MIT CSAIL Alliances | David Clark Podcast Short Cut 1

Welcome to MIT's Computer Science and Artificial Intelligence Labs Alliance's podcast series. My name is Steve Lewis. I'm the assistant director of Global Strategic Alliances for CSAIL at MIT. In this podcast series, I will interview principal researchers at CSAIL to discover what they're working on and how it will impact society.

David Clark is a senior research scientist at MIT's Computer Science and Artificial Intelligence Laboratory. Since the mid-1970s, he has played a leading role in the development of the internet. From 1981 to 1989, he acted as chief protocol architect and chaired the internet activities board.

His recent research has focused on the redefinition of the architectural underpinnings of the internet and the relationship of technology and architecture to economic, societal, and policy considerations. Specific research areas include internet security and internet measurement. David, thanks for joining us today. Can you define online disinformation for our listeners?

Sure. I use the word disinformation. I think most people use the word disinformation as distinct from misinformation. Misinformation is simply somebody that's confused. They've got a hold of the wrong fact.

Disinformation has intention. It has purpose. It implies an actor that is deliberately telling a story that is not true for some purpose. There's an initiator, and you can figure out-- in some cases, you can figure out who they are, and you can try to surmise what the purpose is. But it's a deliberate act, not an act of confusion.

I see. And could you provide some examples of disinformation?

Yeah, let me give you one that I particularly like. There's been a lot of attention recently on the Russian interference in US elections, and so forth. And a lot of this is the deliberate injection of disinformation into the discourse. There's a beautiful example I love that's been very well studied in the literature.

This is an example from Tumblr, where there was a persona called Lagonegirl, and there was a picture that suggested that she was sort of a young, slightly hip Black woman. And this persona made all sorts of comments about the scene as it were developed a bit of a reputation and would occasionally throw in things that were-- well, let me give you one example.

She quoted, the persona quoted Hillary Clinton as having said, I have to say this carefully, I don't believe in free college, and it gave a citation to where that quote came from. And then the commentary by this persona about that quote was, of course, you don't. It might hinder the school prison pipeline that your prison-owning donors depend on.

Now, what Clinton actually said was, I don't believe in free college for-- what she said is, I believe that we should make community college free. In other words, the quote was turned around. But she then said, I disagree with free college for everybody. I don't think taxpayers should be playing to send Donald Trump's kids to college.

So what this persona does is deliberately misquotes Clinton and then throws a comment in that tends to discredit her to the Black community, which is very sensitive to this issue of incarceration of young Black males. It was a Russian agent, and this was thoroughly proved that this identity was outed. The Black community was quite surprised to discover that this person was actually a Russian agent in St. Petersburg.

And there's some other examples that have been fairly well studied. I think the evidence is pretty clear, for example, that a lot of disinformation was injected into the British discourse about Brexit and may have actually influenced to the vote to go in favor of Brexit. We have a long history of big industry, sort of science denying disinformation, tobacco, asbestos, acid rain, and now climate change deniers. And of course, in politics, we have the big lie that Trump won the election. And I think all of these have propagated online, as well as in other ways. And this is a broad spectrum of stuff that shows up here as disinformation.

That's interesting. You had mentioned about intentional. What are some of the lessons about intention from those examples? I mean, obviously, Trump's stealing the election or the election being stolen from Trump, we know what the intention there was. But can you elaborate on that?

That's right. I mean, that was so clear. And I think the science deniers have an obvious motivation too. They're trying to preserve their right to carry on their business interest in an unregulated way as long as they can. And I think tobacco, I think there's a good example of tobacco, where for a long time, they denied that there was evidence that it caused cancer.

And eventually, enough lawsuits, it became clear that not only were they wrong but that they knew they were wrong. And it got them in a lot of trouble. But there are a lot of people today who would like to avoid the consequences of having the businesses having to deal with the consequences of climate change. You can sort of trace these motivations back.

