support message:

This podcast is supported by the Walton Family Foundation. The Walton Family Foundation is at its core, a family-led foundation, working to create access to opportunity for people and communities. The foundation partners with others to make a difference in K-12 education, the environment, and its home region of Northwest Arkansas in the Arkansas, Mississippi Delta. Learn more at waltonfamilyfoundation.org.

Tricia Johnson:

It's Aspen Ideas to Go from the Aspen Institute. I'm Tricia Johnson. During the pandemic, foreign and domestic actors have spread disinformation online, making people doubt the severity of COVID-19. Laura Rosenberger, directors the Alliance for Securing Democracy, which works to counter authoritarian interference in democracies. She says the COVID disinformation could spell trouble for the November election.

Laura Rosenberger:

When you are sowing doubts about the information that the government is providing about the pandemic, you're sowing doubt in citizens, speak in their democratic institutions. That primes us to have less faith in the integrity of the election.

Tricia Johnson:

Aspen Ideas to Go brings you compelling conversations from the Aspen Institute. Today's discussion is from the Aspen Security Forum presented by the Aspen Strategy Group. In 2016, Russia meddled in the presidential campaign. It spread propaganda on social media platforms like Twitter among other tactics. This year, disinformation was on the minds of voters, candidates, government officials and technology platforms ahead of the election. For good reason, experts were seeing new threats by actors at home and abroad. Then COVID-19 hit, and a new battleground emerged around disinformation. With the pandemic and the election, are we in a perfect storm for chaos online? Laura Rosenberger, who served on the National Security Council at the White House is joined by Renée DiResta, research manager at the Stanford Internet Observatory. Cecilia Kang, leads the conversation. She's a technology reporter at the New York Times. Here's Kang.

Cecilia Kang:

So I thought I'd start with you Laura and ask you, we are less than three months from November 3rd from election day. Can you tell us at this point, what are your greatest concerns around election security and disinformation? Are they different concerns than perhaps you might have had around the 2016 campaign?

Laura Rosenberger:

Well, thanks, Cecilia. It's so great to be here with you and with Renée to have this important conversation. So the thing I'd like to do in terms of addressing the question about the elections is actually take a step back a bit, because I think sometimes when we think about disinformation or threats to democracy, just in terms of elections, we often miss the bigger picture at play. One of the goals of especially the foreign actors that I spend so much time looking at, is not necessarily just about changing or sort of manipulating an election outcome. That might be one part of it for some actors, but a bigger part of it for actors like Moscow, actors like Beijing, actors like Taiwan, authoritarians who are using the

information space for geopolitical purposes, is actually to undermine and weaken democracy itself. It's to make people trust the institutions less. It's to make people have less faith in information. It's to really undermine the sense of truth itself, right?

Laura Rosenberger:

A lot of times what we see in the information manipulation space is not necessarily about driving any particular narrative. It's not always about information that's sort of quantifiably true or false, but it's about really undermining that faith in democratic institutions and that sort of sense of democratic governance delivering for people. So to apply that to the election context, the thing that actually worries me most is that so much of that perfect storm that you just laid out, so many of those dynamics are actually aimed at making people have less faith in their government. Making people have less faith in democracy as a system as something that's delivering, having less faith in news media, having less faith in the information they're getting about their health.

Laura Rosenberger:

I worry deeply that coupled with questions about how an election is actually going to be pulled off in a pandemic, all the changes that we're seeing to, how the election is going to be run, all the questions that are being raised by some actors who are acting, I think in less than good faith about what mail balloting might look like and whether it's vulnerable. I worry a lot, not just about sort of the process leading up to the election, but actually the night after, the day after. That there will be an effort to really so doubt about the integrity and the process itself, and make people question whether they can have trust and faith in it. So I think understanding the election as part of that bigger, perfect storm that you just laid out is exactly what we need to be doing and bearing in mind how the focus really needs to be on shoring up these institutions, shoring up resilience, shoring up people's faith in quality information sources, so that we are less vulnerable to these sort of manipulative tactics.

Cecilia Kang:

Yeah. Renée, that was certainly some of the findings in your research around the 2016 election and the tactics by the IRA. A lot of it was to undermine sense of truth, trust in institutions, trust in government trust in society, really. First of all, in response to what Laura is saying, but also what are you seeing that may be different this time around? Are you seeing, for example, Russia deploy different tactics, maybe expand the way that they have had distributed sort of their discipline information campaigns. What are your observations today compared to back then when you were studying it so intensely?

