THE BROOKINGS INSTITUTION

WEBINAR

THE SOCIAL MEDIA WAR IN THE MIDDLE EAST

Washington, D.C.

Monday, January 24, 2022

PARTICIPANTS:

DAN BYMAN, Moderator
Senior Fellow, Center for Middle East Policy
The Brookings Institution

AFEF ABROUGUI
Researcher
SMEX

DINA HUSSEIN
Counterterrorism & Dangerous Organizations Policy Head
Facebook/Meta

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

ALEX SIEGEL
Assistant Professor of Political Science, University of Colorado at Boulder
Nonresident Fellow, Center for Middle East Policy
The Brookings Institution

* * * * *

P R O C E E D I N G S

MR. BYMAN: Hello everyone and welcome. My name is Dan Byman. I'm a senior fellow at the Center for Middle East Policy at the Brookings Institution and a professor at Georgetown.

As everyone watching the session knows the Middle East has long been an area of both conflict and competition with states meddling in the politics of one another, trying to destabilize one another and otherwise engage in very fierce efforts to try to weaken rivals. And it's not surprising that this competition in recent years has spilled over into the social media realm. And we've seen extensive efforts of mutual governments to use the tools against each other and against their own internal opposition.

And I'm delighted today that we have a fantastic panel for you to discuss this problem and to discuss ways that the situation might be improved. I'm going to be very brief on the introductions of our speakers. What I would note is that we have the full bios available on all the speakers at the event page at the Brookings Institution's website and I urge you to see them really amazing set of accomplishments our speakers have.

Our first speaker is Dina Hussein of Facebook. She's the head of counterterrorism and dangerous organizations for the Europe and Middle East and Africa. I would like to point out that Facebook and Meta, excuse me, provides generous support for the Brookings Institution's China program and helps make the work we do possible. I would like to reiterate Brookings' commitment to independence and underscore that the views expressed today are solely and only of the speaker.

She is joined by Alexander Siegel. She's a nonresident fellow here at Brookings and a professor at the University of Colorado and has done extensive research on social media.

We also have Afef Abrougui. She is a researcher who has done considerable work with society in the region offering assistance to mission, individuals and organizations in their efforts in this space.

And our final speaker is Chris Meserole. He is the director of research of the

Artificial Intelligence and Emerging Technology Initiative at Brookings.

So let me kick things off with Dina. Can you set the stage for us please? And can you tell us what Facebook is seeing in the Middle East and North Africa region with regard to malign state activity? Hussein

MS. HUSSEIN: Yeah, absolutely. First off, I'd like to thank Dan and Chris and the Brookings team for the invitation. It's always such a pleasure to engage with you all in this kind of dialogue.

As Dan mentioned, we have been covering all of -- a good amount of work in the Middle East because my team covers the globe, but I specifically had Europe, Middle East and Africa. And I can speak to the work that we've been doing over the last three years. Where we've seen the evolution of the utilization of social media by states has really stemmed from the fact that they are now able to understand the inner workings of both the tool but the policies at play as well behind these social media platforms.

So I'm going to start off by just giving us a very brief intro to the way that our policies work. Our policies are really built around two things. Content and behaviors. And as there has become an evolution of the understanding of that two-fold approach, we've seen that state actors have abused the platform when it comes to content in that they are showcasing and sharing information that might not be accurate or pushing forward info ops at a larger scale that we had been seeing beforehand.

We're also seeing that when it comes to behaviors, things like account integrity exploitations and just hacking more, purposefully locking somebody out of their account has started to peak a little more. We're also seeing the coordination as inauthentic or slightly authentic behavior on the platform as well that is state backed.

And then finally, something that is obviously at the forefront of all of our minds. It's contracting of private actors that are then doing or taking on malicious activity on the platform or in certain cases, and this is applicable across the globe, but does manifest in the Middle East. Utilizing jurisdictional legal vagueness in order to get platforms to legally remove content, which

is another way that we're seeing this.

So it's four different types of abuse, but they're manifesting in very interesting ways.

MR. BYMAN: Great. Thank you. That's a great overview to begin our conversation.

Alex, can I turn to you? I know you've had states in the region and have used social media to target their own opposition among others. Can you discuss how effective this has been?

MS. SIEGEL: Sure. Thanks, Dan. And again, thanks to the whole Brookings' team for having me. It's great to be here today. I think the way I think about this is sort of what are the levers of control that are available to states on these online platforms?

And I think Molly Roberts of this very useful framework where she talks about fear, flooding and friction. And I think a lot of the specific instances that Dina brought up so nicely into these categories. But if we start with fear that encompasses things like both surveillance of opposition and everyday citizens as well as the use of physical repression to curve online dissidents. A lot of this is done under these really vague cybercrime laws. And there's kind of two dimensions of this, right?

One are the laws within each country. So just to give an example of what the language involved in this kind of legal infrastructure looks like in Saudi Arabia. This is the idea that people could be jailed, for example, for posting any content that, quote, unsettles the social and national fabric or any actions that touch the unity and stability of the kingdom under any reason and of any form, right?