But I think the Russians are more pernicious, and I think it's interesting to talk about what are the intentions of the Russians here. Because I think their intentions are very strategic, but they're trying to do is erode the power and the global influence of our nation by turning our energy to internal dissent. Obviously, they'd also like to have officials elected who are sympathetic to the Russians.

But if you listen to the discourse of the Chinese, and I don't have evidence that the Chinese are using disinformation, but I suspect they're just smiling all the way to the bank watching what the Russians are doing. Because what the Chinese are saying is, look, the next decade or the next century is the century of China. And just like Britain, at one point, they ruled the world, and now they're a second rate nation.

The United States is going to become a second rate nation. It has to become a second rate nation if China is going to dominate the world. And the best way to make that happen is to make sure we dissipate our energy internally by fighting among ourselves as opposed to focusing on advancing the energy and the power of our nation.

And I'd say that that's people who are trying to make that happen or doing a pretty good job of it. So you shouldn't underestimate the strategic intention of these foreign adversaries. We don't have wars anymore. We play games by different rules. And it's really interesting how they can be played online.

You mentioned these examples in the political sphere. But of course, it could be corporations doing the same thing or companies trying to maybe make comments about other products or things like that. Does the problem extend to that as well? What's the magnitude of this problem? And is there any way to quantify it?

I think it's hard to quantify. There are people who've studied very specific sectors. And certainly, if you look at something like this Tumblr persona that I described, it's really hard to say whether it had any influence at all. I think if you look at the big lie, well, what is it, 30 some odd percentage of people think that Trump won the election. That's a quantification.

But the point is I think we're seeing this at every scale. And what we're seeing here is an erosion in the relevance of truth. We're seeing an erosion of the concept of authority. Science deniers are deliberately sowing seeds of doubt about science, and we live in a very science technology oriented world today. It's a big loss.

And I think one of the most revealing moments to me was when I was talking to a friend of mine who is a very smart person but somewhat conservatively leaning. And this person said, well, yeah, I'm completely prepared to accept that fact Fox News is a source of disinformation on the right.

But since *The New York Times* is just as much a source of disinformation on the left, why should I believe anything? And the right has actually done a very interesting thing, which is they've taken the criticism of them and flipped it to say the situation must be symmetric. If Fox News is disinformation on the right, then *The New York Times* must be disinformation on the left.

There is no authority left. There is no truth left. So why don't you just go believe whatever you want? And that raises an obvious question, which is, what do you believe? And why would you pick something to believe? I think it's the corrosiveness that is the most serious issue we have to deal with here.

And what role does technology play in all of this? Does it create more problems? I mean, certainly, when we talk about big tobacco back in the day, the internet wasn't the internet, and it was a lot harder, I guess, to spread that disinformation. Where today, it would seem a lot easier.

I think it is easier. I think that's pretty obvious. There are several things that tech has given us. One of them because of the-- and it's really not-- it's not tech as tech, it's the way it's been put together. So we're really talking about-- well, to a certain extent, we're talking about behavior at the application level, not behavior of packets flowing from one side of the country to the other.

But a lot of the applications today give you tremendous power of amplification. If you have 10 friends, and each of your 10 friends has 10 friends, and so forth, and so on, if I forward to you, 10 people have it. If it's forwarded again, 100 people have it. If it's forwarded again, 1,000 people have it. If it's forwarded again, 10,000 people have it.

And exponential growth is a powerful source of big numbers. And of course, this has been deliberately exploited. If you want to get a little sense of this, you can go online as a search term, lookup Trump train, where you can see instructions that the right put together to help people build dissemination pipelines for relevant information so that it went out as fast as you could.

And they actually talked about this as a train, and there were conductors on the train, and they understood how to propagate this stuff. The next issue, of course, is the speed of propagation. If I click that button to send it to 10, and you click that button to speed it to 10, we're clearly in a cycle, where the only latency in the system is how long it takes you decide to forward it.

I mean, the internet's forwarding things that have the speed of light. So we're done. OK, you can't go faster than that. I can get something to the other side of the country and back less than a tenth of a second. So we're back to human reflex time also. And this is the Twitch world of playing games.