Renée DiResta:

Sure. So I think one of the things that's important to understand is that you should think of the social media ecosystem, not as some... It's unique in the sense that this is the kind of new technology of the day, but the idea of influence operations are not new, right? So if you think about the history of propaganda, the history of influence, it's always carried on the most technologically salient platform of the time, whether that was television or radio, there's an incorporation of human agents of influence and undermining society. Anybody who's watched, the Americans has seen the ways in which Russian actors interfaced with civil activists who were highlighting and calling attention to very real tensions in American society. So a lot of the way that we think about this is actually entering into a system part of one more channel in a broad based tool of communication and influence capabilities.

Renée DiResta:

So when you think about it in that regard, what we should expect to see is anytime that system changes, anytime the rules of the system change, the adversaries should evolve so that they can overcome that change. So one example of this would be sort of in the immediate aftermath of us beginning to understand what happened in 2016, Facebook ads became very much a topic of conversation and in response to the recognition that Russia had, in fact run ads to grow audiences for their groups. What we started to see was Facebook began to make changes saying, "Okay, now we're going to verify your identity. We're going to send a postcard home to your address so that you have to prove that you are who you say you are." Now, this is not an insurmountable check for a sophisticated state actor, but it does add a little bit more friction into that system.

Renée DiResta:

So when we see the formation of investigations teams, the formation of public private partnerships, like at Stanford, we do work with the platform companies on identifying emerging influence campaigns, what you see as the evolution of the actor tactics. So it was a lot of the focus became [inaudible 00:08:22] these operations in the context of inauthentic behavior is the term of platforms use. One of the things that my team saw was the rise of groups in Africa, Russian activities in Africa targeting African local politics in eight different countries which they hired locals. So instead of fake identity is run by trolls out of St. Petersburg, what you started to see instead was one or two real people who were incorporated into the operation. Again, we don't know to what extent they were winning or not winning, but that's franchising down into local actors makes it harder for the platform to decide to take down the entirety of the page, because there is some grain of authenticity there.

Renée DiResta:

When in fact these pages came down, you're gaining progression [inaudible 00:09:10], where there's extraordinary article about how the sensors at Stanford were silencing the voices of real Africans, right? So this is the reaction that you get when these pages come down. Facebook is, of course, preventing these very real people from exercising their right to speak on the platform, and that's a very hard narrative to counter, short of saying like here meticulously laid out is our assessment of the operation and how we attributed it the way we did and the extensive research that went into that to justify the takedown. But what matters is for some percentage of people who believe that media ecosystem, it is still ultimately an egregious overreach of censorship.

Cecilia Kang:

We will get to this more about the struggle that or the challenge that poses for the platforms themselves when you're sort of testing their rules and their guidelines with these real individuals that are being used as part of this platform. So we will get to that as well, but that is a great example of the new tactics. Laura, can you talk a little bit about... Then around February and March, the novel coronavirus became a real thing globally. The pandemic was realized as a huge phenomenon. What then did you start observing in terms of disinformation, particularly by foreign actors, as well as domestic around disinformation with the virus?

Laura Rosenberger:

Yeah. Absolutely, Cecilia. I think I'll probably leave most of the domestic piece to Renée because she's got deeper research, especially on sort of coronavirus disinformation there on the domestic side. On the foreign actors side, I'll highlight mostly what we saw. The most interesting story, I think for me especially in February, March was really coming out of Beijing, out of People's Republic of China. I'm going to

pause for one second on a definitional point, which is probably going to sound a little bit pedantic, but bear with me because I'm not going to talk about this in terms of disinformation per se. I'm going to talk about information manipulation because disinformation is classically defined as deliberately false or misleading information, right? Deliberately disseminated false misleading information. The vast majority of what we see in the broader sort of information ecosystem in terms of malicious behavior is not necessarily something that falls into that space.

Laura Rosenberger:

There's a whole range of tactics that we could talk about. Disinformation is absolutely one of them, but I use the term information manipulation to talk sort of broadly speaking about some of these tactics that we see that disinformation is one piece of it. I think that's particularly important in the China context because the Chinese party states tactics have historically been different than what we have seen from an actor like Moscow. I think that comes a bit from their geopolitical positions, right? Putin's Russia is an objectively declining power. It is becoming weaker and weaker on a whole host of geopolitical and geo-economic measures. Beijing is an objectively rising power, right? Is seeking to exert its influence more broadly.

Laura Rosenberger:

So while Putin's interests are much sort of shorter term and much less sort of reputationally, involve much less reputational risk. For Beijing, if you're trying to cultivate yourself as a partner and a leader, in a sort of geopolitical player in a significant way, it's a different risk calculus. So what that had meant was that historically, we'd seen most of the Chinese party states information manipulation strategies focused on creating an amplifying content that was positive about the Chinese Communist Party and suppressing or denying the information space to actors, topics and entities that didn't want to occupy them. It does that through, of course, mass censorship, but also other forms of algorithmic suppression and other kinds of measures.

