Technology and Democracy: Protecting the Digital Landscape and our Elections

00:01: Thank you again, Laura and Renee, for joining. In coming... In putting together this panel, this conversation, I was thinking there's so much that has happened over even the last six months, we can almost think about disinformation pre-COVID and pandemic and post-COVID and pandemic, and a lot of this has directly... There's a lot of... The disinformation is around the COVID virus, is related to the election, in some ways not so much related to election, but it's all kind of a swirl.

00:34: So disinformation was of great concern for voters and candidates, government officials and technology platforms ahead of the election. Experts were seeing new tactics by foreign state actors and new threats by domestic actors. The exercises had grown more sophisticated and broader in reach, and Silicon Valley complicated things in some ways by creating differing policies about speech and addressing content removal and political fact-checking of ads differently as well. And then the pandemic hit and COVID became a new battleground for disinformation, fueled by foreign actors as well as domestic.

01:18: And then adding to this, you have the rise in popularity of new platforms and new technologies and tools, and it all seems like a sort of perfect storm. I know that cliche is overused, but it does seem apt in the situation. So that's the scene setting and where to begin. We thought about... So I thought about let's start talking about the election, and then we can talk a little bit more broadly about the more recent disinformation campaigns and trends that you're seeing, and so I thought I'd start with you, Laura, and ask you, we are less than three months from November 3rd, from election day, and can you tell us at this point, what are your greatest concerns around election security and disinformation? And are they different concerns than perhaps you might have had around the 2016 campaign?

02:16: Well, thanks, Cecilia. Yeah, it's so great to be here with you and with Renee to have this important conversation. And thanks for that great scene setter, which I think really laid out the degree to which this is a complex and dynamic and evolving space. 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 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 Tehran, authoritarians who are using the information space for geo-political purposes, is actually to undermine and weaken democracy itself.

03:21: 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? 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.

04:19: And 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 into 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-in 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 sow doubt about the integrity of the process itself and make people question whether they can have trust and faith in it. And 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 the information, quality information sources, so that we are less vulnerable to these sort of manipulative tactics.

05:20: Yeah, and Renee, 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. What are you also seeing in... First of all, any response to what Laura wass 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 had distributed their disinformation campaigns? What are your observations today compared to back then when you were studying it so intensely?

06:00: 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... And 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. And so if you think about the history of propaganda, the history of influence, it's always carried out in the most technologically salient platform of the time, whether that was television or radio, there's an incorporation of human agents of influence in undermining society. Anybody who's watched The Americans has seen the ways in which Russian actors interfac ed with civil... With civil activists who were highlighting and calling attention to very real tensions in American society.

06:43: So a lot of the way that we think about this is actually in or out of system, kind of part of one more channel in a broad-based tool of communication and influence capabilities. And so when you think about it in that regard, what we should expect to see is any time that system changes, any time the rules of the system change, the adversaries should evolve so that they can overcome that change. And 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, and what we started to see was Facebook begin to make changes, saying, "Okay, now we're going to verify your identity. We're going to verify... 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."

07:38: Now, this is not an insurmountable check for a sophisticated state actor, but it does kind of add a little bit more friction into that system. And 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 is the evolution of the actor tactics. So, as a lot of the focus became viewing these operations in the context of inauthentic behavior, that's the term the 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 in which they hired locals.

08:23: So, instead of fake identities 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 witting or not witting, but that 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. When, in fact, these pages came down, Yevgeny Prigozhin in his FAN, his extraordinary... Wrote this extraordinary article about how the censors at Stanford were silencing the voices of real Africans.

09:03: And 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, here meticulously laid out is our assessment of the operation and how we attributed it the way we did and the kind of 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.

09:41: That's... We will get to this more about the struggle that... Or the challenge that poses for the platforms themselves, that 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. And Laura, can you talk a little bit about then and around February/March? The pandemic really... 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?

10:34: Yeah, absolutely, Cecilia. And I think I'll probably leave most of the domestic piece to Renee because she's got deeper research, especially on the coronavirus disinformation there on the domestic side. On the foreign actors side, I'll actually... 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 the People's Republic of China. And just... 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. Deliberately disseminated false or misleading information. The vast majority of what we see in the broader information ecosystem in terms of malicious behavior is not necessarily something that falls into that space.

