? If anyone wants to chime in? Don't be shy guys. I mean, I can offer a few thoughts just to kick us off which is, you know, I think one of the things that have emerged in the conversation today is like the multi-platform nature of many of these operations. And I just think it's important we understand the different natures of different platforms, what their designed is to do different things. I think that's healthy and so, you know, I think it's useful that Twitter, you can be whoever you want to be that, you know, makes it a space that, you know, is safe, or at least safer, for activists and journalists and opposition figures who are working in really tough closed-in closing spaces. And I think that's like, you know, a really important feature of the platform.

And, you know, it's equally, you know, useful in other contacts that, you know, for example Facebook requires you be who you say you are, and that makes it easier to police certain forms of inauthentic behavior.

So I think, you know, as a whole it's sort of not realistic to expect that there will be any one model, you know, for what anonymity does or doesn't look like online. And that's probably healthy that we, you know, democratic, pluralistic, open information environments, you know, these vulnerabilities from this patchwork of different platforms that have, you know, varied, you know, approaches to questions like this, and to many others too.

But I think there's also, you know, sort of enormous resilience dividends,

you know, to that, to the sort of variable nature of the answers to that question and similar questions. I don't know if others have other thoughts.

MS. DiRESTA: I think the one thing that's been interesting is looking at what are areas in which collaboration or similar policies make sense and then what are areas that we're going to have a different association.

As you know, I think that the, you know, the value of the experience being different, you know, the draw for different user bases, you know, people participating in the types of online experiences they want to. We don't want to see that flattened or homogenized.

But I do think we've seen, you know, terrorism, child exploitation, and then election integrity has actually been I think another big area where there has been a lot of cooperation and it's I think really coming to a more rigorous definition of what it means to have harm and what are the areas in which that kind of, you know, harm framework justifies increased collaboration or increased cooperation or even a recognition that unfortunately, you know, one platform moderating something while another platform does not sometimes actually creates more problems as, you know, as things, you know, as content moves around the Internet.

So tying moderation and policy and thinking about, you know, anything from CIB to this, you know, line of alternate literature around freedom of expression has to be tied, I think into some kind of notion of is this is a high harm area that justifies a collaborative effort or a similar policy or a data sharing relationship versus, you know, something that is more akin to somebody said something wrong on this platform over here.

MS. BRANDT: I think that's right. And like just to layer on, you know, I think we want our policymakers to be thoughtful about what is properly understood as a content problem. Like I would say hate speech, child sexually exploitive material, these are properly understood as content problems and we have sort of long traditions on how to, you know, from the alpine space on how to deal with them and such.

Whereas like many of the challenges we're talking about today, you know, disinformation that's polarizing and misleading and often sort of indistinguishable from, you know, from very authentic behavior online, you know, that's an entirely different problem that needs probably different solutions.

DR. WANG: So I think I'll share a little bit about my viewpoint on this issue because this panel we talk about the information operation across the border, right? So information operation in other countries.

So when we talk about this issue actually there's a very small amount of accountability that we can actually see because when we talk about accountability as it's related to human rights, most of the accountability is actually decided by the court, it's decided by the judge. But their power cannot extend across the border, right, so when there is an information operation from other countries, from foreign countries, actually there is very little that the court or a judge can do. There is little accountability that any government can really do about it.

So the only thing that I think the government as well as the patron can do is to reveal the information. Just like a feature writer, that feature, anybody that will release the archive about a coordinated behavior from the nefarious country for research, to do their research for popular opinion to be informed that such behavior exists. I think that is the most accountability that we can do toward this issue.

So I think that is what I am going to say, it's really how to put accountability into this cross-country information operation.

MS. BRANDT: And yet at the same time I think, you know, foreign influence operations don't trigger the same. While they trigger a complex set of political and sort of fraught political dynamics as almost everything does, it's sort of next level when you can, you know, sort of consider, you know, the role of domestic actors.

MS. BELOGOLOVA: And one thing I'll say on that front really quickly is, you know, we've seen a trend in the operations that we've identified over the years. Of

course we've spent a lot of time talking about foreign threat actors but a lot of the operations that our teams are finding are domestic in nature and they're focused on domestic audiences. And we've seen an increase in that if you look at some of the numbers that we have in our SIO stat report in May 2021 versus some of the numbers we published at the end of 2021, you know, we've seen certainly an increase in domestic refocused operations that we've found.

Now they may have always been there but we're starting to see more and more of them as we look for this type of behavior because we are in our investigations agnostic to whether, you know, we're focused on the behavior, we're not focused on foreign versus domestic until we sort of unpack it and start to look at what really is under the hood once we identify the operation.

MS. BRANDT: We've received a couple questions here that focus on the role of emerging technology in the information operation space and I'm curious. We heard a great deal about sort of the trends you're tracking and like what's to watch and how are the teams and actually very little about deep fakes or, you know, AI generated, you know, profile images or chat bots or, you know, sort of AI empowered, you know, we use this for information technology. So I'm curious, you know, do you think that that technology will have an impact at the margins, that it's having impact already, or that, you know, sort of the fundamentals are what will sustain these kind of operations going forward?

MS. DiRESTA: Yeah, I'll tease that we have some work coming out on the AI generated text, you know. It is a space where text space constant is it's very hard to detect, you know. A lot of the signal that we have in video or in audio or in images is just not present in a lot of mechanisms for, you know, the kind of uncanny value feeling that is still present even though in another couple of years I think that will be gone.

But, you know, we've done some recent work on a network of a couple thousand GANs generated bases on LinkedIn, you know, it's just massive numbers, it's almost become table stakes at this point and people just use them. They will get better,

they'll be harder to find, ergo platforms are investing capabilities into thinking through, you know, what new and novel technologies, you know, how will new technologies change the game. And that's how we think about it at SIO. A lot of our work on this front is saying emerging tech is one of our distinct kind of four practices areas and we think about how does emerging tech intersect with information operations, how does it intersect with trust and safety questions, which are more things like harassment or other areas of online abuse.

And, you know, we see it again as the technological landscape is not stagnant, it will continue to evolve and so adversaries will continue to incorporate new and novel technologies in new and interesting ways into their operational playbooks. And we just try to think through what is that going to look like and what are potential responses.

I think Deep Fakes are particularly interesting in that platforms and researchers both invested extensive amounts of time in looking at the video detection capabilities. I think Facebook and Goggle both, if I'm not mistaken, you know, sponsored some research prizes and, you know, and data sets and things like this. And one of the effects of that is it also reached the public, right?

So on this education piece that is so critical, I think just absolutely foundational going forward, how should the public think about propaganda, what does propaganda look like today. There is this opportunity to educate and to say there are these new technologies that enable the following things to be created. And that was very much part of the public conversation around Deep Fake video and potentially is, you know, going to become more of the conversation around imagines and texts as, you know, technologies continue to capture the public imagination.

MS. BELOGOLOVA: I'll also add that I think, you know, over the years we've seen, you know, an increase in use of GAM images as part of these operations, but that doesn't necessarily mean that, you know, this has become, you know, a new technique that has fundamentally changed the detection picture.

We, you know, we find these operations and maybe, you know, it's a little bit

better for them to take a picture off of this person does not exist .com instead of, you know, stealing a picture of a celebrity and using it as their profile picture. But I wouldn't say it's necessarily sophisticated persona building just because one takes a gam image instead of, you know, some stock profile picture.

But, you know, as Renee said, we are continuing to look at when these operations are investing in these types of techniques but ultimately, it's helpful that we focus on the behavioral element when trying to define these operations because, you know, the operators will use whatever lowest thing for the buck they can get, right? If they can run the operation without having to use any sort of sophisticated techniques, then they're going to do it. And, you know, perhaps investing in more actually, as Renee mentioned at the very outset of this conversation, analog techniques because those are harder to detect, there isn't as much resilience around those in society. We haven't talked as much about some of those analog techniques we've seen throughout history.

And the last thing I'll mention is, you know, a specific example where I believe it was in March, you know, about a month after Russia's invasion of Ukraine began, where there was, I would say, a cheap fake video of President Zelenskyy, it's very clear to anyone looking at it that, you know, his neck didn't really match up with his head and where it was. And Zelenskyy's team effectively went and pre-bunked because they knew it was coming. And that was really effective because it basically just sort of helped the public understand that this fake was coming and what it was and that it wasn't him and that he wasn't there, and he didn't say those things.

And so there's a lot of ways in which people are starting to think about, to Renee's point, how to address this problem before it becomes a bigger one.