Laura Rosenberger:

This is very much a part of their strategy internally, right? In terms of what we hear about it with the Great Firewall of China, which has both technical and legal components to it. But we've increasingly seen China as its external strategy has become more assertive and it's gained interest more broadly expanding its information strategy outside of its borders. What we really saw around February, March of this year with COVID, was an acceleration of some trends that we had started to see over the past year, which was both Chinese officials with their foreign ministry, other parts of their official bureaucracy, as well as party and state back media becoming much more aggressive in their use of information, taking on some tactics that actually look a little bit more Russian.

Laura Rosenberger:

Now, I think it's important to be clear that there are still significant differences in the way these two actors engage in the information space. Some of the things that we saw that seems like a departure from past practice from Chinese actors, these were all really aimed around what I would characterize as acting out of insecurity, right? The party actually early on in its response to the coronavirus crisis was really seeking to deflect blame from itself or its own initial failings and dealing with the virus. The Chinese government was being blamed by the US and others for allowing it to get out of control. So deflecting blame was a really big piece of it, and so we saw a few different pieces, I think come into play that appear to be new elements of the Chinese party states information manipulation strategy.

Laura Rosenberger:

The first is very aggressive engagement on Western social media platforms, particularly Twitter by Chinese officials, what the Chinese themselves have dubbed wolf warrior diplomacy, much more sort of aggressive trolling tactics that we've seen evolve over the past few months. The second piece of it, is the spreading of actual disinformation in particular about the origin of the virus. In part, we actually saw a few different narratives about what the origin of the virus might have been. We saw coordinate the campaign to promote those different narratives using material from conspiracy theory websites that form a sort of central part of actually the pro-Kremlin disinformation ecosystem.

Laura Rosenberger:

So that also felt like a difference and something that actually had some similarities to activities we've seen from Moscow when it sought to deflect blame from itself about the poisoning of Sergei Skripal in Salisbury or the Downing of the MH 17 airliner over Eastern Ukraine. So for me, one of the big questions is whether this is a sort of permanent departure and new phase of tactics or whether this is a sort of aberration of testing and trying out new things. But those are just a few of the dynamics that we've seen over the past few months in particular with how China's engaged around with coronavirus information.

Cecilia Kang:

It's fascinating that you mentioned Laura, that they're taking some cues from the Russian playbook at the same time, Renée, you just published a really fascinating report on sort of the ecosystem of China's information apparatus and how it goes back so far in history, and they have sort of an established playbook that's online and offline. Can you talk about what your observations, combining with sort of feeding off of what Laura was just saying. You know where I was going Renée. I was going towards your research that was just published last week, where you give a really fascinating look at the ecosystem of information sort of tactics by the Chinese government dovetailing on what Laura was saying on the new tactics that they're deploying that look very similar to what Russia was doing over the last few years. We'd love to hear from you what you found in your study, and also, can you give us a sense of how threatening the Chinese information sort of apparatus is when it comes to... And I'm glad you Renée sort of distinguished the vocabulary information manipulation as well as disinformation?

Renée DiResta:

Sure. So the work that we did, we have a project at Stanford right now called the Virality Project, which is sort of a double entendre because we're looking at coronavirus. But we chose coronavirus in part because it allowed us to have a... This is one of the few moments in history, I think where the entire world has been talking about the same thing, right? That doesn't happen very often. When governments, particularly authoritarian governments have to justify their existence and their continued existence in the form when massive numbers of people are dying. So we looked at Russia, China, Iran, Saudi Arabia, the US, so not limited to authoritarians. I think Venezuela is next up on deck. So we have a pretty broad assessment of how states have been using both media and social media and then overt and covert tactics.

Renée DiResta:

That's been the framework that we've tried to use at SIO more broadly, for maybe just about almost a year now, or we've tried to again, understand social media as yet one more channel and an influence operation or information operation writ large. So the work that we did on China with our colleagues at Hoover, first contextualizing China's capabilities looking back to the sort of origin of the CCP. Again,

understanding that propaganda has always been an integral part at the highest levels of government. There's no attempt to conceal that. It's sort of a public diplomacy and the attempt to use established broadcast ecosystem. Some of it is inward facing. We've chosen to focus primarily on the outward facing content, the content targeting the rest of the world.