So you see how vague this language is. It just instills this kind of underlying sense of fear that people could be and are prosecuted and physically repressed for their online activity. There's also kind of interesting developments around using the language of Western platform content moderation in the legal infrastructure in these countries.

For example, accusing opposition after this of spreading misinformation or hate

speech and using the kind of very language that you often see in platform and policymakers using to try to keep platforms safe against opposition and to target opposition.

On the flooding side, this is where the coordinated and authentic activity that Dina was mentioning comes in. And here the idea is that rather than censor opposition language or activity on the platforms, regimes can either produce their own bots, trolls, soft puppets, other kinds of inauthentic accounts or hire them. We've seen this kind of explosion of digital mercenaries or sort of disinformation for hire kind of outlets cropping up that are used to flood the online environment and drown out opposition voices.

And then on the friction side. This occurs both at the infrastructure level but also at the network level. The idea that regimes can restrict access to the internet itself to specific platforms or to content. And I think on the one hand, we think of this as sort of an older blender approach that we saw in the early days of the Arabia spraying on the region, but it's still going on today. Some recent examples include Egypt throttling access to Facebook during 2019 and 2020. Protests, Jordan had some national internet shutdowns and restrict Facebook live during recent -- a teacher's union protest.

And we've seen a lot of sort of larger scale internet shutdowns in Yemen both by the Houthis and more recently we see in the Saudis actually targeting telecom infrastructure to silence information coming out of Yemen.

So these kind of three categories of fear, flooding and friction, I think do a good job of laying out kind of the authoritarian toolkit. And I'm happy as we go on to talk about the success of these different approaches, but what we often see is, I think at the same time, regimes advance their ability to control online information. Opposition actors also find new ways to use the tools to achieve their goals.

So I hope today we can talk a little bit about kind of the back and forth there as well. So thank you so much.

MR. BYMAN: Thank you, Alex. That's actually a crocked segue to Afef whom I'm going to ask basically that question, which is can you discuss how some of the society actors

view this sort of state activity in attempts to whether it's influence or surveillance?

You know, how does this affect their efforts? And what have they done in response to these aggressive campaigns?

MS. ABROUGUI: Thank you very much, Dan. So basically, of course, the use of these digital oppression tools and tactics including surveillance and disinformation and malicious campaigns online is a constant threat that civil society organizations and human rights defenders in the region have to gravel with.

And that's how they see it. It's this existing threat and risk that they need to continue graveling with while trying to continue to work in a very repressive and authoritarian environment.

And the way it has been affecting their efforts, it's based -- I'm going to talk a little bit about surveillance because it's been covered a lot lately in the news and particular the use of the NSO spyware that has used several governments in the region to target the civil society organizations, to target their opponent's dissidents. And most recently frontline defenders published a report where it under covered the use of that spyware by the (inaudible). And Jordan's target of women human rights defenders.

Surveillance in particular has a chilling effect because it facilitates the gathering of very sensitive information that these civil society organizations hold. Sensitive information that could be about the people that work at their own organization and who may not want to appear publicly that they are associated with such organizations because it's a very, very risky environment.

But also, gathering information about witnesses, about sources and using also some of that information in sham trials, but also to target these organizations either online -- in online campaigns, but it's also in the mainstream media.

So what we -- in the past -- I mean years like with the proliferation of these spying and surveying campaigns and combined like these tactics combined with the offline tactics including the traditional harassment. But also, imprisonment of activists and the

restrictions on their rights and freedoms that are essential to their efforts like freedom on expression and information. But also, the right to process, the right of -- the freedom on assembly and association.

These tactics have contributed greatly to the shrinking of the civic space in the region. And in some cases, it's decimation.

In terms of -- so these are the impacts in terms of how they have been adopting. So a little bit about how just the rights organizations have been trying to support CSOs to adapt because this is where the (inaudible) that I have. I work as just to rights consultant and researcher with the social media exchange and just rights organizations with the region.

And in the past year, what we've seen, we've seen an interest from organizations, (inaudible) and others in providing digital security support to these organizations to help them deal better with these threats. Either in terms of detecting these attacks, detecting breaches in the technical threats but also in terms of providing emergency support to deal with such threats.

And the other tactic or the other way that these organizations have been trying to support CSOs in the region was to try to respond to manipulation contents but also to harassment of individual activists and try to coordinate with social media platforms to address these types of campaigns and threats.

MR. BYMAN: Thank you. Thank you very much. Chris, let me turn to you to kind of broaden this discussion beyond the Middle East. You've looked at global trends in this space. The terrorism side, on the visual authoritarianism side.

And could you talk about how you feel threats in this region are different or similar to broader events you see around the world?

MR. MESEROLE: Thanks, Dan. And thanks to all the great panelists for their time and comments as well.

But I think, you know, I would build up what they've been saying to kind of try and contextualize this within a broader trend which is that most of what we're seeing in the

Middle East is actually part and parcel with much, you know, much broader issues related to digital authoritarianism and kind of the way that states, and particular authoritarian states, are leveraging and exploiting online spaces.

And so, the two kind of -- the most prominent states in that regard are definitely Russia and China. And I think in two ways they've really kind of pushed forward with new ways of state control and developing ways in which regimes can exploit and leverage, you know, the digital platforms for, you know, greater social stability and control within their countries and even abroad.