MS. BRANDT: Well let me just say thank you, a big thank you, to all of our panelists for a very rich discussion. It was, I think you all helped to lay out like what democratic societies are up against but also, you know, what they can do about this problem. So we're very, very grateful and thank you again.

At this point I'm going to hand the discussion over to my colleague Melanie Sisson, who is a Fellow in the Strobe Talbot Center for Security, Strategy, and Technology here at Brookings.

She's going to be talking to some of our other Brookings colleagues from across research programs, looking at advanced military technologies in the U.S./China competition, and asking the question, how advanced are they really and how much do they really matter.

So let me hand over to her with a big thank you. And looking forward to this next discussion. Thanks so much.

MS. SISSON: Thanks very much, Jessica, very much appreciated. I'm delighted to be here. And to pick up a little bit where you and the last panel left off talking about emerging and advancing technologies.

In this case it's a real pleasure to welcome everybody to this conversation on advanced military technologies, in particular in the U.S./China competition.

As Jessica said, my name is Melanie Sisson and I'm delighted to be joined today by two people that I have the privilege of calling colleagues. Caitlin Talmadge is Associate Professor of Security Studies in the Edmund A. Walsh School of Foreign Service at Georgetown University and a non-resident Senior Fellow with the Foreign Policy Program here at Brookings. Caitlin is a careful and thorough researcher and a prolific and I think enviably cogent writer on the most important defense and security issues facing policymakers today.

We're very fortunate also to have Tom Stefanik, a Brookings Foreign Policy visiting Fellow. Tom's career includes years of managing hands-on research and development of advanced technologies, including but not limited to machine learning, image recognition, and autonomy. Tom's also a very serious thinker about the implications of these technologies for military tactics and operations. And these topics are in fact the subject of his forthcoming book about which we're all very excited, that he's entitled

Information War; How Artificial Intelligence is Driving U.S./China Military Competition.

The emphasis in Caitlin and in Tom's work on emerging technology of course is neither accidental nor coincidental. It reflects the reality that one can't be conversant in national defense, military modernization, or geopolitical competition without considering whether, which, and how, advances in technology might affect the ways in which nations structure, equip, and use their military forces.

Recent advances in technologies like machine learning and hypersonic missiles have produced a very potent mixture of enthusiasm and anxiety that's reflected in sometimes excited language about the future of warfare. So we hear about robot armies and sputnik moments and transparent oceans. And this reflects in some cases the assumption, and I think in other cases the concern that these technologies are truly transformative or very soon will be and that as a result they're central to the course and ultimately the outcome of the competition with China.

So I'm especially pleased to have Tom and Caitlin here to help us think through what these technologies can and can't do, the ways in which they do or don't enhance military capability and their potential implications for the ways in which international competition might unfold.

All of which is to say Tom, Caitlin, I'm counting on you to tell me just how enthusiastic or anxious I really ought to be about these emerging technologies, and welcome to you both. Thank you for being here.

To our audience, a reminder to please submit your questions to Events@brookings.edu.

So Caitlin, I'm going to start with you, I'm going to give you the first bite of the apple on a general question that I will then invite Tom to follow up on. And it is the sort of big and basic question. Are any or all of these technologies in fact transformative or likely to be in the near term which we can consider say the next 10 years?

MS. TALMADGE: Great. Well thank you so much. Big question,

interesting question. It's great to be here with you. Thank you for the introduction. It's great to have the opportunity to have chat with you and with Tom about these really important issues.

And I think you've hit the nail on the head with the big framing question, which is, you know, does, you know, how concerned should we be, do these technologies really matter, and if they do, how, and why, and where.

And I guess my take is a bit tempered on this topic. I think that technology, and advanced military technology specifically, certainly matter in the U.S./China competition. It would be kind of silly to say that they have no role. But I do worry sometimes that the role of technology has become a bit over hyped and over anxious in our discussions of these issues in the U.S./China relationship.

For my part I don't think technology is the major driver of competition in the relationship, although you could be forgiven for thinking that, I think, sometimes based on what we hear. Nor is it likely to be the main determinant of the outcome of U.S.-China competition over time. I think in many ways technology has sort of become a proxy for lots of other concerns in the relationship and people are concerned about the relationships and they get more concerned about technological competition even though I think technological competition often just reflects what's going on in the relationship rather than actually being the engine of those dynamics.

And, you know, we clearly are, as you noted, living in a time of really significant technological change. I mean ask Alexa, look down at your Smart Watch. I mean I think we all kind of know that there are both civilian technologies that have military implications, and some of that was discussed a little bit in the last panel. As well as advanced military technologies, you know, like hypersonic missiles from the sensing and so forth, that clearly are changing some things.

But fundamentally, in my view, I think the real driver of both the course and the eventual outcome of U.S./ China competition is not likely to be technological. Those

drivers I think will be above all political and strategic organization, dot trainable, geographical. And of course all those factors interact with technology, but I think they are distinct. And I'll give you an example to kind of sketch what I mean when I say this.

You know, one of the technologies that we hear the most about, and I think you previewed this, is hypersonic missiles. So missiles that can travel really fast, five times the speed of sound, you know, we hear a lot of concern about them. And, yeah, they're a notable military technology and they are important in the U.S./China relationship. But I would posit that those missiles really only matter because of other competitive political dynamics in the U.S./China relationship, often involving much older technologies I would add.

If you think back to summer of 2021, so not this past summer but a summer ago, we heard a lot about China's test of a nuclear capable hypersonic glide vehicle mounted atop a fractional orbital bombardment system. And there was a lot of concern about this. General Milley, you know, was asked like is this a Sputnik moment? And he didn't say yes, it is but he said it was very close to a Sputnik moment. You know, and people were concerned about it but, you know, I am a bit less so simply because, you know, the reality is that, you know, first of all missiles that can reach the U.S. homeland that carry nuclear warheads and travel faster than the speed of sound are not a new thing. We already have had missiles around like that for, you know, 60 plus years. They're ballistic missiles, I think, you know, we sometimes forget that, and those actually travel faster than hypersonic missiles by a lot.

And this fractional orbital bombardment system that China use to deliver the, use to carry the hypersonic glide vehicle, that's also not a new thing. That's, you know, technology that's used to launch the space shuttle. So this isn't, you know, a cutting edge set of technologies here. It's true that hypersonic glide vehicles like the type that China tested can maneuver to their targets unpredictably in ways that ballistic missiles don't because ballistic missiles flight is ballistic, right? And so you know where it's going to land.

And it's true, you know, if China mounts a nuclear capable weapon on the spa delivery system, then they can approach from this other hemisphere where the U.S. has no missile defenses deployed and, you know, that could be significant if you think that currently U.S. missile defenses otherwise would protect the U.S. from strategic nuclear attack.

But, you know, I guess my point is first of all I think this isn't really cutting-edge stuff, but secondly, it's important to step back and sort of ask well why was China doing this in the first place? Like why did China test this? And, you know, this goes back to what I was saying about kind of political and strategic factors having primacy because I think, you know, what China was trying to signal with this test is, you know, hey, if you, the United States, ever engage in a nuclear first strike against us, China, we're still going to be able to land Chinese nuclear weapons on U.S. soil even if you, the United States, deploy missile defenses, right? That's what showing this capability I think was about.

You know, that the United States can't have its homeland as a sanctuary if it's lobbying nuclear threats against China, and missile defenses won't, you know, won't change that.

So, you know, yes, this sort of system potentially enables China to make threats of nuclear retaliation against the U.S. more credible if you think they're not credible in the status quo, which makes the U.S. less able to make credible nuclear threats versus China. The U.S. has to worry more about escalation coming back on its homeland.

But I would just step back from this whole discussion and sort of ask like, is the problem here really hypersonic missiles or is it that we live in a world in which China's concerned about, you know, U.S. nuclear first strike? It strikes me that the latter is really what, you know, what is concerning people here.

And to put it another way, you know, is the concern the hypersonic missiles or is the concern a world in which the United States feels that it needs to be able to lob credible nuclear threats vis-à-vis the Chinese arsenal, because of concerns about what

China might do conventionally in the region against the United States or its allies.

And, you know, these are open questions. You can have different answers to them, but my point is those sound like political strategic global issues to me. They don't sound like technology issues. Technology might make them a little bit worse but taking the advanced technology out of the equation doesn't solve the underlying strategic and political dynamics that are producing conflict and creating anxiety on both sides of the nuclear relationship.