11:38: 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. I think that's particularly important in the China context, because the Chinese party state's tactics have historically been different than what we have seen from an actor like Moscow, and I think that comes a bit from their geo-political positions. Putin's Russia is an objectively declining power that is becoming weaker and weaker on a whole host of geo-political and geo-economic measures. Beijing is an objectively rising power. It is seeking to exert its influence more broadly. And so, while Putin's interests are much, sort of, shorter term and much less, sort of, reputationally involved, much less reputational risk, for Beijing, if you're trying to cultivate yourself as a partner and a leader and a sort of geo-political player in a significant way, it's a different risk calculus.

12:45: So, what that had meant was that historically we had seen most of the Chinese party state's information manipulation strategies focused on amplifying... Creating and amplifying content that was positive about the Chinese Communist Party and suppressing or denying the information space to actors, topics and entities thatit didn't want to occupy them. It does that either through, of course, mass censorship, but also other forms, algorithmic suppression, and other kinds of measures. This is very much a part of their strategy internally, 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.

13:36: And 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-backed media becoming much more aggressive in their use of information, taking on some tactics that actually look a little bit more Russian. 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. But some of the things that we saw that seemed like a departure from past practice from Chinese actors, these were all really aimed around I think what I would characterize as acting out of insecurity. The party actually early on in its response to the coronavirus crisis was really seeking to deflect blame from itself for its own initial failings in dealing with the virus.

14:37: The Chinese government was being blamed by the US and others for allowing it to get out of control. And so deflecting blame was a really big piece of it. And so we saw a few different pieces come into play that appear to be new elements of the Chinese party state's information manipulation strategy. 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 aggressive trolling-like 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. And in part we actually saw a few different narratives about what the origin of the virus might have been.

15:35: And we saw it coordinate the campaign to promote those different narratives using material from conspiracy theory websites that form a central part of actually the pro-Kremlin disinformation ecosystem. And 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 MH17 airliner over Eastern Ukraine. So for me, one of the big questions is whether this is a permanent departure and a 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 has engaged around the coronavirus information.

16:29: It's fascinating that you mentioned, Laura, that they're taking some cues from the Russian playbook. At the same time, Renee, you've done... You just published a really fascinating report on the ecosystem of China's information apparatus and how it goes back so far in history. And they have an established playbook that's online and offline. And can you talk about what your observations are combining what Laura just... Sort of feeding off of what Laura was just saying about these sort of imitate...

17:07: Oh, no, I lost you right through the question. [chuckle] Oh, I lost you for a second. Oh, there you are. You're back. Okay. Muted.

17:23: You know where I was going, Renee. I was going towards your research that was just published last week where you talk about... You gave a really fascinating look at the ecosystem of information 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. Would 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 apparatus is when it comes to... And I'm glad you, Renee, distinguished the vocabulary, information manipulation as well as disinformation.

18:07: 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. That doesn't happen very often. And when the response... Governments, particularly authoritarian governments, have to justify their existence and their continued existence in the form... When massive numbers of people are dying. And so we've looked at Russia, China, Iran, Saudi Arabia, the US, so not all the major 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.

19:04: And that's been the framework that we've tried to use at SIO more broadly for maybe the last just about almost a year now, where we've tried to, again, understand social media as yet one more channel in an influence operation or an information operation writ large. So the work that we did on China was with our colleagues at Hoover, first contextualizing China's capabilities, looking back to the origin of the CCP. And 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 in 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.

19:52: 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, 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 re-tweeted, which affords it even more reach. So there's just a slightly different dynamic there. That's the kind of social media as marketing. Marketing for an idea or propaganda being and... [chuckle] Almost a marketing campaign for a particular idea. You can say that they're using the same tactics in a lot of ways at this point.

20:34: Where we see the covert side come in is the incorporation of things like bots. There's a spectrum of... And this is again going back through history, a spectrum of understanding how concealed an account or an 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, kind of, again transforms, makes it potentially more efficient to run completely unattributed campaigns, but they do in fact take some work. And 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. So they have a multi-year history of engagement. They worked to connect with influencers. They worked to ensure that they were re-tweeted by extremely prominent people who have phenomenal reach with their target audience, and that's on the left and on the right.

21:40: We had Jack Dorsey re-tweeting some of Russia's fake Black activist trolls, and we had Donald Trump Junior re-tweeting some of their fake right wing activist trolls. 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. One of the things if you visit io.stanford.edu, one of our data research assistants made a beautiful graph showing a turning on of the accounts over time topically. And so, 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 the couple of weeks to month. So they're not laying the groundwork and doing this very sophisticated type of persona creation that's useful for persuasion.