And I think one of those is surveillance which Afef did a good job, I think of laying out. These tools provide -- especially if you couple them with social media. They provide a really easy way -- or easier than any kind of prior technology has made it possible for states to identify and track and monitor folks who might have this net use or who might be, you know, developing viewpoints that the regime would view as threatening to them and their continued survival.

The other kind of piece of this. Since the Afef did a great job of kind of laying out the surveillance side. The other kind of pioneering work that a lot of -- that Russia and China in particular have developed is kind of this notion of influence operations both domestically and abroad. And, you know, Alex kind of laid out a bit of this when she was talking about flooding and some of the other types she described.

But I want to make one broad point which I think is really critical to understanding what's happening in the Middle East and ties to these global trends. Which is that, you know, we've had propaganda for a while. That's not something that's new. What is new with these influence operations is that they're participatory in nature.

And I think people misunderstand exactly what these campaigns are really trying to do. They're not -- the point of kind of pushing out a conspiracy theory or pushing out kind of even something that's maybe a little bit more mainstream, but it's not necessarily on the fringes. Is not to change somebody's mind, it's to instead to encourage people to, you know,

effectively confirm their own biases.

And so, you know, when you have these online spaces where people are able to kind of comment and like and be tweeted, et cetera. The more you can inject or strengthen narratives that you find conducive to your own strategic interests, you know, the stronger you will be in terms of how you're able to operate on these platforms and how you're able to recruit support both domestically and abroad.

And I think where this kind of plays into the Middle East. We've already seen it happening, for example, you know, when COVID came out. You saw, you know, procedure-Iranian accounts kind of saying that COVID was like a creation of the U.S. and that it was kind of -- it was like literally like they had it to like Trump as the crusader, that narrative.

And I don't know if they were really changing anybody's mind about, you know, their view of the U.S. or kind of what was happening in the region. It was instead kind of confirming longstanding narratives with a kind of new twist. And getting people -- important in getting people to participate in that narrative.

And I think the, you know, one of the most interesting things about it is from the flipside of this is what to do. You know, what can states do to clamp down on this kind of behavior? And this is where it gets a little bit tricky because especially in authoritarian regimes or areas that are not fully democratic. There actually are uses for these platforms within their countries, which is why they are actually reluctant in many cases to shut off access completely to the domestic internet and to domestic services. Or kind of to the access to, you know, platforms like Facebook or Twitter domestically. Because they gain value from it, but at the same time they're aware that kind of, you know, if you're Saudi Arabia that Iran might be implementing narratives domestically that you don't like.

And one of the things that they're starting to do in addition to kind of restricting access or -- you know, because they're reluctant to do that fully, is, for example, not only leveraging kind of platform's policies but they're starting to pass even new legislation.

Like Turkey, for example, is trying to pass legislation requiring foreign

companies, foreign social media companies, to locate personnel within the country. And they're kind of effectively turning employees of some of these platforms into -- you know, this maybe undiplomatic. But they're effectively kind of turning them into hostages almost in order to pressure the companies into doing -- you know, into monitoring platform in the way that they would like.

Which is a, you know, a more targeted way of going out there in their view. That's what's happening on these platforms without necessarily cutting them off all together. And so, you're starting to see kind of a lot of experimentation with different ways beyond just crude instruments of just we're going to shut the internet off or we're going to shut Facebook off.

Ways in which states are able to maintain the benefits obviously of these platforms while also restricting, you know, the abuse cases that they're concerned about. And hopefully, we can talk a little bit more about that. But I think it's a really alarming trend that I think has come up in the last year or two that is one, you know, policymakers in the U.S. and abroad should really be focused on.

MR. BYMAN: Great. And thank you, Chris. And thank you really everyone for really laying out a large variety of issues. I want to follow up on some of the remarks made.

I want to start with both Dina and Afef on a very basic question of given this abuse and the kind of dangerous threats to activist and the broader problem that's being created. You know, how are social media companies like Facebook trying to handle this?

And then, for Afef, I'd like to ask are there additional things that you would ask these companies to do to be able to protect activists and to ensure that there's better online discourse? So, Dina, let me start with you and then go to Afef.

MS. HUSSEIN: Sure. Thank you, Dan. So I would describe this as a three-fold way of addressing these kind of challenges that we're facing.

The first for us really is from an outreach perspective. As we mentioned, a lot of the work that we're seeing or a lot of the work that we're doing really in addressing who is being targeted, the methodology of targeting and then as a third (inaudible) stream of work is

addressing that legislative environment that might be hostile.

But the first portion of our work really is outreach to the individuals or the communities or the organizations that are being targeted. When we are aware of any sort of malicious activity, we're trying to give our -- the human rights activists on our platform tools in order to securitize their presence on the platform.

Now, again nothing is perfect. And we're working to develop more tools, but we've applied this not just to the Middle East. We've applied it in Afghanistan during the Taliban takeover. We've applied it in sensitive areas like Syria and others. That's the first portion is the outreach to the communities and individuals targeted by it.