And I'll just pause there for now, but I think that that, you know, kind of provides an example of why your technology, we always kind of have to look at it in this broader context. So I'll pause there for the moment and, you know, we can follow up or perhaps hear from Tom.

MS. SISSON: Thanks very much, Caitlin. You've introduced a lot of themes and issues that I know that we're going to look forward to returning to as the conversation progresses.

Tom, are you as sort of moderated in your perspective as Caitlin? Do you share her perspective in any or all ways, or points of disagreement? In short, what is your view on the extent to which these technologies are fundamentally transformative in the military domain?

MR. STEFANIK: Well first, thank you very much both, and thank you for our audience for being here and taking the time.

You know, I think Caitlin laid it out perfectly. You know, the primary factors here are geopolitics, international relations. And technologies can influence in its specific behaviors, but the major driving force is the really long-term historical driving forces are geopolitical ones.

We have two examples in front of us now. In Ukraine, as Caitlin mentioned, we've been living for 60 years plus with nuclear weapons. It's clear that the U.S. behavior and Russian behavior vis-à-vis the Ukraine and the war in Ukraine, has been strongly

influenced and continues to be influenced by the presence of large numbers of strategic nuclear weapons in the Russian arsenal and the U.S. arsenal. Russia's used that sort of rhetorically on a large number of occasions. It's affected, maybe even constrained, some U.S. behaviors, and, you know, it's a concern.

It remains a concern. I mean to the point that the director of national intelligence, Avril Haines, last May testified that, you know, if, when asked what would cause Russia to use those nuclear weapons, she said well, it might be a Putin and his close circle thinking they have an existential threat to the regime or the state. And when asked, well what would constitute an existential threat, it would be well, possibly losing in Ukraine.

Now we don't know exactly what that means and I'm not going to get too far into that but there's a perfect example of what Caitlin said is that it's nationalistic, geopolitical concerns that are the drivers here.

I'd like to focus, there's another major technological change that has been happening roughly over the same period of time, and that's our shift from analog data to digital data and digital technologies. I mean it started in the 60s and is now been punctuated by kind of various outgrowths of that. Some of it being, most notable probably being the Internet, which was a topic of the last panel's discussion, and the impacts of that.

In the military side I would say that the major impact of that is the proliferation of very inexpensive sensing globally cheap satellites. Drones that are very inexpensive with sensors on them, not weaponized, but just sensors on them. So I think that's the major technologically theme that has many, many kind of offshoots but none of them dominate the themes that Caitlin mentioned. The real drivers here are these geopolitical pressures. Over.

MS. SISSON: Thanks, Tom. So I want to, so what if we changed the phrasing of this and instead of asking about these as drivers of competition, we have to acknowledge that technology is the place where there's considerable strategic interaction, right?

And so I'm curious, Tom, from your perspective whether we want to call it a direct competition or if you want to call it addressing the strategic changes and other states' sense of capabilities. Is there a particular area at the operational or tactical level where you see this measure/ countermeasure strategic interaction happening that is actually particularly important?

You mentioned sensing for example. Is that an example? Are there others that are a front of mind for you where you see the United States, and China in particular having to work to understand where the other is and how to counter that?

MR. STEFANIK: Yes, absolutely. I think, I'll tell you, if I could take just a second and put it in the framework of information a little bit more generally and talk about information, you know, we have the previous panel was, you know, excellent, and I got to see a good part of it.

A big part of what is going on in the information in the broader kind of societal/political information operations that have been discussed in the previous panel. Those are operations that are leveraging the power of the business models that have grown on top of the digital Internet.

So we have digital technology, the Internet grows out of that, and then new business models grow out of that, Google, Facebook, etcetera. So if we wanted to just sort of simplify what those business models look like, they're largely about advertising. And they're largely about figuring out which ads to send to which people.

And so if I could put that in sort of military terms for a second, and then I'll move off that because there's a lot of differences in actual strategic military or tactical, operational military operations.

You know we are the targets. We are the targets of advertising. It's very important for these businesses, for their business model, to have good information about our behaviors our, you know, what we're interested in for example. Our senses are of course our mobile phones and our devices. They collect that information, they use it, and they use

that to send literally targeted ads.

Well switching to the military side, if we take for example in the Ukraine right now one of the most important aspects of the fighting there is both sides, and we see this dynamic working out in ebbing and flowing, both sides struggling to find out where things are in the Ukraine and the Donbas, and what they are. And then deciding to attack them with force.

The same would be true in any hypothetical, hopefully not, conflict in the Straits of Taiwan or the East China Sea or South China Sea. But that information in the military sense is understanding what's present in the battle space, what it is, and where it is. And that is by far the most, that's a simplified version of the most important thing that militaries have to do. Now I'm leaving aside the things that we're all familiar with, which is ships and airplanes and bombs, are all things of the physical domain. But that's because I think the growing geopolitical or maybe I should say technical and operational emphasis will be on information itself, finding where things are because without that information and targeting information these missiles and bombs and, you know, are essentially wasted. Or tragically in the Ukraine case, are used against civilians.

So I think the upcoming, especially with regard to China, the upcoming dimensions of the military competition will be in trying to see more of what is present in the western Pacific on a real-time basis, and trying to move that data. And at the same time to one's own military commanders but at the same time the other side will be trying to deny that data and those images or sensor data and trying to do that within using jamming and electromagnetic warfare and various methods.

So I think that is where I would focus the future technological competition rather than on particular physical, you know, bombs and rockets and that sort of that thing. All of which remain important, but I think the information demand is kind of the emerging operation side.

MS. SISSON: So, Caitlin, taking Tom's conversation about advancements

that are currently happening and his belief that that will continue to be a focal point of research and development in technologies, making states more capable of seeing longer, further, in more difficult terrain, inhospitable terrain, and being able therefore to find each other's assets.

This could have some considerable implications in the nuclear domain where stability basically is underwritten by uncertainty. The uncertainty that you could find the other states, the entirety of their nuclear assets and thereby insulate your own homeland against attack.

So how worried are you about the development of those sort of seeing and finding technologies? Should I be losing sleep in the near term? How long do I have before I need to really start worrying? Thanks for any either comfort or continued anxiety you can provide on that account.

MS. TALMADGE: Sure thing. Well I mean if you study nuclear politics today, I mean there's always a reason to deal with these unfortunately. I guess this panel is just how much of the lost sleep should be over technological developments.

And I think it's a really important question thinking about, you know, what do new technologies mean for nuclear stability. And you mentioned the kind of hide or finder issue, you know, what does AI mean for technology, you know. And I think that's an important one although you can even think of, you know, additional applications of new technology to nuclear stability.

I think you and I have talked some also about the question of, you know, integrating automation in the nuclear communication control, for instance. Well, you know, what does that mean for stability. And we should certainly get Tom in on this since he's our, you know, AI expert.

But I mean it's a challenging thing to answer because, you know, you're really talking about two sets of things that we don't have tons of data on, right? Which are nuclear crises and wars, and of course the lack of data on those is good, we don't want

more data when it comes to, you know, nuclear crises and nuclear wars. And, new technologies, right? So like technologies we haven't necessarily observed in a type of conflict that we also haven't really observed much. And so, you know, we're left with, you know, what we political scientists would call hypothesis. I promise not to use that word again.

But it's something I've noodled on, and I think, you know, for now mostly what we have are sort of some different ways I think that emerging technologies, and particularly, you know, artificial intelligence, could impact nuclear stability. And a lot ultimately depends on how these things are actually deployed. Which kind of goes back to what we were talking about before, which is to say like the technologies, the technology, and how it impacts stability depends a lot on doctrine and organizational capacity and political decisions.

And I'll give a few examples because I know that's kind of, you know, 30,000 foot, but I just, you know, I think it's important to be modest about what we actually don't know when we're talking about two hypothetical things, you know, nuclear conflict and these new technologies.

You know, I think the pessimism case, you know, would be partly, you know, what you just laid out, that a world where you have, you know, artificial intelligence that's linked up with improvement in remote sensing, you know, you really could get a big boost to states' efforts at counterforce, that is their efforts to find and destroy adversaries with their weapons. So if you go back to that kind of nightmare scenario that I laid out in my, you know, cheerful opening remarks about, you know, a U.S.-China nuclear conflict like let's say we are in the role where the United States is hunting Chinese mobile nuclear missiles. You know, a lot of those missiles are going to be in transporter erector launchers. They look a lot like trucks. You know what else there is in China? A lot of actual trucks, right? And so, you know, the question is not how do you find the transporter erector launchers, the tells, it's how do you find the tells when they're mostly surrounded by trucks? And, you know, it turns

out like AI, that's something that, you know, machine learning can help you with a lot, potentially.