Renée DiResta:

So we looked at ways in which that apparatus was deployed towards coronavirus. We've looked at the wolf warrior diplomacy because as Laura mentioned, it does manifest on Twitter, right? Because that is where you reach the majority of the world instantaneously today, and accounts that happen to be funny or irreverent or sarcastic, their content is frequently retweeted, which affords it even more reach. So there's just a certainly different dynamic there. That's the kind of social media as marketing, marketing for an idea of propaganda being... Almost a marketing campaign for a particular ideally. We can say that they're using the same tactics and a lot of ways at this point. Where we see the covert side come in, is the incorporation of things like bots.

Renée DiResta:

Again, going back through history, there's a spectrum of understanding how concealed an account or operator is. Sometimes they are still real people who are agents of influence in the sense that you don't know who they're working for, who's funding them. But oftentimes what we see with Twitter and with Facebook is there's this extremely easy way to create completely fake people. So that dynamic just again, transforms makes it potentially more efficient to run completely on attributed campaigns, but they do in fact, take some work. What we saw with Russia was a multi-year commitment to begin to establish its personas. The personas that they were using in 2016 were created back in 2014, right?

Renée DiResta:

So they have multi-year history of engagement. They worked to connect with influencers. They worked to ensure that they were retweeted by extremely prominent people who have phenomenal reach with their target audience, right? That's on the left and on the right. We had Jack Dorsey retweeting some of Russia's fake black activist trolls and we had Donald Trump Jr. retweeting some of their fake white activist trolls, right? So they really put in the work to understand what would resonate with American audiences, what kind of personas would play. We haven't seen that sophistication from China. We have seen sloppiness, we've seen the creation of extremely thin personas.

Renée DiResta:

One of the things, if you visit io.stanford.edu, one of our data research assistants made a beautiful graph showing the turning on of the counselor of the time topically. You see a bloom when coronavirus hits, because all of a sudden they have a bunch of coronavirus focused personas that were all created relatively within a span of couple of weeks to month, right? So they're not laying the groundwork and doing this very sophisticated type of persona creation that's useful for persuasion. What we see instead is this kind of creation that actually mimics very closely Saudi Arabia's work around when Khashoggi was murdered, turn on this collection of accounts and just flood the zone, and a very distinct different strategy because oftentimes those accounts are called almost immediately.

Renée DiResta:

They're easy to find, the platforms find them, bot spotters and researchers find them. They come down very quickly, but what matters is that in that moment when people are paying attention, that's when

they're active. So it's a very different, far less sophisticated commitment to a long-term influence strategy. It's curious to see, we've actually been very interested in why they operate in this way in part, because the [5o sub-party 00:23:25], which is common to army focused inward has been operating since 2004. So the presence of fake personas participating in conversations within the Chinese internet ecosystem is actually not new at all, and so we've all been waiting to see how this would manifest in the outside of China, in the Western social media ecosystem, and it's been sort of surprisingly have hazards.

support message:

This podcast is supported by the Walton Family Foundation. Everyone deserves an opportunity to succeed no matter where you live, what you look like, or how modest your beginnings, but how do you create access to that opportunity? So people have a chance to discover their promise and reach their full potential. The Walton Family Foundation believes in the power of opportunity to transform lives, build strong communities and protect a natural world that sustains us all. For more than three decades, the foundation has been inspired by those who never see a challenge without striving to overcome it. Those whose inventions are driven by necessity, the dreamers, the doers, those who are closest to the problem because they are closest to the solution. Opportunity thrives in healthy environments, it Withers an ailing once. Opportunities should never be limited by geography, no one ever solved a big problem by thinking small. It's never easy to overcome difficult challenges. It takes time and steady resolve. One thing is true, everyone deserves an opportunity to succeed, learn more at waltonfamilyfoundation.org.

Cecilia Kang:

Laura, as far as the way that Renée was describing the Chinese sort of flooding the zone, does that have potential more scale in reach? In other words, I know this is a very blunt question, but like in perhaps too simplistic, but I'm trying to assess or trying to think about what potentially has greater threat? The Chinese sort of approach or not. Laura, can you bring this back to how does this affect the elections that if China's and the whole apparatus is spreading manipulated information about COVID.

Laura Rosenberger:

Yeah. So let me pick up on a couple of different things. One is, I think Renée's point on the lack of sophistication that we continue to see, especially from the covert side of operations is important. I think it also speaks to a broader question here. One of the things that we saw happened in the beginning of the anti-racism protests in the US, was both in Moscow and Beijing, sort of seized on this narrative about not... It wasn't a disinformation narrative. It was just what we would call sort of what about as some argument like, "Hey, look, police are beating protesters in the streets in Washington and in Portland and Minneapolis," and "Hey, you criticize us for when this happens in Hong Kong and Moscow, so who's smiling now, right?" So they want this, what about this kind of thing.