The second portion of it is operational. So we've built out tools that both through manual review but also through automation are able to identify malicious action. And we've done that to address both types of ways that these manifests. So if it's content, we're able to do this on an automated level a lot faster. So we've got automation that allows us to find piece of content that we have found to be malicious in some way, shape or form or sharing of disinformation. And we're able to backtrack and find who sharing it, which then leads us to the individuals and the networks and the behaviors.

And then a team on our trust and safety pillar that is led by Nathaniel Gleicher and I have colleagues on there like Olga Bulgova (phonetic) who are experts in identifying these kinds of disinformation operations and blocking out the entirety of these networks in one fell swoop.

And then finally the very last portion of this that Chris did touch on is we are constantly facing these new legislative challenges. And the way to address that from my perspective really is leading into transparency from our side. So one of the things that I am always very surprised a lot of people don't know about, but I'm always very happy to shed light on is we started to try and hold ourselves accountable to be more transparency. But the governments that aren't engaging with us.

So if you haven't been able to reach out and check out Facebook's

transparency center, you'll find that there are two very useful resources. One, the government request for user data, the resource. Where we share the number of requests that we get from each government. But we also found that there is a really very specific type of way that certain governments go about this by restricting things through their own WADs.

And so, another tool that might be useful to you is the content restrictions based on local law tab and not transparency side. And that allows us to not just share what we're doing but also shed light on the kinds of questions and requests that we're getting.

Now, in an ideal future, we'd have transparency from governments as well around how they're defining the kind of very opaque cyber laws that Alex very rightly highlighted. But for this -- at this point in time, we're trying to do our best to share transparency. So really it's that three-fold effective outreach from an operational perspective, securitizing everything and then being very transparent.

MR. BYMAN: Thank you. Afef, I think I had ask you to follow up on this please.

MS. ABROUGUI: Yeah. Sure. So I mean there are a few thoughts or a few ways that social media platforms can do a better job in trying to deal with these types of threats but the factual side of organizations.

The first is to really do like a better job when it comes to prioritizing these types of campaigns that targets people's sites, organizations but also vulnerable communities like individual activists, individual women, human rights defenders who may not have -- who may not be associated with a certain organization that may help them to reach out to platforms and coordinate with those platforms.

I had once a conversation with a woman activist who was being impersonated on Facebook. And when she flagged that page, she got a response that that's a public personality page and that it cannot be taken down because she's a public personality. So that's one area. So there is a need to really prioritize these types of reports and to maybe coordinate more with other organizations in the region to try to tackle these types of campaigns.

But also, to prevent abuse of flagging mechanisms. And this is something that

has been going on for a while. Usually these mechanisms can be abused simply to censor or to silence certain activists or a certain group. And so many users would be using this perspective just to silence them to get the context. They take it down.

And that's also important when it comes to content. Moderation is to pay attention to the sociopolitical context and to try to put in more human resources and train the content moderators about human rights, about how to moderate content in a human center way and in the right center. With the human right center approach to protect the rights of civil society. Organizations, those working in civil society organizations but also with activists.

The other two thoughts is it's very important to push back on government demands. And but also to conduct due diligence. I mean social media platforms or technology companies are really interested in expanding their operations beyond Western Europe and beyond North America. And there is an interest in the regions specifically the Gulf region, for example.

Recently or last year, Google announced a Cloud region in Saudi Arabia. And that raises so many questions about how the data that's going to be hosted in Saudi Arabia -- how it might be abused by the Saudi government? It's really important that companies are transparent about the due diligence that they take on that. If they conduct any due diligence when it comes to launching new products or services in the region.

And the other point I wanted to share is automation. Automation like, of course, can help platforms and companies deal with these types of conflicts a lot. But we have to remember that a lot of these tools are not really trained in the context of the region, but also in the languages of the region. And that can result in the removal of censorship of certain content that should not be taken down. While at the same time, hateful speech or disinformation campaign would remain online.

So it's very important to test these algorithms really while -- and to train them well, but also to be transparent about how these technologies work and to make sure to provide users with appeals mechanism to appeal those decisions that platforms take.

MR. BYMAN: Thank you. Alex, one thing that you kindly offered was to discuss effectiveness of big WAD. And I'd love to hear your thoughts on what you feel is working. And also, if you feel there are certain methods that are not as effective as outsiders might think.

MS. SIEGEL: Sure. So I think sometimes it feels like kind of a strange framing to be talking about, you know, almost giving authoritarian regimes a roadmap, right, for what tools work for repression or not, right?

So I think one way to kind of flip this around is to center it on activists and opposition. And talk about sort of resilience censorship and resilience to information control.

And I think one of the kind of perhaps counterinitiative dynamics that we see a lot both with censorship of online content but also sort of physical repression of activists for their online activities. Things like arrests or in some cases even torture in the region is that often these are more severe and obvious forms of online and offline repression generate a great deal of backlash.

And even people who might not have been as politically engaged with these kinds of issues or politics at all. Upon seeing, you know, well-known activists with hundreds of thousands of followers get arrested for their online activity and may be sort of engaged in and brought into the dynamic.