And so, you know, is that stabilizing or destabilizing? Well, it kind of depends on what you, you know, what your view of nuclear deterrent is and how much you want the United States to be able to hold Chinese nuclear weapons at risk. I think there's, you know, some people, you know, certainly in the U. S. government, who would say that actually could be stabilizing because it would deter China from getting involved, you know, in a crisis in the first place.

But in any event, like from the kind of standard classic deterrent perspective it's not good for the reasons that you laid out, right, the uncertainty is kind of the price we pay for nuclear stability. And if one side really has this technology that enables improvement to its counterforce capabilities that could be destabilizing.

There are also concerns on the pessimism side that artificial intelligence in nuclear command and control could make it more vulnerable to hacking. This is something we hear a lot about. You know, I would just note that that is not really a new problem. You know, Tom was kind of alluding to some of our electronic warfare efforts, you know, in the cold war as well. But I mean, you know, as long as there have been nuclear weapons, there have been state efforts to interfere with adversary command and control of their nuclear weapons. I mean that was something that we did, you know, when everything was analog.

And it's interesting, like in the late cold war the U.S. had this program called Canopy Ring, which basically enabled it to infiltrate the command-and-control system that would have launched Warsaw Pact nuclear capable aircraft in Europe, with the idea of being able to disseminate false orders to Warsaw Pact pilots. Again, this is like the age of eight track. So, you know, is that good? No. But is that new, probably not. You know, that's a project the U.S. has been working on for a long time.

And then I think just one other concern that we hear a lot about, kind of AI and nuclear weapons on the pessimism side is that it could become so integrated into

nuclear decision support that decision makers actually come to over rely on or over trust an automated decision support system in nuclear crises and, you know, you kind of could get the human out of the loop to the point where, you know, if the system is encountering a type of crisis or a type of signaling that it hasn't been trained on, you could actually have a heightened risk of nuclear accidents.

If you look back at the Cold War, you know, the instances in which false alarms were averted, you know, why was that? It was usually because the human being actually said, this doesn't smell right, I'm, you know, I'm either calling off or I'm, you know, I'm reading this as a, you know, false warning or whatever. And so, you know, again, it's like your automated decision support is only as good as the scenarios and the data that you train it on.

So I think there are some reasons for pessimism. But I'll just say I think there are also plenty of people who can envision mechanisms by which artificial intelligence being integrated into nuclear decision making or just, you know, being a technology that nuclear capable states deploy in various ways could actually end of being stabilizing.

You know, if you do integrate artificial intelligence to your nuclear command and control, I mean presumably you're doing that to improve your situational awareness, that your intelligence and your warning and, you know, there's a lot of people who would say that those are good things. That reduces, you know, pressure on decision makers in a crisis, it reduces the risk of false alarms, it helps decision makers process information faster, you know. And even the sort of strange love scenario of, you know, states automating certain launch procedures. You know, why would they do that?

Well, you know, if you look at why the Soviets developed their Dead Hand system in the Cold War, it wasn't for deterrent purposes, it wasn't to convince the United States that hey, if you attack us, you're still going to get nuclear weapons lopped back on you. They didn't signal that they had the capability. The U.S. actually found out about it through like counterintelligence and like didn't believe it because it sounded so crazy.

But like the reason the Soviets developed that was to reduce crisis pressure on their own decisionmakers, right? So that decisionmakers in Moscow facing the potential for a decapitating first strike wouldn't feel pressure to launch because they would know that, you know, even if their command center was taken out, their nuclear weapons would still eventually, you know, be launched. And fortunately we never like saw that system tested.

But my point is, like states actually adopted this stuff because they thought it would be stabilizing, they thought it would reduce pressure in a crisis.

So, you know, I don't have a pat answer to your question but, you know, I think the way that we should be thinking about this is looking at these mechanisms and then thinking about like what choices are states actually going to make because, you know, in that political and strategic and geographic and organizational context that we actually get to the effects of stability in particular cases. Over.

MS. SISSON: So you don't have to worry about it not being a pat answer. It's a great answer because pat answers might be good for, you know, reality TV, but, you know, answers that include context and conditionality make good policy advice. So I'm glad to hear all of that.

Tom, I want to turn to you for a question that kind of comes from me. I was having a conversation over the dinner table the other night about, you know, military modernization and the DOD acquisition problem, as one tends to do with their children over the weekend.

And one of the kids just piped up and said, well, mom, why don't they just buy whatever they need from Amazon? Right? So my question for you, Tom, is why can't the DOD, you know, just buy what it needs for its digital modernization efforts from the commercial sector?

MR. STEFANIK: Now that's a very good question. Well, there's a few reasons. I mean military systems have to operate in a very different sort of physical environment than sort of commercial ones. You know, if it's a sensor, it might be taking off

from an aircraft carrier on a helicopter or something and, you know, it bangs into the aircraft carrier when it lands, and there's shock; it's got to operate lots of different environments. It's got to be very reliable.

And so that's part of the reason. I think the bigger part of the reason is that in terms of the kind of data that you need to collect for military systems, it's data that's very peculiar to the things that military systems do.

So for example, one of the most, I think, consequential capabilities that the United States has just given to Ukraine is a missile that homes in automatically, really, really autonomously after it's launched and it's on its way. It homes in on radars and it specifically homes in on radars. It's got to pick out what the radar's signature is and, you know, all kinds of factors that distinguish radars say from a decoy. And the whole point of that is that those radars are the things that could shoot down Ukrainian aircraft or helicopters or even Ukrainian drones that are being used to collect data.

So there's an example of something that's very, very specific but very, very important. Because it's kind of a key element in this struggle over information. The Russians are trying to get information about what's in the air, Ukrainians are trying to get information about what's on the ground, using drones. They have to destroy those Russian air defense systems. So that's an example.

I'd like to, though, also maybe turn a little bit off your question and get back on to sort of artificial, this concept of artificial intelligence. It's a notion. So actually it's been around for a long time, it changes form. And today, I mean we talk about artificial intelligence today because of some very particular algorithms that have kind of done some pretty amazing things in the research, as well as in the commercial sector over the past eight years or so using banks of, you know, millions of, you know, pristine images of faces that have been collected over the Internet or lots of other things. It's been used to learn how to play computerized games or a computerized version of an aircraft versus aircraft dogfight. That was a recent computer simulation developed by DARPA, these deep neural network

algorithms which are called AI now, is used to learn how to be very, very effective within that simulation environment. And actually beat a human, an expert fighter pilot that was operating within that simulation environment.

So there's a lot of news coverage on that. I think it tends to get extrapolated too far because in many of these cases they're fundamentally different than the military environment. In the military when you're trying to sense something, the environment gets in the way a lot. The clouds cover oceans three-quarters of the time so you can't see through clouds. And if you try to use a radar to look through the clouds, those can be deceived or jammed and, of course, you know if there's a satellite going on, everybody knows when that satellite's going by.

So the information environment of the military is radically different than the, you know, the Internet based and research information environment that we've seen a lot of their capabilities come out of. And this is why we've seen, you know, tremendous strides in artificial intelligence adoption over the past 10 years in the internet and Google in 2015, now use a deep neural network in search, lots of other cases.

The military has been, it has a difficult doing that, and I'll actually mention this, the data's hard to get. It's a small data environment. The Internet communications, Internet commerce, that's a big data environment, that's what it used to be called in the 2010s, in 2000. It was all called Big Data. And it was these algorithms that came along and they were just suited for that environment. They're not well suited for the small data, low information, low data environment of the military. Over.

MS. SISSON: Well, Tom, I'm not going to lie to you, I think my kid is going to be very disappointed by your answer. But I'll be sure to break it to her over dessert.

We do have just a couple of minutes left. I want to take advantage of them to ask each of you for your sort of main take away message here. So if you can leave me and the audience with sort of that one thing we should carry with us in our heads about the role of advanced and emerging technologies in the military domain, about what you're

seeing in terms of military technologies in Ukraine, what you think about artificial intelligence. One thing that you really think people, you know, can't hear too many times as part of this conversation, I'll be grateful for that.

So, Caitlin, I'll start with you, and then, Tom, you'll get the last word.