Laura Rosenberger:

In Beijing, we also saw it and then think from Moscow, this attempt to argue like, "Look, protestors in the street means democracies and chaos and all this stuff." I'd frankly, retort that while the reasons for the protest was being in the streets, and the fact of police lashing out of protesters and press was not a good thing. The act of the protest themselves is a sign of democracy, messy as it may be actually working, right? That's something you can't see in these regimes. But one of the more interesting moments was when one of China's foreign ministry spokespeople was attempting to tweet in solidarity with the protesters. She actually tweeted, I believe it was a quote tweet, excuse me, but she tweeted All

Lives Matter and she did that... It's hefting to express solidarity with the protestors, not realizing that in fact, All Lives Matter is a rejection of the Black Lives Matter mantra, right?

Laura Rosenberger:

So there's a lack of sophistication, I think about some of the broader cultural cues as well that we have seen Moscow actually be a little bit more adept at certainly in a lot of the IRA activity in 2016, right? Found those [inaudible 00:28:21] where they could pull those scenes. I think that's also an area where we see China definitely still lagging behind. To get a little bit more to your question about, what's the bigger threat and sort of how does this affect the election? Let me take those in two different parts. The first is, to me, I think it's really important that we take a step back. It's my favorite thing to do, taking a step back and understanding... Sorry for the beeping in the background, I'm trying to turn off my notifications here. I'm a sort of new National Security person by background, I spent a lot of time in government working on China and the US trying to form policy with China relations.

Laura Rosenberger:

So for me, it's trying to understand, what is China actually trying to achieve here? What is Moscow trying to achieve? All these things that we're talking about right now, they're tactics in a broader strategic effort to both use information for influence as Renée has said, but also both Beijing and Moscow are seeking to advance a different vision and autocratic vision of the information space. One where governments have a greater ability to monitor control what their citizens do online. They do that through infrastructure that's designed to enable that monitoring and control, and through legal and governance regimes that promote sovereign internet, sovereign information space. You alluded to the platform TikTok earlier in your perfect storm of issues, right? The debates, we're saying now about what should happen with TikTok, this platform I think is another big piece of this puzzle.

Laura Rosenberger:

So I think for me, the threat is not just from the actual influence vectors of the information itself, but that broader information ecosystem that these regimes are trying to create, because I think that's fundamentally at odds with a functioning democracy, which relies on deliberative debate with information and sort of truth and being sort of at the ground of it. That will bring us back to the elections right here, right? Which I think is that, the reason that I think that COVID disinformation is a concern in an election context is two things, right? One is, there's a very specific nexus there between health disinformation and disinformation about voting and how those two things are going to be interrelated, right? But there's a broader sense here of the fact that when you are sowing doubt about a government's ability to respond to something like a pandemic, when you are sowing doubts about the information that the government is providing about the pandemic, right?

Laura Rosenberger:

When some of the domestic actors that Renée's studied as well, right? Are promoting things like this pandemic documentary, right? That it sought to really sow doubt about some of the core figures, right? In our public health ecosystem and whether or not they're in fact telling the truth. You're sowing doubt in citizen's faith, in their democratic institutions, and I think that both primes us to have less faith in the integrity of the election. It primes us potentially to be less inclined to participate in democratic processes. It primes us to just be less trusting of our elected officials incredible sources of information. To me, a number of these different things are sort of gateway drugs, right, to the broader disinformation

ecosystems and health disinformation. Coronavirus disinformation right now is certainly playing a central role in a lot of that.

Cecilia Kang:

I mean, gateway drug is probably a very frightening term as suppose probably very apt for what we're seeing here. Renée, I would be remiss if we didn't go explore a little bit on the domestic side, but you've been seeing and what you're seeing with different platforms. Can you tell us sort of what are the biggest threats that you're seeing and how sort of strategies are being deployed?

Renée DiResta:

I think one of the challenges is, there are some guidelines the platforms have with regard to takedown by foreign state actors. We've alluded to them in the form of inauthentic activity. The question of what to do about health misinformation spread by real people, particularly domestic actors in the US for freedom of expression is paramount concern, means that those policies are less robust. The platforms treat everything sort of as an isolated case. There are policies, but they're not necessarily well-executed policies at this point. What that translates to is things that go viral that are not addressed in a timely fashion leading to oftentimes very ham-handed takedowns after the fact, I presume have been viewed eight million times as in the case of the pandemic video, that then lead to second order effects in which there's a controversy about censorship and platform censorship, making them then further reluctant to take things down earlier for things that need to be taken down. That's created a more misinformation ecosystem domestically.