And Jen Pan (phonetic) and I have some work on this where we find that pretty systematically following the arrest of well-known activists and their subsequent release from prison. While the activists themselves are sort of diminished their political criticism and online activity for kind of every day social media users that we found on Twitter. We observed some backlash with either increased searches, search volume in Saudi Arabia, for example, for these activists on Google trends as well.

So sort of a public and private dimension of interest and in a variety of other context. Past research suggests that more obvious forms of censorship of any sort of online content often draw more attention to the very content that regimes themselves maybe seeking to hide.

I think the place where we've seen less sort of systematic research is around the chilling effects of surveillance, but there's certainly kind of anecdotal evidence and I think that, you know, many who have been targeted by these operations report big changes in their behavior and a lot of fear. And I think especially is that kind of transnational that I mentioned of this that have been mentioned, have really upped the level of fear and the potential chilling consequences of surveillance when we talk about, you know, like the Pegasus spyware and other ways of really tracking the day-to-day activity of well-known activists and opposition figures.

I will say at the same time being an activist or known opposition figure in these context is a very dangerous, you know, and scary sort of activity and brave sort of activities to be engaging in in the first place.

And so, you know, it would be interesting to hear more from the Afef and from others about how kind of surveillance or the authoritarian use of online platforms changes this calculus from just the day-to-day realities of being an opposition or activist figure in an authoritarian regime.

MR. BYMAN: Thank you. I'm going to switch things over in a few minutes to take some questions from our broader audience.

But before I do, I want to ask Chris one final question from me which is a lot of what we're talking about today is traditionally the realm of government. That it's actions by state some hostile to the United States and its allies. Some allied to the United States and its allies.

There's a tremendous role for the broader, I'll say, European Union policies, your national community in general. What should the response of democratic governments be to all of this? Whether it's regard to social media companies or helping activists? How do we think about that big question?

MR. MESEROLE: That's a major question and I think there's a couple of things I'll say to it.

You know, on the one -- the first one I would start with is actually ask what they

should do and more of what they shouldn't do? And that is, you know, there's a lot of pressure and kind of conversation that we should start to fight fire with fire. And I would really push back on that particularly when it comes to information operations and influence operations.

I don't think democracy is when -- even if you can get an advantage in one particular local context or something like that. I just -- I really do not believe democracies win in the long term if we undermine the idea of truth and we undermine kind of legitimate political discourse. Whether it's, you know, domestically or abroad.

And so, the first point I would make is despite kind of, you know, certain kinds of political inertia that might push democratic countries to think more open mindedly about some of these more aggressive information operations. I would really push back on the idea that that's the direction we should head. If we're worried about Iran or China or Russia or the Middle East, Turkey or Saudi Arabia and how they're using some of the platforms, I cannot, you know, emphasize strongly enough that we should not go in the direction ourselves.

What we can do I think is to support through, you know, both diplomatically and, you know, diplomatic levers and just kind of technical levers, you know, those civil society groups on the ground that are kind of at the front lines of this issue. And that, you know, tech companies themselves.

So, you know, one example would be, you know, I mentioned earlier some of these legislative proposals that are being put on the table in places like Turkey. Countries that may not be fully authoritarian but kind of have some democratic process. I think we have some leeway as a country to kind of push hard on, you know.

I think with a country like Turkey, I think we could exhibit some leverage or use some leverage to push back on these kind of proposals about, you know, mandates that countries have domestic employees kind of that the government can, you know, arrest if they don't like certain kinds of content or kind of if they want changes to content or moderation policies on type ones.

I think the government can play a more aggressive role in pushing back on

some of that. Whether it's, you know, in the Middle East or elsewhere. You know, Russia would be the other kind of big example of that at the moment.

The other thing that they can do, I think would be to strengthen some of the -- at a more local kind of level where it kind of even further upstream in the tech stack. You know, strengthen the ability of civil society organizations to operate outside of the surveillance capacity and capabilities of some of these really powerful states.

And so, what I mean by that is investing, frankly, in an encryption and, you know, certainly I'm not trying to undermine it but actually kind of actively strengthen those technologies which, you know, I realize that some of them are controversial because they are, you know, other considerations and there's other stakeholders within democracies that might say, you know, we need to kind of weaken that encryption because we need, you know, greater access to certain kinds of information that could contribute to kind of public harm.

But I would say on in the aggregate we really need to do a better job of creating channels in which dissidents can actually communicate with each other effectively outside of the surveillance apparatus of, you know, powerful states. And so, I would say, you know, if we're concerned about NSO leveraging, what's that for other kind of end and encrypted applications?

We should really double down and make it as hard as possible for those kinds of states to use that kind of technology. So that's kind of those other things that they could do too. But those would be my big kind of points. One, you know, don't fight fire with fire. Fight it with, you know, the core values. And two, kind of invest in the technologies that will allow people at the frontlines to really effectively operate outside the surveillance capacity of authoritarian regimes.

MR. BYMAN: Thank you. I'm going to switch over to some of the questions we've received from the audience.

And I want to start with a question from Moseyed (phonetic), which was really asking about some of the expertise that is helping a number of these governments, that I agree with you around others, are they drawing on foreign governments for help? And in particular are

they drawing on the United States or other democratic countries for personnel? For individuals who are effectively acting as contractors? And are there sensible restrictions that can be done to try to limit that sort of help?