MS. TALMADGE: Great, thank you. I mean I would close by kind of reemphasizing the points I began with, which are that technology is definitely consequential. It's definitely an issue the United States used to pay attention to in the competition with China. And there's no doubt that we are in a period of serious technological change.

Where I would encourage people to pump their brakes, though is in thinking that technology is a driver or, you know, determinative of outcomes in the competition only because I worry that we over focus on technology to the point that we may actually be overlooking other more simplistic stuff that's right in front of our faces that's actually going to determine outcomes.

I mean I think Tom's reference to the high speed antiradiation missiles in Ukraine is a great example of that. You know, how many times in the last, you know, 10 or 15 years have we worried about, you know, kind of new-fangled technologies that Russia has tested and announced? You know, nuclear torpedoes, right? You know, all of these sorts of things.

But like what's actually driving a lot of outcomes on the ground? It turns out it's these hard missiles rigged up to like big fighter jets which is this, you know, strange marriage that I never thought I would see. But, you know, those missiles are old. I mean those missiles were -- do you know when did we -- I remember learning about them in the Kosovo War, you know, and that was like 23 years ago, right?

And, you know, I spent a lot of time thinking about Taiwan. And I know, Melanie, you do too and are just back from there. And, you know, when I think about like what's going to determine the outcome of a U.S./China conflict over Taiwan? I mean what's the most important issue that, you know, we should be focusing on in that relationship? It

isn't cutting edge technology. It's really not.

You know, I think the outcome of that conflict on the hardware side is going to be determined probably by old technologies like ballistic missiles, like cruise missiles and fighter jets and air defenses and even really old stuff like C mines could be really consequential in a Taiwan campaign. You know, and there's a bunch of stuff that would matter that just isn't hardware and isn't technological at all.

You know, like what is Taiwan's defense posture? How well can Taiwan mobilize? Are the Taiwanese going to resist the way the Ukrainians have? Are they going to train the way the Ukrainians have? When and how would the U.S. intervene militarily and, you know, economically and in other ways? In some ways, it's like, well, that's kind of an all to note. But it's like, yeah, but that stuff isn't technological.

You know, those are really important political strategic level factors that I think you're going drive outcomes. And so, it's not to say that we shouldn't pay attention to technology, we should. But perspective and context matter a lot. And when we ignore those, we can get over focused on technology. And then I fear really surprised in a crisis or a war when technology isn't the silver bullet or isn't the boogey man that we were expecting. And something else turns out to be really decisive.

MS. SISSON: Great. Thank you, Caitlin. Tom, you're turn.

MR. STEFANIK: Yes. Well, that was a really terrific summary. And all of that I think is just very well put.

I would add I think something that's actually a little bit different. And it's more kind of at the determinant or the problems of an overfocus on a particular technology. AI is one of the big ones now. And again, I would -- I hesitate to use the word AI because it's really this particular style of computer program or computer algorithm that happens to have these nice properties.

But that overfocus and we've seen this in the National Security Commission on Artificial Intelligence. You know, a strong focus on big funding increases for this one

particular style of technology. And it's completely counter to the way of thinking about solving problems in a kind of engineering or developmental or cost-effective context, which is you come up -- you understand the requirements. You understand what you need to do to operate in a sustained way to deal with the logistical problems, to deal in a way where you don't have to make sudden decisions about the use of destructive force against a nuclear armed power like China, Russia.

And so, the overfocus on a particular technology can distort the spending in a way that's just not the right mix. Now, that's a complicated problem to come up with the right mix, but it includes all of those things that Caitlin mentioned, logistics, training. A lot of things that are not, you know, the latest and greatest technology or the presumed greatest technology.

So that I think is -- that putting a technology first in funding and decision making I think is more likely to lead you to misallocating scarce funding resources and we have scarcity.

MS. SISSON: Well, Tom, Caitlin. Thank you so much for a really rich and substantive 45 minutes. You covered a lot in depth and breadth and I'm really grateful for your time as I know the Brookings audience is as well.

I think that we are going to sign us off so that we can move into the next section of this really excellent forum. I'm going to have the pleasure of handing the reigns over to our colleague, Chris Meserole, who is the Director of Research for the AI and ET series of work here at Brookings. And I think it's probably apropos that I'm being sung out by the low-tech lawnmower that my neighbor has decided to deploy at this very moment. Chris, over to you and thanks again to our audience.

MR. MESEROLE: Thank you so much, Melanie. And thank you for moderating such a rich and vibrant discussion. You know, after two great panels of this symposium so far, we've got a lot to live up to here in the third, but we look forward to giving it a go. So thank you again, Melanie, to you and your colleagues for such a great

discussion.

During this session, we're excited to talk over how AI and other advanced technologies are being exploited by nonstate actors in rogue states a like. Terrorists and criminal groups have a long history of being early adopters of new and destructive technologies. And there's every reason to expect that they will do so with AI and other digital technologies as well.

At the same time, authoritarian regimes are also adopting and leverage those same technologies for surveillance and repression. Often, ironically on the pretext of cracking down on terrorist groups and nonstate actors.

So what we want to do today is bring those two issues into a conversation with each other. You know, how do democratic societies guard against the malicious use of digital tech by violent nonstate actors on the one hand? And against authoritarian regimes who leverage new technologies for great surveillance and control on the other? What are some of the policy frameworks that we should rely on to help think through that balance?

All of these are questions that we'll be wrestling with in this conversation. And to answer those questions and others, fortunately, I am extremely grateful to be joined by three really fantastic colleagues and guests. The first is Sarah Kreps who is John L. Wetherill Professor of Government at Cornell as well as a Senior Nonresident Fellow here at Brookings and an expert on technology and conflict.

Another is Dahlia Peterson a Research Analyst at the Center for Security and Emerging Technology at Georgetown University. And the author of a number of leading studies on digital surveillance technologies including and especially Chinese surveillance technologies.

And then last but by no means least, our third guest is Ishan Sharma, a Fellow and Advisor for Strategic Initiatives with the Federation of American Scientists, who has also written extensively on responsible use of surveillance technologies.

So without further ado, I think we can dive into the discussion beginning,

frankly, with just some level setting on just what these technologies are and how they're being used. So, Sarah, let me start with you.

How exactly, you know, as AI is kind of a buzz word out in the era right now as are kind of all these emerging digital technologies. So can you walk us through kind of what -- how nonstate actors might use these technologies and what kind of capabilities that they afford nonstate actors in line with the great new paper that you released earlier last year?

MS. KREPS: Well, thanks, Chris, for convening this distinguished panel. The topic is obviously important and timely.

And so, I guess I would just sort of start with some of that brush clearing that was covered a little bit in the previous panel, but for those joining here, I think it's important to note that we talk a lot about AI. And I think that's because it is useful shorthand for a much more complicated kind of set of ideas.

And I'll use it too, but I think what we really want to kind of think about is AI not as kind of a hardware, but rather an enabler that is a combination of algorithms and software that intends to kind of -- that learns from what it's trained on. Whether -- some kind of dataset to improve the efficiency of whatever it's doing or what it's trained to do. And so, I think we'll probably all talk about that in different ways, but I think in the context of AI and nonstate actors, it's important to think about AI in this context of enabling something that they're already doing.

So in my paper, I look at three I look at three different areas. So I look at drones, I look at cyberattacks and I look at online misinformation. And in each of those contexts, it's not now allowing these nonstate actors to do things they weren't doing before. What I show is that in these contexts of drones and cyberattacks and misinformation, it's -- the AI is allowing them to do these attacks more efficiently than they were before.

And so, I'll take just one example. And so, if we think about, let's say, misinformation or cyberattacks, these are both kind of online activities. And how do these

cyberattacks or how does online misinformation work? It works by finding vulnerabilities. And those vulnerabilities can be more easily identified through algorithms that based on previously successful attacks can now in the future target or micro target more efficiently those vulnerabilities that they have found. So it makes these attacks that have already kind of been shown to be an interest of nonstate actors, it makes them more efficient.

I think we have a lot to talk about so I don't want to take up too much air time, but I think just kind of putting that out on the table might be a starting point for my colleagues to kind of graft onto that.

MR. MESEROLE: That's a great starting part. I think the one quick just follow up question is, you know, these technologies, I think a lot of people are associating AI or kind of digital technologies with the need for like really sophisticated technical skills.

And I'm curious if you can just talk a little bit about how accessible are these technologies even to small groups of users or to organizations that might not have, you know, 100 computer scientists, you know, working in a lab somewhere? Is it still possible to kind of get advanced kind of capabilities even with, you know, trivial technical skills, but, you know, at least enough technical skills to kind of download different packages from the web or things like that?