22:41: And 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 these accounts are culled almost immediately. 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, in that moment when people are paying attention, that's when they're active. And so, it's a very different, far less sophisticated kind of commitment to a long-term influence strategy, and it's curious to see. We've actually been very interested in why they operate in this way, in part because the 50 Cent Party, which is a kind of commentor 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 actually all been kind of waiting to see how this would manifest in the outside of China, the kind of Western social media ecosystem. It's been surprisingly haphazard.

24:05: It's interesting. I will remind the audience, and there are many of you here, that we will take questions for the last 15 minutes, and you can ask a question by using your raised hand function, which is located in the center of the meeting control bar. I think the questions will not actually queue up until we open it up, but I want to give you sort of a heads-up now so you can start thinking about your questions. So, Laura, as far as the way that Renee was describing the Chinese sort of flooding the zone, does that have potential more scale and reach? In other words, I'm... I know this is a very blunt question but... And 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. And, Laura, can you bring this back to, well, how does this affect the elections? That if China and the whole apparatus is spreading manipulated information about COVID.

25:11: Yeah. So, I think upon a couple of different things. One is, I think Renee's point on the lack of sophistication that we continue to see as restricting the covert side of operations is important. I think it also speaks to a broader question here. One of the things that we saw happen in the beginning of the anti-racism protests in the US was both Moscow and Beijing sort of seized on this narrative about... It wasn't a disinformation narrative. It was just what we would call sort of a whataboutism kind of argument, like, "Hey, look. Police are beating protesters in the streets in Washington and in Portland and in Minneapolis, and hey, you criticize us for when this happens in Hong Kong and Moscow. So who's smiling now?" So, a lot of this is like whataboutist kind of thing.

25:57: By Beijing, we also saw, and I think from Moscow, this attempt to argue, like, look, protesters in the streets means democracy is in chaos and all this stuff. And I'd frankly retort that while the reasons for protesters being in the streets and the fact of police lashing out at protesters and press was not a good thing, the act of the protest themselves is a sign of a democracy, messy as it may be, actually working. And 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. And she actually tweeted, I believe it was a, quote tweet, but she tweeted "All Lives Matter." And she did that in attempting to express solidarity with the protesters, not realizing that in fact, "All Lives Matter" is a rejection of the "Black Lives Matter" mantra.

26:57: And 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, where they found those fissures and where they could pull at those seams, and 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 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, again, a step back. It's my favorite thing to do, taking a step back and understanding... Sorry for the beeping in the background. I am trying to turn off my notifications here. That to understand from a... I'm a national security person by background. I spent a lot of time in government working on China, and US-China foreign policy and US-China relations.

27:57: So for me to try and understand, what is China actually trying to achieve here, what is Moscow trying to achieve and 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 Renee has said, but also, both Beijing and Moscow are seeking to advance a different vision, an 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 kind of monitoring and control. And through legal and governance regimes that promote a sovereign internet, a sovereign information space, which they are advancing at both at home and in places like the UN and other multi-lateral fora.

28:56: And so I think it's important that we talk about the threats of these particular kinds of approaches, that we not just think about it in the tactical stuff, but understand the broader strategic game being played here. And that's where things, like you alluded to the platform TikTok earlier in your perfect storm of issues. And the debates we're seeing now about what should happen with TikTok, this platform, I think is another big piece of this puzzle. And 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 at the ground it.

29:48: And that will bring us back to the elections right here, which I think is that... The reason that I think that COVID disinformation is a concern in an election context is two things. 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 inter-related. 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, when some of the domestic actors that Renee studied as well are promoting things like this Plandemic documentary, that it sought to really sow doubt about some of the core figures in our public health ecosystem, and whether or not they're in fact telling the truth. You're sowing doubt in citizens' faith in their democratic institutions.

30:55: And I think that 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, and it primes us to just be less trusting of our elected officials and credible sources of information. And so to me, a number of these different things are sort of gateway drugs to the broader disinformation ecosystem. And health disinformation, coronavirus disinformation right now is certainly playing a central role in a lot of that.

31:35: Yeah. Gateway drug is probably a... It's a very frightening term as well as probably very apt for what we're seeing here. And Renee, I would be remiss if we didn't go explore a little bit on the domestic side, what you've been seeing and what you're seeing on different platforms. Can you tell us what are the biggest threats that you're seeing and how strategies are being deployed?