I'm not sure, frankly, who is the best person to begin tackling this question. Alex, I was kind of thinking of you when it came across the monitor. Maybe others who are best positioned with it.

MS. SIEGEL: Yes. So I mean I think something that's gotten a lot of attention is kind of the idea that China is serving as an exporter of surveillance technology. And they were sort of the original kind of successful internet sensors in some ways despite the fact that their infrastructure was very different than what we see in the Middle East, for example.

But some of the kind of tools and approaches that they have, have been, you know, exported in various ways. There's also been, you know, a lot of recent journalistic reporting on Israel's role in, you know, helping countries in the region engage in different kinds of surveillance activities with activists and dissidents.

But I don't personally have kind of much knowledge or expertise of the U.S. side and the audience member was asking about.

MR. BYMAN: I'm not sure if --

MS. ABROUGUI: Can I?

MR. BYMAN: Yes, please.

MS. ABROUGUI: I mean I have one example I can share which is a Dark Matter group. It's an Emirate-based cyber security company. Well, it's called Cyber Security but what it does -- what it did in the past probably continues to do now is targeting human rights defenders in the UIE.

And like there were several reports that revealed that (inaudible), national security agency employees who used to work for the American government were actually employed by this company which used their expertise to spy on human rights defenders and dissidents. So this is just one example I can share.

MR. BYMAN: Thank you. Chris, I saw your microphone was turned on to respond to this.

MR. MESEROLE: Yeah, I was going to site the exact same example. But the -- you know, I think, one, to the broader point.

One of the reasons we're seeing these kind of surveillance technologies in the Middle East in particular is that, you know, the model that I talked about earlier that Russia and China pioneered. It's something that it's really going to only be adopted, at least, you know, now by states that have significant resources. And that, you know, for it to work, you need a combination of resources and expertise basically.

And states in the Gulf have the resources. They don't always have the expertise. And, in fact, they very often do not have the expertise domestically to do this, which means they need to bring in that expertise from elsewhere.

And so, thankfully, you know, after the example that Afef just mentioned, you know, I think the U.S. has kind of woken up to the issue and has started to kind of put in place measures to make it harder for former contractors, for some of our intelligence agencies to go and work with the Emirates and others on these.

But I think we need to monitor it much more closely. I think that's kind of one of the main takeaways of NSO and Dark Matter is that democratic governments, I think need to be much more proactive about ensuring that the personnel and some of their intelligent agencies when they leave those agencies don't them go and work for companies that can kind of support authoritarian countries as they try to build out these capabilities and capacities.

MR. BYMAN: Thank you. To switch gears to another question from William Deer which is about Israel.

You know, it's unusual to have a long discussion about the Middle East and not have Israel mentioned at all. And in this context, how is the Israelian government handled social media posts with regard to the West Gaza that the government thinks should be taken down?

We do have some capacity in terms of using reporting mechanisms of many

companies to try to spread their message and take down those they think are wrong. Dina, can you begin by kind of talking about the engagement of Facebook with the Israeli government on these issues?

MS. HUSSEIN: Yeah. I'm happy to touch base on a few of the points that were brought up in the question.

So when it comes to our engagement with any government, and this includes the Israeli government, we have public policy personnel that engage with all of the countries in Europe, Middle East and Africa. Some of them are based in countries, and some of them are not. They are based somewhere else.

When it comes to our engagement with the Israeli country as a company engaging with the Israeli government, we have engagements that outlines our policies. We engage in the same way that we would engage with partners in the Middle East or in the U.S. to outline and understanding of what our policies are, what the restrictions are to the work that we do and the work around transparency that we also will be doing once we engage around any type of content that's sent our way.

Now, across the board I think it's something of interest to people watching this webinar. We do have continuous conversations with law enforcement across these countries as well because it's a two-way conversation. We're trying to engage them to flag to us anything of concern that might actually be malicious on the platform. But we are aware of the political and sensitive dynamic there.

So to answer the question, yes, we do engage with the Israeli government but not in a way that is not that cannot be replicated in other countries across the globe. Now, I think the concern here is around preferential treatment.

And I think we are trying to address this is our engagement with any government partner, we are trying to push transparency. The resources that I mentioned earlier on are our first step around that. I know we can get better there, but it is available to everyone and it includes Israel but multiple other countries as well.

MR. BYMAN: Thank you. We have a question from Keith Hanley about alternative narratives. I wanted to ask about that to start out with, which is are there ways whether it's for the United States or for the society actors to have their interpretations and their voices elevated to try to correct or at least provide more powerful alternative sources of information that are better for informing people? How can we go about doing that in your view?

MS. ABROUGUI: So better for informing people like about what in general? About like the platforms or --

MR. BYMAN: I'm sorry. For better informing people about whether it's a human rights situation or a political situation or the bilateral kind of rivalry situation where the UAE is criticizing cutter and cutter is criticizing the UAE. Are there ways to more truthful and accurate narratives out there?

MS. ABROUGUI: Yeah. Well, I mean there are definitely different tactics. I, myself, I work before as an editor. And as an editor focusing specifically on the intersection of technology and human rights and focusing on how certain policies and practices in relation to this intersection affects people.