MS. KREPS: Yeah, Chris, I think that's really important because what started with -- what's different, and I say this in the paper. What we used to have was with, say, nuclear proliferation was that it took so much expertise and so many resources and still does to have a nuclear program.

And what's different now with AI is that it is really democratized. It's relatively affordable. It's all available in the civilian space or the consumer space. And so, if we think about something like misinformation online and something I've worked on empirically is to try to understand the ways in which something like GPT3, a natural language model, can be used to create and manipulate public opinion through micro targeting. Understanding kind of how people think. How people tick.

Now, we have all this big data that can be analyzed, and this technology is out there very easily and accessible to create less I.D. fakes for misinformation at scale that can then be used by these nonstate actors. Again, they're very affordable and accessible ways to target massive amounts of people.

MR. MESEROLE: Thanks, Sarah. And, you know, I appreciate the point about how accessible these are. And, Dahlia, I want to turn to you now because if nonstate actors and kind of even small groups are able to use this then certainly large states are too, right?

And you've done a lot of great work on how China and other states have developed surveillance technologies using AI and other digital technologies. Can you talk a bit about -- especially in light of some of the recent work that you've done both yourself and with colleagues like Samantha Hoffman -- just some of the trends that you're seeing in terms of the emerging capabilities that states have for surveillance and repression in particular in China?

MS. PETERSON: Yeah, sure. So thank you so much, Chris, and to Brookings for having all of us. It's a really great pleasure to be here.

So China really uses AI in its surveillance systems to target everyone across the country. It essentially doesn't assume innocence in any individual and it views everyone as a potential threat to social stability. So this includes every day citizens, but there's an especially magnified scrutiny on what China calls, focused personnel.

So those are those who are suspected of terrorism, for example. So that includes the Uyghur minority. But also includes those with mental illness and those who petition the government, for example. So we could see with the New York Times in their recent, incredible investigation into surveillance procurement data in China that companies like Megvii are identifying people in those exact specific categories of focused personnel.

But beyond every day citizens and focused personnel there is also targeting of foreigners in China. So this can include journalists, but it can also have much more direct

national security implications because it could be used as well to identify, for example, case officers or intelligence assets who need an especially high degree of anonymity.

So China has a particularly broad tool kit and it also uses it very iteratively over the years to add capabilities. So these days, they rely heavily on AI enabled methods such as face recognition, voice recognition. They also to a lesser but increasing extent use things like iris and gait recognition. So these are all biometric recognition tools. And they also increasingly use tools that are enabled by predictive policing to be able to potentially stop crimes before they occur.

So where Sam Hoffman and my work comes into this is that we were looking at things in the sense of a biometric surveillance technology stack. So that very quickly has four layers. The first is the smart devices. The second is data transmission networks so that's like 5G or Wi-Fi networks. The third is the Cloud infrastructure so that's what ingesting and storing the data from the first layer. And then the fourth and that final layer is the Cloud applications which process that data and then conduct analytical outputs.

So while that stack definitely isn't unique to China, I think where China really sets itself apart is the extent to which it has a shared scope of coverage and its reliance on AI enabled technologies. It has a truly nationwide scope in terms of going from urban to rural areas with several different national surveillance programs. And this is something that I just haven't seen matched by any other country in terms of scope.

And the last thing I'll say before passing it on is China also sets itself apart in the sense of how it relies on national standards. So it's codified things like ethnicity recognition. So that implicitly includes Uyghur recognition as well.

MR. MESEROLE: Thanks, Dahlia. That was just a fantastic sort of horizon of kind of all the surveillance technologies as part of China's surveillance state. You know, personally, I have to admit to being a little horrified by all you shared, but hopefully we can talk a little bit and come back to exactly what democratic societies can do to pushback on that kind of surveillance technology.

Before we get to that though, I want to turn to Ishan and kind of hear a little bit more from you based on the great work that you've done on things like responsible surveillance technologies and development. You know, how unique exactly is China's surveillance technologies?

You know, I know that there's a lot of other countries in the world that develop surveillance technologies including even in democracies, right? Like I think Dahlia mentioned predictive analytics for policing. That is something that's happening in the United States and the U.K. and elsewhere. How should we be thinking about, you know, what other states are doing in his space as well?

MR. SHARMA: Yeah, it's a good question, Chris. And thank you to you and to Brookings for the gracious invitation. It's a pleasure to joint Dahlia and Sarah on this panel.

I think the question is partially answered by Dahlia, which is that I think China itself has one of the most advanced (inaudible) to deploy modern surveillance technologies. And so, that allows them to create an ecosystem that is a lot of different and one that is often not really replicable broadly internationally. But that doesn't stop other countries from trying or being sold on the promise of certain types of surveillance tech that that exists from China.

And so, I think the unique advantage of China's surveillance technologies per se is that they are by far the market leader when it comes to surveillance tech. I think they own about 45 percent, 50 percent of the AI facial recognition market. And what that does is the customers that consume China's surveillance tech end up providing data to feed the algorithms themselves, right?

And so, the broader array of customers, for example, facial recognition is historically terrible when it comes to recognizing darker skin faces. If China is able to train algorithms that are more predisposed to recognizing that by, for example, giving facial recognition terminals for free to Venezuela or -- sorry, Venezuela or Nicaragua or other

countries across the world. They're able to develop algorithms that are more accessible broadly.

And so, when you think about the long-term implications for our market states, it is pretty easy for China to take advantage or sell those countries on a dependency on certain types of surveillance that comes from China.

But I think broadly in terms of the difference between democracies and autocracies, I think there's this really interesting book that recently came out from Wall Street Journal Reporters Josh Kin and Liza Lin, which details the model that China is putting forth to the world is one that remakes the social contract. One that offers more security between, you know, a democracy that maybe open or tainted as is more fraught with crime or more open ended and whatnot. And one that comes from China that is more repressive inherently like what we've seen in Xinjiang but one that offers a more state lined model security.

I think that revision of the social contract is appealing to a lot of countries across the world as we consider in the next 10 to 15 years, the second half of the world is going to gain access to the internet. And so, China can find within those market spaces opportunities to sell, for example, as Dahlia pointed out, ethnicities to specific algorithms.

That type of tech is not something that necessarily U.S. firms or lesser firms will peddle though they might, right? And there's circumstances in which they have peddle (inaudible) tech. But that's something I'm really scared about. And I think it underscores the needs to develop a certain alternative social contract one buys for the 21st century.

MR. MESEROLE: Thanks, Ishan. And hopefully, we can get into exactly what that kind of model might look like.

You know, Sarah, I want to come back to you in terms of you did an excellent job just kind of laying the land as far as how nonstate actors are using these technologies. And, you know, how exactly should democratic societies think about countering that? And especially, you know, as I ask that I'm kind of cognizant that we just

heard from Dahlia and Ishan about how authoritarian, you know, uses of technology often under the pretext of counterterrorism have turned out.

So, you know, what are your thoughts on exactly what democratic societies can do to begin to counter these trends?

MS. KREPS: Yeah. It's a great question and I think a really challenging one because, you know, one of the ways and instinctive ways possibly to address some of these threats is almost to take a page out of that same kind of autocratic playbook. You know, so if we have online risks. Well, we're just going to shut those down.

And I think that first and foremost, it's important democratic societies to kind of default still to kind of a free and open society. And then the question is how much of that kind of beyond that once we're sort of making assumptions and hoping that we can maintain that kind of what are the appropriate steps? So that's a kind of normative, you know, prescription is to not revert -- not take some of that autocratic page of the playbook.

But the second is on questions of AI and autonomy, I think there's also a way in which for a democratic society, it's almost impossible now to have you regulate an algorithm? And so, I don't think it's even necessarily feasible. I mean we think about some of these initiatives of NGOs to regulate autonomist weapons on the battlefield. You know, one could argue that that's allottable, but I also think it's a really difficult one to achieve because these are lines of codes. They're algorithms. I think that's really challenging to actually think about -- I mean it's not even entirely clear what that line is between autonomous and semi- autonomous anyway.

So in the report I wrote, I kind of pointed to a different set of considerations not so much trying to put that genie back in the bottle because I don't think it's desirable and I don't think it's possible. But I think there are a couple of approaches that might be more fruitful.