And I think the third thing that technology, again, because of the design of these applications, I don't know the right word to describe this. I'm going to call it promotion. But it's liking, it's upvoting, and so forth. And you can cause things in-- I think this is the language of Twitter. You can cause things to be trending.

And they pick trending things. And so by simply having 10,000 identities up click something, you can cause it to be trending. And then it's not just being sent to your 10 friends, it's being sent to people that you've never heard of before, because this is trending and you might want to see it. And I think there's another issue about technology that's fairly fundamental here.

Although the apps have exploited it, which is technology masks a lot of the cues we use to establish identity and trust. You don't know who you're talking to, you go to the grocery store, you go to the corner shop and you buy a coffee every day, they may not know your name, but they say, yeah, he's come in here every day.

I sort of have a sense of who this person is. We develop trust through continuity. You don't necessarily count on continuity on the internet, because you can always get a new identity anytime you want. And they're limited, but the social scientists would call the affordances of the channel to try to help you sort of build a model of who you're talking to.

And I think in that space, we're distanced from each other. That makes it easy for promotion to be based on bots, entities that don't actually exist. And of course, the Russians are creating bots as fast as they can, and they're using them to upvote things, and like things, and cause them to go trending. So it's a space where technology is not only intrinsically fast, but it's provided all sorts of tools to amplify and promote ideas which at the roots, it may have been disinformation.

So what factors are at the root of the problem?

Well, being a technologist, I like to begin by saying it's not just technology. And this is an area where I'll come back to this later if you want, but if you really want to study this problem, you have to come at it from a multidisciplinary angle. Because a lot of technologists say, oh, well, let's put a technology-- let's put some tech fix in there.

I've been collaborating in this space with a behavioral psychologist, who keeps saying to me, just tech may have amplified it, but stop thinking tech is at the center. What you have to understand, basic aspects of human behavior. Because the attackers fully understand this.

And if the attackers fully understand how to exploit attributes of human behavior, then the defenders have to understand that as well. So start talking to psychologists. Start talking to sociologists. So I might give you a couple of examples. But obvious one is why do people choose to believe what they do.

And I was talking about this earlier, how do they establish trust? What authority do they pick in a space, where there's been a deliberate attempt to erode authority? You listen to people you trust. They may not be knowledgeable, but they're sort of trustworthy.

And there's another dimension to this, which is really important, which is that the sense of belonging to a group may actually be a stronger driver of belief than an assertion of truth, and that we sort of-- we live in this academic space, where we sort of worship rational thought.

So we think about the rational human. And what my behavioral psychologist friend said, she said faith in the rational human is misplaced faith. And there are a lot of examples of places, where you can see people choosing what they choose to believe as a commitment to belonging to a community.

There are a couple of examples of this, which are sort of silly. I don't think the flat-earthers is disinformation. I think flat-earthers is a collective willful acceptance of a piece of misinformation for the joy of being part of a group. And some of them actually almost admit that.

They've interviewed, some of them said, well, maybe there it's not that. But I like to believe that. I like to believe something that they're willing to understand is sort of not true, but it is shaping their behavior. There's this guy who tied 50 helium balloons to a lawn chair and went up in the air to try to find the edge of the planet.

That guy could have killed himself thinking the Earth is flat. I mean, you know. And there's another dimension to this, which again like the woman I'm collaborating. She's named Sarah Wiedman. One of the things Sarah said to me was, there's a lot of literature on how people deal with rebuttal.

If you label something is wrong, what do they do? And a lot of the evidence is they doubled down on their belief. Because in fact, it's easy to look at the rebuttal and say, well, that must be the disinformation. And so rebuttal can backfire.

And there's this phrase called confirmation bias, where people are more interested in hearing things that support their belief, whereas the opposite of confirmation bias as people dismiss things that caused them not to believe. And there is this sense of psychological, physiological arousal. A tremendous driver of that is moral outrage.