And this is one tactic that could be used is to use credible reporting but also to use storytelling for advocacy to tell the stories of those people who get impacted and the communities. Particularly the most vulnerable and the most marginalized focusing on the different intersection. For example, women human rights defenders can face -- when they face these -- they can face far more serious consequences, for example, than others or minority groups or, let's say, civil society organizers that work to protect the rights of minority groups.

So storytelling, credible reporting. We need more stories about these issues. And in the past few years, there has been a lot of reporting done about the practices and policies of certain governments but also of platforms. And we need more of those stories coming out from the region.

We've seen that happening last year in relation to Palestine and the Palestinian voices who are being silenced as a result of the implementation of Facebook's policies in

relation to Palestine and Israel. And that kind of helped. I mean those stories kind of helped shift the narrative but also helped to bring some change and some coordination between the platforms and civil society organizations when it comes to this too.

MR. BYMAN: Thank you. Dina, I want to ask you to pile on to a point that Chris raised about thinking about the roles of governments. And in particular, are the things that you would look to from whether it's the United States or European or other governments to share their own information?

Obviously, social media companies have tremendous knowledge of this information space. But a lot of it comes from other sources. There's a lot of information out there. What do you think will be useful to learn from government in terms of trying to make this problem better?

MS. HUSSEIN: That's a really interesting question, Dan. So I think we -- to answer that question we need to take a step back and look at the kinds of abuse that we'd like more information around, right?

The initial portion of this is very tactical. And the secondary portion of this is a lot more strategic. On the tactical perspective, as tech companies, we have actually come together on a few occasions to address a few types of abuse where we are sharing information and knowledge. So for example, in the terrorism sphere that you and Chris are very familiar with.

We've brought together the global internet forum to counterterrorism where not only are we sharing the kinds of baseline best practices that we have. We're also trying to understand the kind of abuse and threat. And in that world, we get a lot of debriefs from experts and academics the global network on extremism. And technology engages regularly with us. It's a group of academics that are willing to come and share their expertise with tech companies.

We have been a little bit more sensitive towards engagements, obviously, with governments because of all of the human rights implications that have been highlighted. But I do think there is an avenue there for transparency and sharing of that kind of information. So

creating bodies where there is an ability to share information and insight. And that requires resourcing that the tech companies should participate in flushing out.

But I do think creating bodies where that dialogue is being had about the trends that we're seeing because unfortunately one of the things that tends to happen is we focus on big companies that have a lot of resourcing in order to identify and action these kinds of abuses. But we forget that a lot of people have multiple different apps on their phones and many of them are smaller tech companies that will fall foul in this kind of abuse as well. So that's the first portion of it is creating those forums.

The second part of it is, I think really expecting that governments will take equal action in the same way that tech companies are expected to. So to use the example of NSO. One of the things that I think was very interesting to see is seeing that commerce added NSO group and other foreign companies and entities to a list of malicious cyber activity actors.

So that was an action that I don't think was very precedented and we haven't seen before. And that allows then tech companies to feel more comfortable in engaging in proportional responses to this because at the core of this, one of the things that we're all dancing around here is whether we want to acknowledge it or not, there is a difference in power infrastructure when it comes to an individual user versus a state functioning on a platform.

And to ignore that power dynamic is to ignore the harmful impact that it then has. So that's where government voice and government action is a really important because it sets the tone for proportional response that a company can take.

MR. BYMAN: Thank you. I'm glad you put that out there because I think that shapes a lot of our discussion today.

Alex, can I ask you a question as a researcher, which is are there steps that social media companies can take that would make understanding of what's happening in this space much better for -- in order for serious outsiders like you to provide some degree of, I'll say, insight into these broader problems without having to necessarily rely on governments or companies that have their own interests in certain answers.

MS. SIEGEL: Yes. So this is a great question. And I think often the kind of limitation that external researchers have is we only have these particular public metrics available to us that we can use to try to get a handle on reach and impact of something like, say, a foreign influence operation or the spread of online hate speech or, you know, online extremism, these types of harms.

We can measure things like how often were posts on a given platform liked or shared or publicly engage with in some way, but we're at a loss when it comes to things like how many eyeballs were actually on this content for how long? What types of people were differentially exposed? What types of communities' online experiences were negatively shaped by a particular, you know, coordinated and authentic event online, this sort of thing?

And I think understanding the scope of these things requires going much beyond these public metrics of engagement. The number of people that actually click on things or share things or comment on them is a very small subset in most cases of overall kind of exposure. And so, if we're to understand impact and harm, having more access to data that enables us to get it kind of reach and exposure on these broader data, I think is one really important place to start.

I also think, you know, there's this question of who should be the arbiters of what content is allowed on the internet if these diverse cultural contents, right? And it probably can't be individual and governments. And it probably can't be individual tech companies, right? And so, having external actors who are able to get their hands on data in a safe way in order to characterize the harms from hopefully a more neutral perspective, I think is a pretty important step forward.