One is for countries like the United States to kind of demonstrate use norms that it would want other countries to emulate. And I recognize that realists would probably

say, well, even if the United States and its allies do not use fully autonomous weapons that says nothing about whether nonstate actors or autocratic countries are going to abide by the same use of force norms as probably the case that they won't. But I think it at least puts us on a solid footing in terms of setting in motion or kind of setting a landscape that other actors might consider following as appropriate.

I think another thing that I talk about in the report that we've seen actually in the last couple of months is with this Chips and Science Act. Is more offending for stem and R&D research. So in this AI space when we think about detecting and deterring emergent threats, AI enabled threats, by nonstate actors. Democratic states can really only begin to address those issues if they can understand that technology and how it's being used.

So I think it's good to see that on the U.S. part at least that there's a lot more funding going into AI research in the stem field. So I think that's another way to think about this is to better understand the technology and along with that I think we'll follow kind of technologies that can help identify, detect, and deter those threats.

MR. MESEROLE: Thanks so much, Sarah. You know, I couldn't agree more on the value of understanding the technology and kind of any solution to these challenges ultimately rooting with greater kind of -- or being rooted in greater technical expertise.

I want to turn now to Dahlia to get your perspective on, you know, again we just saw some great examples of how democratic societies can push back on some of the malicious uses by nonstate actors. You know, you've written on this as well. What are some of the things that democratic societies can do to begin to counter digital authoritarianism of the kind that China has pioneered?

MS. PETERSON: Yeah. That's an excellent question and one that is especially pressing right now. So I would argue that the U.S. needs to work with its allies within existing structures that it isn't really currently leveraging fully.

So I'll give a few recommendations to that effect. But before even any

concrete recommendations, I just think that it is really crucial for both the U.S. and its allies, I think we discussed earlier the use of facial recognition and predictive policing in countries like the U.S. and the U.K. It is really important for all of these countries to be able to demonstrate that they can use AI responsible at home.

So one of the recommendations that I've made in my work is for the National Science Foundation and DARPA equivalence in both the U.S. and other countries to fund privacy preserving computer vision research. So specifically, where the images are automatically pixelated and do not automatically identify individuals unless it is required to after the fact if they actually engage in a criminal act. So that you don't necessarily lose meaningful expectation of privacy the moment you go out.

And this is something that already has precedent to some extent. Some companies have already implemented this in the EU in response to the general data protection regulation. So I think that would be a really great thing to explore further and fund more research in.

And then recently in May there was more -- there was discussion about how there was considerations to put Magnitsky sanctions on Hikvision, the world's largest surveillance company. And I really think that this would be a positive move even if it as expected would inflame tensions between the U.S. and China. I think it would be a very effective complement to existing actions that are placed on Hikvision such as the entity list and investment bands that would really hurt Hikvision's ability to do business abroad.

I believe it makes 27 percent of its revenue abroad. So this could really affect its ability and companies and bank would not want to touch Hikvision if they had Magnitsky sanctions placed on them.

Another thing that I would argue for is for U.S. government and democratic allies and partner governments to support their companies in participating in international standard development organizations. So this would prove to be a very valuable alternative to standards at bodies like the International Telecommunication Union where China has

really taken the lead there and their standards are fast track for approval in broad parts of the world.

But yeah, the last thing I would say is with these standards it is, I believe, important for civil societies organizations to be able to take part in some way since they have a very good sense of how the ethical and human rights impacts of these technologies work. And yet, these standard development processes are very much a closed-door process. So that's where I would make a few recommendations to that effect.

MR. MESEROLE: All right. Thanks so much, Dahlia. You know, I want to kind of latch onto the point you made about democracies needing to be able to demonstrate responsible use of AI and other technologies at home first before they start to counter others.

Ishan, you kind of actually just wrote a great piece on that in the Bulletin, I believe. And would you mind just kind of talking. You know, picking up on some of the comments made earlier as well as kind of Dahlia's contribution about, you know, what some democratic alternatives are to the surveillance state and how they can use these technologies responsibly?

MR. SHARMA: Yeah. Absolutely. Thanks, Chris. So I would say the largest challenge for democracy in architecting somewhat alternative to the very scary civilian state of, you know, if you would put China as the end of the spectrum. Is creating a system that is immune to mission creek. And what do I mean by mission creek?

Well, I mean architecting -- when you design a system that empowers certain agencies or certain law enforcement officers to be able to have this as the wording. You know, that authority is very amendable to being corrupted down the line a visa powered down the line. And so, you know, thinking with foresight of how do you design a system that is immune to that? Is actually just really difficult.

You know, a lot of systems we've seen from across the federal government to date end up getting quite corrupted. Whether it's in the immigration sphere or it's in the

prison program or especially in the surveillance context. And so, I think the piece that I wrote recently is really trying to take a very bottom up, middle out approach to designing what this surveillance state should look like. Or what sort of alternative to the surveillance state should look like in democracies.

But what I think what it really homes in on are applying principals rather than just talking about ideas of transparency, proportionality. I think I spent a lot of time trying to think about the local context with law enforcement officers and state and local governments. Folks that I had a chance to interview a few years back in the sort of larger report. What does surveillance look like there?

And if you think more extensively what is the model version of democratic surveillance look like? I think, you know, there's four principles. One being transparency, right? Like citizens should never have to worry about who, what and where they're being surveilled. I think another one is proportionality, right? Like if you were deploying the most intrusive types of surveillance tech but in the most medial types of crimes, I think that's a real problem.

The other is enforceability. A citizen should have an opportunity to be able to engage in public platforms that holds officials that are deploying the surveillance tech accountable. They should know, for example, what surveillance tech is being purchased ahead of time. Be involved in the discussions at the outset.

And then the last one, I think is perhaps the most important which is intersectionality. I think the idea and the story that you asked -- and I'm sure in plenty of other places abroad are that minorities have borne the brunt of surveillance, right? Surveillance effects everyone not just equally. And that makes those particular communities be the best experts to design a system immune to mission creek.

And so, those specific folks should be brought in to whatever extent they're willing into discussions about designing those types of surveillance systems. And in terms of moving from those principles to actions, I think there's a few things, right? You know, it's a

lengthy list on my wish list, but I wanted to call out is this model for community led surveillance ordinances, which essentially provide -- well, zooming out across 15 U.S. cities, you know, like Oakland, California, for example.

State and local governments have made good on their promise to engage communities. Engage their citizens before they deploy a surveillance tech, before they purchase a particular type of surveillance tech, involve them on discussions such as like, you know, what is the intended use case here? Is there a particular community problem we're trying to solve by buying this tech? Is that something that we all collectively agree on as a priority?

And then that body, that sort of independent citizen led oversight body stays on to evaluate whether or not those surveillance technologies exist and are actually meeting their goals as initial tech. You know, that juxtaposed to the status quo. And the research I had done about two years ago, which involved speaking with over, you know, 40 different state and local police officers, folks from the ACLU to Palantir Tech, a wide variety of multistakeholder interest groups that Dahlia very much really kind of helped us write.

And the takeaway was that in the U.S. we're not leading by example at all. The main takeaway actually is the version U.S. is espousing in terms of surveillance or a model of it is best described as a wild west without any transparency and oversight over how law enforcement deploys this tech. So as Dahlia pointed out if we're really going to expect other countries to be responsible in how they deploy surveillance tech, we have to get really specific at the state and local level about what leadership by example looks like.

And I think these surveillance ordinances are a big component. And then I know -- I'll just end with one other recommendation which is, you know, the Chips and Science Act called out by Sarah and the brilliant recommendation by Dahlia to sort of marry work ongoing with NSF and DARPA in terms of advancing computer vision I think is so, so important. And I think one that is particularly useful and timely now given the CHIPS and Science Act which created the National Science Foundation's sort of new directorate for

technology, innovation, and partnerships.

The idea is that it's really great to have this research. But what the Chip director focuses on is taking that research and scaling it to the market place. And so, that, you know, the more in which we can introduce more regulated types of algorithmic development and bring that to scale so that surveillance vendors in the West can easily deploy those within their own systems. I think the better will see the results and the (inaudible) those are the investments into, for example, the research side.

MR. MESEROLE: Thanks so much, Ishan. You've clearly done a great job of kind of laying everything out because the audience questions are coming fast and furious. We've only got a little bit of time left so I'm actually going to bend a few of the questions that we've gotten.

One just kind of picks up a little bit. I'm going to adapt it slightly. It's about emerging kind of developing countries. So countries that are not China or the kind of the countries in the global south outside of China and the United States or Europe and their capacity. Like you just mentioned, for example, kind of local ordinances in a variety of ways that governments can use these technologies responsibly. Can you speak a little bit to just how scalable that is globally as opposed to just in the U.S. context?