32:03: I think a lot of challenges is there are some bright lines that platforms have with regard to take-downs by foreign state actors, and we've kind of 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, where freedom of expression is kind of 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. And what that translates to is things that go viral that are not addressed in a timely fashion, leading to oftentimes very ham-handed take-downs after the fact, after the video has been viewed 8 million times, as in the case of the Plandemic video, that then lead to second order effects in which there is a controversy about censorship and platform censorship, making them then further reluctant to take things down earlier as they are, are the sort of things that needs to be taken down.

33:05: And that's kind of created a morass in the information ecosystem domestically. So one of the things that we've seen, I started working... I 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 mom, and I 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 [laughter] to get people calling their elected representatives to pass the bill that we wanted to see passed, right?

33:45: And that's just activism, that is the nature of activism today, and that has evolved over the last five years. And so the interesting thing is the same information pathway is 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. And so the challenge for platforms has been how to think about what to take down.

34:32: There's a kind of three-part framework: Remove, reduce, inform. Remove is what actually needs to be taken down, reduce is where you see kind of a coordinated, like a deprecated, temporarily throttle or permanently throttle the virality of something that is found to be misinformation that has harm, that causes downstream harm. And then the last is remove, reduce, inform, which is where you just kind of put up the interstitial, informing people about a fact check, kind of posting a link to a fact check. One of the challenges with pandemic, you know with Plandemic, the video, 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.

35:19: 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, and 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?

36:01: And unfortunately with Plandemic we had seen the initial post, looked at it, said, "This is going to be viral," and 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 is viewed 8 million times, what 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. 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 kind of moved on to the next thing.

36:57: 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 kind of jump through, in an attempt to develop a better understanding of how to detect signal of emerging virality, emerging velocity earlier, and 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 8 or 20 million people have seen something. And 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?

37:56: And can... Laura and Renee, can the platforms see as early as you're describing? I mean, you guys have, you definitely have a lens into it, are they sufficiently looking ahead, like sort of around the corners? There's not even really a sharp corner to look around, right, when it comes to some of these trends?

38:14: I think the question becomes focus. Where is 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 things happen across all platforms simultaneously, or they hop from one to the next, or they're coordinated to happen, it's not accidental, and so there's that question of monitoring the internet as system. I feel like Laura could probably respond to this in the context of Hamilton or some other work that they do on that as well.

38:48: Yeah.

38:49: Yeah, I think Renee's exactly right. A lot of it is a question of focus. A lot of it is a question of, where are you watching the signals come from. Renee talked about all the different signals that you can use in this context, and I think there's a lot of different directions that these signals come from. And so one of the challenges, I think, is figuring out how do you have multiple different angles on one problem. And 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 about a broader... Renee's point of sort of a systems approach. We've been talking a lot about the foreign actor, disinformation targeting democracies. But one of the greatest travesties that's taken place in part by social media was the use of Facebook by the Myanmar military apparatus to prosecute genocide of the Rohingya.

40:00: And 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. And 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. And there's a huge part of that, don't get me wrong, and Renee's team and others are fantastic in doing that kind of work. But there's also just the broader monitoring of the ecosystem that needs to be happening with an understanding of what's happening in said place at that time? What's happening in this country that we need to be aware of?

41:07: And that's where I actually think that a real, true systematic approach involves a significant amount of coordination and information-sharing on threat vectors and different signals between government actors, the platforms, and society actors or outside researchers. Because each of those different constituencies or entities has visibility into a certain kind of analysis or a certain kind of indicators. And 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 powerful approach. And certainly, some of the work that Renee does with, and NSIO does with the platforms does that. The work that my team does with the Hamilton dashboard that we operate really looks primarily at the overt state actor piece and how those actors engage with what we think of as the gray space. Which is not necessarily always covert, but these are quasi-attributed actors in that space. And again, it's one piece that feeds into this broader sense of what's happening in the information ecosystem.

42:24: But I totally agree with Renee's description from earlier on of needing to see this spectrum of social media being just one piece of this broader information ecosystem. And that systemic approach is I think where we still need to make a lot more progress in terms of the... Not just the platforms stepping up what they're doing, but actually having the cross-sector cooperation that we really need at scale.

42:51: And I'm going to just remind people who are watching, the attendees, that you can submit a question now. We are taking Q&A, and I should have given you a warning a little bit earlier. So submit them right now so we can get them queued up. Okay. That is... The Myanmar example is... Renee, you were talking about focus and were talking about looking around corners. That was just right in your face. So that's probably an example that... A very good example, 'cause it is so egregious. One thing, I'm going to look and see how the questions are going. No questions yet. But oh, 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.