Renée DiResta:

So one of the things that we've seen, I started working actually got my start in looking at misinformation and the spread of narratives, looking at the anti-vaccine movement in America in 2015. As an activist myself, working on getting a bill passed in California to eliminate vaccine opt outs which I was just interested in as a mum and was really kind of blown away by my own ability, actually, to just set up a Facebook page, we call ourselves Vaccinate California and to micro-target to get people calling their elected representatives to pass the bill that we wanted to see passed, right? That's just activism. That is the nature of activism today, and that has evolved over the last five years.

Renée DiResta:

So the interesting thing is, the same information pathways, the same virality tools, the same ability to micro target, to achieve particular reach, to leverage the groups' ecosystem, to spread information in a very participatory way. Regular ordinary people can be used for pro public health or Black Lives Matter or any number of different social movements that most of us have been pleased to see come into the world, but at the same time, they do offer the same affordances to people who want to spread health misinformation. So the challenge for platforms has been how to think about what to take down. There's a three part framework; remove, reduce and inform. Remove is what actually needs to be taken down, reduce is where you see a coordinated like a deprecated temporarily throttle or permanently throttled, the virality of something that is found to be misinformation that causes downstream harm.

Renée DiResta:

Then the last is inform, which is where you just put up the interstitial informing people about a fact check, posting a link to a fact check. One of the challenges with pandemic, the health misinformation video is what we found when we studied it at Stanford is that we could see indications that it was going

to be happening beginning two months prior. So beginning in April, 2016, we began to see evidence that anti-vaccine activists were trying to elevate this person, Judy Mikovits, who spread these insane conspiracy theories about Anthony Fauci, having people killed and so on and so forth. Conspiracies about masks, about murder, you name it, it's all in there. We could see early indications that this was a coordinated effort to turn this person into an influencer, and yet there was really no actionable moment for the platforms to respond to that.

Renée DiResta:

So the question becomes when this is just the information ecosystem, when anybody can use these tools and tactics, when is the appropriate intervention point and unfortunately with plandemic, we had seeing the initial post looked at, it said, "This is going to be viral." Then sure enough, the next morning, I had, I think 95 emails in my box with alerts and mentions and things just this is here, it is, it happened. One of the challenges has been after something's viewed eight million times, what do you do with it? What we found was that it actually took about two days for the fact checks to start to come out. The New York Times did some, Science Magazine did some, a couple of YouTubers, very prominent YouTubers did them.

Renée DiResta:

But the challenge is when there's that two day lag between when the misinformation goes viral, and then when the fact-check comes out that basically seeds the space for the misinformation for such a sufficiently long period of time that then the fact-check doesn't get the same attention because people have moved on to the next thing. So, one thing that we've been trying to do at SIO is develop a better understanding of the velocity and the volume at which this occurs, the specific pathways that things jumped through and an attempt to develop a better understanding of how to detect signal of emerging virality or emerging velocity earlier.

Renée DiResta:

Then to think more about what's a more appropriate intervention. We don't want to see platforms taking things down constantly. That's not the kind of information environment that we want to operate in, but if you're going to use inform and put out a fact check, or if you're going to use, reduce and throttle it, the time to use those two tools is not after eight or 20 million people have seen something. So the question is, how do we improve our understanding of this is how information flows today. So what are the norms and the policies, and potentially the regulations that we want to see around those dynamics

Cecilia Kang:

Laura and Renée, can the platform see as early as you're describing? I mean, you guys definitely have a lens into it. Are they sufficiently looking ahead, sort of around the corners, is not even really a sharp corner to look around, right? When it comes to some of these trends.

Renée DiResta:

I think the question becomes focus. Where's your focus? Where's your attention? There are certainly people who are looking at it. One of the things that's challenging oftentimes though, is these happen across all platforms simultaneously, or they hop onto the next or they're coordinated to happen. It's not accidental. So there's that question of monitoring the internet system. So that's where I could probably respond to this in the context of Hamilton or some of the work that they do on that as well.

Laura Rosenberger:

Yeah. I mean, I think Renée is exactly right that it, a lot of it is a question of focus. A lot of it is a question of like, where are you watching the signals come from, right? Renée talks about all the different signals that you can use in this context, and I think there're lots of different directions that these signals come from. One of the challenges I think is figuring out how do you have multiple different angles on one problem, right? I'll give one specific example where I think there was a blind spot in the past where we've seen some attempts to deal with this, and then I can talk a broader Renée's point on sort of a systems approach. I mean, we've been talking a lot about sort of the foreign actor disinformation targeting democracies, but I think one of the greatest sort of travesties that's taken place in part by a social media was the use of Facebook by the Myanmar military apparatus to prosecute a genocide of the Rohingya.