MR. SHARMA: That's a great question. This is something that I think is an exciting area of research and one I hope to spend more time doing. But I think there's one specific example I call out in Nigeria, which in the last two years there's been an emergence of community led policing efforts.

Initially, in the area of, you know, there is these -- it's called local community police officers, which serves to in an ad hoc way provide information up given security breakdowns that the region is facing. And so, what I would propose in this context and something I had written about in the recent Bulletin piece is some sort of coordinated effort from the Summit of Democracy participants that are engaged in this particular issue to negotiate with high level but also provide frameworks at a local level for what would sort of

be community level transparency or surveillance ordinance model look like translated abroad.

At the fundamental level, it is about things that are transferrable, right? Having more engagement from communities. Having transparency, you know, having posted signs, for example, as like a really easy physical way to track what this model looks like. That doesn't really solve all the problems, right? And certainly not when, you know, epic tensions breakdown and you have, you know, sort of this capture of the system itself or mission creek.

But I think having some sort of coordinated engagement from the subject democracies to analyze where countries that have these emerging principles like in Nigeria might be amendable to adopt to the model. That would be a pretty high leverage line of effort for the Summit of Democracy participants to take as a next step.

MR. MESEROLE: All right. And thanks. And maybe at the next summit, we can do another event like this right beforehand and you can share a little bit more about that.

The other kind of set of questions are also concerned what the U.S. had done lately. There's been the Science of Chips Act. There's also been new found export controls. There's been discussion around, you know, outbound investment screening and inbound investment screening.

Sarah, and Dahlia, I'm going to just kind of turn to each of you, I guess, in turn. Are those kinds of, you know, whether it's on the Chips Act on the one side and the investment that it's providing on the one side or kind of the constraints that some of the new export controls have provided. Are those the kinds of things that the U.S. government should be engaged in? Or are there things that the government should be doing that you'd like to see more of? And I guess I'll start with you, Sarah, and then move to Dahlia.

MS. KREPS: Yeah. I mean it's a great and very complicated question, of course. I mean if we think about the case of semiconductors this is like just pivot away, but

either 500 different steps in manufacturing, you know, a chip.

And many of them are in different places. And so, you know, I think that some of this emphasis on reshoring, for example, follows a broader pattern that we've seen. Kind of an anti-globalization backlash in the last few years where there's a real bipartisan interest in kind of, you know, made in U.S., bring jobs back home. But I do think there is a risk of overreach there which is that the same kind of export controls that are intended to, let's say, hinder China's development can also have the effect of hindering our own American industry because these steps are all kind of interdependent.

And kind of further, it looks like in many of these cases, China is developing this technology whether we have the export controls in place or not. And in part because there's a great piece in the Wall Street Journal a couple of weeks ago that said that most of these export controls are being circumvented anyway. And so, it feels like a real case where there's a lot of politics going on which doesn't, you know, may not come as a surprise.

But I think there are many, I guess it speaks to this question of whether these export controls, A, are effective and, B, actually might be counterproductive. And so, I'm a bit weary of those and I think in this context, you know, as I've said in other Brookings' pieces.

I think there are other approaches like kind of a tech alliance where we are either friend-shoring, near shoring these kinds of measures that can try to take advantage of some of comparative advantage, not trying to do everything at home which probably will increase the cost of all steps of this but actually be more effective as well. So, yeah. The long and the short of it, I'm weary of some of these measures.

MR. MESEROLE: Dahlia, how about you? I know that there's again kind of a discussion about in different for about how to counter digital authoritarianism and this idea of kind of denying them access to certain kinds of semiconductor capabilities has been one of the proposed solutions. Is that something that you kind of -- or kind of adjacent sort of policies -- is that something that you would as integral kind of plan to pushback on digital

authoritarianism globally?

MS. PETERSON: Great. So I definitely think that the moves that the U.S. government has taken to date with placing over 20 different companies and public security barriers in Xianjing, for example, on the export control entity list. I think it is commendable but as Sarah said there has been a fair amount of coverage that really questions its effectiveness and the degree to which loopholes exist for these Chinese companies to continue accessing these technologies.

Supply chain data is remarkably complicated and difficult to get clear access to. So this is one question that I have repeatedly had is just how well the entity list is actually working? And to the extent that it is possible. I continually advocate for either the Commerce Department which is running this entity list or the State Department or through some interagency process release some kind of public report that for public credibility messaging purposes details how well these actions have worked or not.

Because this has been something that has been ongoing in both the Trump and Biden administrations, and it is just simply not very well known to the public if these efforts are really stopping China's surveillance efforts because on the surface it doesn't look like they are.

And another thing I would say is like even with those major companies on the entity list, there are still just thousands of surveillance companies operational in China and many of them active in Xianjing. And it is not possible, not feasible to put all of those companies on -- subject them to export controls.

So I wouldn't advocate for not putting companies on the entity list, but it is good to be cognizant of that they may potentially not have as positive effects as we may hope. One thing I would add in the sense of the investment bands is there was this very strange host that came up, clarification from the Treasury Department that said that after the one-year divestment window, there's no further action that you could take.

So in effect, if you didn't really do anything in that one-year window, you

could still be holding shares and you would basically be forced to continue holding. And I just found -- my colleagues and I found that to be a very odd clarification and not really sure why that policy exists from the Treasury Department. So that is one thing that I would love to get more clarity on and what the goals were behind the investment band if you cannot take any further action after that one-year window has passed.

MR. MESEROLE: Thanks. And if anyone in the audience is a member of Treasury, please be in touch. We'd be curious to hear exactly what that was about.

I think we have time for kind of one more round of questions. The question that just came in was actually about standard setting. And, you know, I guess on a more affirmative note. I guess now we talk about some of the export controls and entity list and whatnot. You know, how optimistic are each of you?

And if we can kind of start with Ishan and then go through the whole panel about the notion of improving digital surveillance via places like the ITU or just even more broadly in the less formal sense just developing norms around the responsible use of surveillance technologies?

MR. SHARMA: Yeah. So not to bring it back to export controls but I think I will loop there. So I would say that I think the fundamental issue that we suffer from on an international agenda setting effort is one of information.

Often times, you'll have western firms like the NSO group from Israel sort of pass the notion that there's no possible way we can be responsible for what the end users of our technology end up doing. Like there's no way we know and can know. And I think that's fundamentally false, right? I think that there is a line of effort to be had that raises both the accountability but also the technical understanding of how surveillance technologies are being used.

There's this really interesting response to Bureau of Industry and Security RFI in 2019 from Microsoft, which essentially advocated for the idea of having technical firewalls that can sort of walk surveillance technology's use in cases of (inaudible), right?

And so, that's like a really interesting underexplored, high leverage R&D question on is it possible to sort of scale the types of oversight mechanisms from a technical lens and use that as a way to collect more information?

That we are getting really specific in setting these global standards on which countries or which firms within countries are, you know, sort of at the forefront of, you know, peddling abuses abroad? You know, there's this notion that, of course, it's China, right?

But there's also this deeper notion that like, you know, the West has been responsible for, you know, facilitating a lot of human rights abuses abroad to the export of different types of firms. And, you know, the defense from those firms is like we won't, no. And so, my response to you would be, you know, if there's a world in which we can get more specific about these technical firewalls and get more information, I think we'll have a much better ecosystem going forward. But I agree sort of with my colleagues that this sort of the bludgeon of export controls right now isn't really to just naming entities doesn't really seem particularly useful or sustainable going forward.

MR. MESEROLE: That's a great point. I think just very quickly. We'll actually I think we're basically out of time. So I think I'm just going to pause here and just kind of thank each of you for a really just tremendous conversation around this issue of what to do about digital authoritarianism on the one hand and then also just the exploitation of digital technologies by nonstate actors on the other.

Clearly, we could continue the conversation I think probably throughout the rest of the afternoon and evening. And hopefully, in the future we'll have ample opportunity to engage in this discussion further. But in the meantime, I just want to thank you each for this. I want to thank the audience for joining us this afternoon. It's been a long series of rich discussions for about two and a half hours now so thank you for joining us.

And then finally, I want to give a really great just thank you to the ITT at Brookings and the tech team at Brookings for their intrepid and brilliant work as always and letting us hold this event. So thank you to all and thank you as well for a great event. Take

care.

* * * * *

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