And platforms have taken steps towards this, right? So one example is Twitter has done a really good job recently of when there are takedowns of influence operations. Releasing these datasets that are hashed in a way that protects user privacy but still gives researchers a better sense of kind of the scope and content of the operations. Feedback has given researchers access to crowd tangle which enables them to get some insight into some of

these dynamics. But again, not really sort of the reach and views that you might want to see in a more granular level to understand the scope of the harms.

But I think it's a challenge in the sense that there is so much data and how do you protect user privacy particularly in these sensitive context that we're talking about while still giving external researchers appropriate access to data. And I think kind of negotiating the terms of that is an important step forward. And there's been a lot of progress made, I think in the interface between academics and tech companies and making some of this possible, but still a long way to go.

MR. BYMAN: Chris, can I turn to you? Again, taking your knowledge of outside the region and applying it to the region? If you look at some of the problems in the greater Middle East today. We've seen these techniques and methods used by Russia in the past.

And sometimes, what happens somewhere else in the world shows up in the Middle East a day later or sometimes it's a year later. Are there things happening in this broader issue space that you feel we should be watching and preparing for in the Middle East because it is going to be a problem if it's not addressed soon?

MR. MESEROLE: That's a great question. I think one of the challenges that I think is coming is really this issue with data localization, the kind of splintering of the internet. I think is kind of -- we're at the, you know, I didn't want to kind of take the conversation necessarily in another direction earlier with my comment about what governments could do.

But I know with kind of some of these concerns around like if you're a regime concerned around influence operations and in particular foreign influence operations. One of your instincts is to kind of, you know, shelter your internet. Basically, take the China model, right? And like, you know, create a nationalized internet of some kind that you have full control over.

And, you know, I think we're on the precipice now of, you know, we've got China. We have the EU which is increasingly pulling away from the U.S. in terms of their understanding of data localization. There's a whole set of court cases known as Schrems One

and Schrems Two that have kind of made it very difficult for companies operating in Europe to share information between -- or data between the U.S. and Europe.

And I think it's kind of we're inching towards a world where companies that are global in nature, begin to have to have effectively like European operations, North American operations. India, depending on how they go in the next couple of years could potentially do something similar. And if they do, I think once you're in a world where, you know, the EU, India, China and, you know, North America all have kind of different data models. It's going to hard to see how we don't -- like the rabbit is kind of out of the hat at that point.

And I'm a little worried that we're going to end up with a world with a lot of different splintered internets effectively. And it's going to I think, you know, even if somebody is concerned about the ease at which foreign influence operations can take place precisely because of the open and kind of fluid nature of the internet. And I'm worried that that will start to appear even within the Middle East that you'll have kind of a Saudi internet and an Emirate internet.

And you've already started to see a little bit of motion in that direction, but I don't -- you know, as concerned as I am about some of these issues, I don't think that's the solution. And I think it would make it easier for authoritarian regimes to kind of implement some of the more excessive abuses of digital platforms of like Russia and China have developed. And so, I would be really weary if that starts to become the dominant mode of thinking within the region too.

MS. HUSSEIN: Dan, do you mind if I jump in there very quickly?

MR. BYMAN: Please. I'd be grateful. Thanks.

MS. HUSSEIN: I'll try to be as brief as possible. I wanted to double down on what Chris was saying because I do think it's useful to present the tech perspective here.

One of the things that we have noticed is exactly this fragmentation of laws and legislation based on a regional jurisdiction. And one of the things that I do want to emphasize is for certain legal protections, let's say, tech companies are only actually legally required to

implement in a specific region.

So GDPR, for example, is a really great example of this. We've chosen to apply globally. But one thing that does tend to happen is with the implementation of one legislation, you see a domino effect. Other countries want to apply something similar. And it becomes very difficult for us to ignore the fact that these regional legislations that are trying to get at a very specific obstacle in one country then get applied at a global scale.

And if tech companies then start to just agree to apply them jurisdictionally that means that you have two situations that are occurring. Number one, an imbalance of the protections for global user bases, right? Where certain governments that are not authoritarian viewed as democratic are applying these laws and only their citizens get that protection.

So there is a need for a global dialogue about this. And myself and Dr. Anne Saltman who is part of the GCTR is writing a little bit more around this. But the second portion of this is one way to Chris' point. Legislation that might have great intention in one country can then be replicated with malicious intent in another country. And then the tech companies are placed in a position where they have to say, we are going to rank and rate governments and pick and choose who's laws we apply.

It's not a situation that I think is equitable or fair. And I don't think anybody wants the tech companies to be the arbiters of this. To use Alex's descriptor. So I do want to emphasize that, number one, regional legislation that then has global impact really needs to be considered.

Number two, understanding that when one country applies a legislation, it can very easily be replicated by another country that might not have the same intent. And there really isn't a defense against not cooperating with one country versus another that doesn't start to get us in some very, very difficult and icy waters.

MR. BYMAN: Thank you, Dina. I think that is sufficiently an important cautionary note for us to end our discussion. A reminder of the incredible complexity of not only the problems, but also potential solutions that people bandy about.

It's been really a fantastic hour. I want to thank everyone who's watching this on YouTube for joining us today. And particular thanks to our four speakers who I think have provided a fantastic discussion of this very difficult problem. Thank you very much.

* * * * *

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