Laura Rosenberger:

A lot of that took place in part because, or it was not detected, I should say at least in part because Facebook didn't even have people on the staff who had the language capabilities to understand, let alone the cultural signals that would have potentially helped signal early on that this kind of language around such a charged issue had potential to have disastrous consequences, right? So I think sometimes there's a sense that you have to have a lot of deep under the hood looking at all the different activity happening at a technical level. There's a huge part of that. Don't get me wrong, and Renée's team and others are fantastic at doing that kind of work, but there's also just the sort of broader monitoring of the ecosystem that needs to be happening with an understanding of what's happening in said place at that time, right? What's happening in this country that we need to be aware of?

Laura Rosenberger:

That's where I actually think that a real true systematic approach involves a significant amount of coordination and information sharing on sort of threat vectors and different signals between government actors, the platforms and the society actors or outside researchers because each of those different constituencies or entities has visibility into a certain kind of analysis, right? Or certain kind of indicators. Each of them on their own can see pieces of this. It's the combination of that, that I think is where you can actually have a much more sort of powerful approach, and certainly some of the work that Renée does and SIO does, the platforms does that.

Laura Rosenberger:

The work that my team does, the Hamilton dashboard that we operate really looks primarily at the overstate actor piece and how those actors engage with what we think of as the gray space which is not necessarily always covert, but these sort of quasi attributed actors in that space. Again, it's one piece that feeds into this broader sense of what's happening in the information ecosystem. But I totally agree with Renée's description from earlier on of needing to see this sort of spectrum of social media being just one piece of this broader information ecosystem. That sort of systemic approach is I think, where we still need to make a lot more progress in terms of not just the platform, stepping up what they're doing, but actually having the cross sector cooperation that we really need at scale.

Cecilia Kang:

We do have some questions I'm going to go ahead and launch right into it. I do want you to, at some point though, Laura, because you said something very chilling about how after the election, it's the day after that you're thinking about too. I mean, I think a lot of us haven't even wrapped our heads around

that, but it could be a long, very contested process going forward and the information sort of manipulation around that, but let's take a question.

member of the audience:

So the voting is a state and locality issue mostly, and obviously the federal government provides some standards recommendations, but it's really run by the states and localities take that information and try to run with it. But the sophistication typically when you get down to local level when you're talking digital or digital tools is usually not the primary thing that they're responsible for, the thing that they're promoting. Usually they don't have the money and usually they don't have the people. So coming back to elections, what do your speakers think about elections officials building support networks in states cross different localities to start building some digital tools to communicate like a mobile app, which seems to be pretty popular, I've heard, to communicate with the voters in their jurisdictions about... It could be as simple as just information, but it also could be as sophisticated as supplying sample ballots like they've tried doing in some counties with some success. But also it could be providing congestion information for polling centers where somebody might want to visit in person rather than voting remotely through the mail.

Cecilia Kang:

Thanks, Sean. Laura, what is working now? What are you seeing is actually working on in that space in terms of mobile apps? Do you want to answer that, Laura?

Laura Rosenberger:

Yeah. I'm happy to. I will admit if you saw me twitch a little bit, when you said mobile app. I have a lot of still Iowa caucus triggering happening over here. I'll come back to that once again, but Sean, I think your question gets at a really important point here. I mean, so one of them is that the officials who are on the front lines of this often have sort of the least amount of resources and capacity and knowledge about these kinds of issues, right? Yet we sort of need them to be on the front lines, but the other piece that was embedded in what you just asked, which I love is this idea of affirmatively building in pathways for quality information and building resilience in advance. This is one of the things that my team has been doing a lot of work with state and local election officials on, which is the moment to start getting out quality information about the election and how it's going and where to go for information is not the week before the election.

Laura Rosenberger:

Just to Renée's point about how the ground was being laid for the plandemic video for the past, almost four years, election officials need to be laying the groundwork several years ago, but really if you haven't started it doing it now to be using their information channels, hopefully verified Twitter accounts and Facebook accounts, their websites that hopefully have a.gov address so it can be protected by the US government to the fullest extent possible, right? That they're using these channels of information now, both because if you don't use them until a week before the election, nobody is going to follow you or know that they're there, but two, you need to be getting that information out now to build resilience in people's minds about expectations. What's going to happen with the election, with all these changes that are happening, right? I think over communication is essential in this area and doing that through quality verified channels. Now, to that end, while I'm all about finding sophisticated ways of getting information out to people where they're going to find it, I'm very skittish about things like mobile apps for a couple of reasons.