43:47: And think a lot of us haven't even wrapped our heads around that, but it could be a long, very contested process going forward in the information manipulation around that. But let's take a question from Sean Roberts. It's going to take a few seconds.

[pause]

44:12: Here's Sean.

44:16: Oops.

44:19: Should we take a different one or is Sean there?

44:21: Can you hear me?

44:21: Hi, Sean. Yes, we sure can. Welcome.

44:25: Unfortunately, I'm using another tool that [chuckle] seems to have stepped in front of you, but for the video. But I can give you the audio. So 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 is, 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 they usually don't have the people.

45:06: So coming back to elections, what do your speakers think about elections officials building support networks in states across 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.

45:58: Thank you, Sean. Laura, yeah. What is working now, what are you seeing that's actually working in that space in terms of mobile apps? There's... I do want to... Oh, hi, Sean. Now we see you. Okay. Do you want to answer that, Laura?

46:16: Yeah, yeah. I'm happy to. I will admit if you saw me twitch a little bit when you said mobile app, I had a lot of... I'm still like Iowa caucus figuring happening over here... I'll come back to that once again. But Sean, I think your question gets at a really important point here, which... So one of them is that the officials who are on the frontlines of this often have the least amount of resources and capacity and knowledge about these kinds of issues, yet we still need them to be on the frontlines. 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. And 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 that 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.

47:21: Just to Renee'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 ground work several years ago. But really if they haven't started it doing it now, to be using their information channels, their hopefully verified Twitter accounts and Facebook accounts, their websites that hopefully have a dot gov web address so it can be protected by the US government to the full extent possible, 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? I think over-communication is essential in this area and doing that through quality verified channels.

48:25: 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. One is it's not something that people... Everybody is going to have to go out and download it and digest it themselves and learn how to use it and whatever, and that's not naturally fitting into their information absorptive habits. One. Two, security challenges are a big question when it comes to mobile apps. And so we'll just put that to the side. But the third, and frankly, this is what was the problem with the Iowa app, it wasn't actually that there was a security challenge. It's just that it had never been tested in the way it needed to be to be run at scale, to make sure people knew what they were doing. And so you had the appearance that something had gone seriously, seriously wrong when, in fact, it was basically a combination of just bad testing and user error and nothing malicious.

49:26: 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 advanced information.

49:46: Oops. Cecilia, you are muted.

49:49: Thank you. Let's take another question from Emelia Probasco. And it takes a few seconds. She should be up very soon. Here we go. Hi, Emelia. Emelia?

50:06: Can you hear me now?

50:17: Yes, we sure can. Hi.

50:19: Hi. Sorry. Thanks so much for this session. You had mentioned earlier about the needing to bring together platforms in 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?

50:42: Great question to... Renee, would you like to take that or Laura?

50:46: Let me start with that one. So the... There's a few different ways in which engagement happens, right, and 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's 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 kind of one of the first bodies to come about because of the pressing nature of that particular issue, particularly after Christchurch.

51:22: So there is a very robust framework there. With the election monitoring stuff, I can't speak to the relationship they have internally, 'cause I'm just... I don't have visibility into it, but what we have is a public-private partnership forum, more broadly, are channels of communication by which either threat information or assessments of potential for interference, or after action reports in particular take-downs or... That includes domestic take-downs as well, are... There's an effort to incorporate in signals that various entities have, while remaining mindful of things like preserving user privacy and 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 kind of the platforms didn't want to be seen, this is right after Snowden, of course.

52:31: Platforms didn't want to be seen as doing the bidding of the US government, even when it came to putting out information about or taking down terrorist accounts, and 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 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 purposes of understanding what's going on. And there are these kind of signal sharing frameworks in place to ensure that when we see something bubbling up, there is a way to route that information as appropriate, and that includes, per a prior question, state governments as well.

53:15: 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 happening. Where is it coming from?" What don't want to see as the immediate default to "It's the Russians." [chuckle] And so we do have these triage processes that we're working towards to ensure that research organizations, academics, civil societies, 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.

54:14: Well, we are at around the... We are pretty much at the end of our time here. I really want to thank Renee and Laura, when I kick it back to Anya, we covered a lot of ground and a lot more to consider ahead of the election and in general. So back to you, Anya. Thank you, Laura and Renee.