Laura Rosenberger:

One is, everybody's going to have to go out and download it and digest it themselves, learn how to use it and whatever, and that's not naturally fitting into their sort of information absorptive habits. Two, security challenges are a big question when it comes to mobile apps, and so we'll just sort of put that to the side, but the third and frankly, this is the problem with the iOS app, right? It wasn't actually that there was as security challenge. It's just that they had never been tested in the way it needed to be run at scale, to make sure people knew what they were doing. So you had the appearance that something had gone seriously, seriously wrong when in fact it was basically a combination of just like bad testing and user error and nothing malicious. But I would very much hesitate to start injecting new pathways for information certainly at this point in the cycle, but I would use the tools that are available and use them now and use them often to get out sort of advanced information.

Cecilia Kang:

Let's take another question.

member of the audience:

You had mentioned earlier about the needing to bring together the platforms and the government, and I was curious as to your assessment of how that's going right now, what's working well in terms of the relationship between those two and where could you see it going in the future?

Cecilia Kang:

Great question. Renée, would you like to pick that up?

Renée DiResta:

There's a few different ways in which engagement happens, right? I don't work at a platform, so I'm not going to speak to their policy teams or their integrity teams and their direct interfacing with government. But there're things like the global internet forum to counter terrorism, which is a consortium of a variety of governments, civil society, organizations, and tech platforms that do work with a particular focus on terrorism. That was one of the first bodies to come about because of the pressing nature of that particular issue, particularly after [inaudible 00:50:01]. So there is a very robust framework there. With the election monitoring stuff, I can't speak to the relationship they have internally because I don't have visibility into it, but what we have is a public private partnership for more broadly channels of communication by which either threat information or assessments of potential foreign interference or after action reports from particular takedowns, that includes domestic takedowns as well.

Renée DiResta:

There's effort to incorporate in signals that various entities have while remaining mindful of things like preserving user privacy and sort of core principles of engagement on that front. So there is, I think a far more productive working relationship now in 2020 than there was in the early days of dealing with ISIS in 2015, where there was very much platforms didn't want to be seen. This was right after Snowden, of course, platforms didn't want to be seen as doing the bidding of the US government, even when it came to putting out information about our taking down terrorist accounts. So there was not a very good working relationship back in 2015, but that has improved significantly now. I think one of the challenges that we have, we've recently set up an election integrity partnership at Stanford with a number of other

research organizations that are looking at election 2020 misinformation ranging from the technical to the qualitative purchase of understanding what's going on.

Renée DiResta:

There are these signal sharing frameworks in place to ensure that when we see something bubbling up, there is a way to route that information as appropriate. That includes the prior question state governments as well. There are a number of... We recognize that state secretaries of state and others don't necessarily have the technical capabilities within their teams to do assessments, and so when they see things like, "Hey, in my local Facebook Group, this voter suppression narrative, is this happening? Where is it coming from?" But we don't want to see as the immediate default, it's the Russians, and so we do have these sort of triaged processes that we're working towards to ensure that research organizations, academics, civil society, some even technical providers with the capability to assess those emerging narratives have the ability to look and help and investigate, and that all of that signal is shared among the stakeholders who can then communicate effectively with their constituents or elevate as necessary

Cecilia Kang:

We are pretty much at the end of our time here. I really want to thank Renée and Laura, we covered a lot of ground and a lot more to consider after the election and in general. Thank you, Laura and Renée.

Tricia Johnson:

Laura Rosenberger, is a senior fellow at the German Marshall fund of the United States. Renée DiResta, investigates the spread of malign narratives across social networks. She's advised Congress, the state department and other organizations on the topic. Cecilia Kang, oversees technology and regulatory policy for the New York Times. Their conversation was held in August at the Aspen Security Forum, which is presented by the Aspen Security Group. Make sure to subscribe to Aspen Ideas to Go wherever you listen to podcasts. Follow us on social media at Aspen Ideas. Listen on our website, aspenideas.org, and sign up for our newsletter. Today's show was produced by Marci Krivonen. It was programmed by the Aspen Security Forum team. Our music is by Wanderly. I'm Tricia Johnson. Thanks for joining me.

support message:

This podcast is supported by the Walton Family Foundation. The Walton Family Foundation is at its core, a family-led foundation, working to create access to opportunity for people and communities. The foundation partners with others to make a difference in K-12 education, the environment and its home region of Northwest Arkansas and the Arkansas, Mississippi Delta. Learn more at waltonfamilyfoundation.org.