And you can use moral outrage-- if you're an attacker, you can use moral outrage to trump critical thinking. And we've actually done psychological experiments that determine that some people are more susceptible to that, and other people or not. There are some people who in fact, because of their makeup, are more willing to come back and say, wait a minute, let's go back and sort of think about this, and there are other people who are just carried away.

So a lot of people associate this very simplistically with lack of cognitive ability. Those must be stupid people. And the answer is no, they're not stupid people. They're very smart people in that space, but they have a psychological buildup. But I think there's an interesting test in this space, which is, have we lost the ability to detect parody and satire?

And I would just quote something. It's worth looking this up online again if you want. It's something called Poe's law. P-O-E, Poe's law. And Poe's law was posed, I think, in the context of creationism. But Poe's law is a wonderful assessment of the current state of the world. Poe's law states without a clear indication of the author's intent, every parody of extreme view can be mistaken by some readers for insincere expression of the views being parodied. This is not technology. It's a much deeper issue than that.

So it sounds like you're saying that there might be a solution or could be potential solutions for solving this disinformation problem. But people might not be willing to adopt them, or they're happy with their ignorance belonging to a group of people. Even if that's disinformation is being propagated, they're willing to accept it, because they have the sense of belonging to a group, or they identify with the group's ideals. Is that what you're saying?

Yeah, that is what I'm saying. I think if you look at people who have a somewhat conservative point of view and you look at the reasons why they may choose to believe that Trump won the election, it's actually aligned with their wishes. This is, as I said, confirmation bias. And it's fairly easy when you're a group of people who have collectively decided this is what you want to believe, to just say, yes, that must be the reality that we choose to live with. And what you're really seeing is the alternative of sort of alternative realities here.

So let's talk about some of the proposed solutions for solving this disinformation problem.

Yeah. We can do that. But let me just give you a little context here, which is when you try to set out to solve this problem, one of the issues you have to address is, who owns the problem and its solution? It's not the creators. I mean, they're intentionally doing this.

It's not that you can take them off and sort of explain to them they're wrong. There's the channels through which this stuff is propagating, the tech platforms. There are the consumers or the propagator. And when you're trying to solve the problem, you have to say, where could you try to solve this problem and position it?

And again, you have to look at the motivations of the actors. Because if you're going to try to persuade them to incorporate some solution, it has to be aligned with their motivations. And we talked about the motivations of the consumers of this stuff.

But if you go to the literature and you read about various solutions today, there's a lot of papers that do what I-- there's a cynical phrase that's been used in this space, which is there are a lot of papers that spend a lot of time admiring the problem. And when you then read the paper about what they propose a solution, it's actually a very superficial analysis of the solution.

So for example, one of the things people say is, well, you should just-- we should just go to tag all the information as to whether it's right or wrong, and then we solve the problem. Well, no, of course, you haven't solved the problem. First question is, who does the tagging? By what authority do the tagging? And who would believe the tags?

How should the tags be used? If the tags are actually used to block content, it's become a very political process. Now, let me point out, there are other circumstances in which this works right. There are classes of content in which it's pretty easy to understand what the content is and whether it's crossed the line.

The most obvious example is child sexual abuse material. And in that case, there are people who tag, tagging leads to take down and prosecution. And that process works. I mean, there's a lot of CSAM out there. But this process works. Because it's pretty clear what the stuff is.

But in the case of disinformation, it's sort of like mushy. And so who gets to do it? And if the tag only produces a warning, a sort of a, this may be wrong, all we're doing is trigger the double down phenomenon. You can also say, why don't we teach digital literacy?

And the answer is actually, it appears the teaching digital literacy to kids has some benefit. But which personality types are most likely to internalize the lessons? It's not clear that the audience we most want to reach are the ones that we could internalize those lessons.

So you have to think about the incentives of the actors. And it's important to think about going to the platform providers who are propagating this and saying, you should change how your platform works. Because actually, much of what's happening here is to their financial benefit, that is to say.

Their economic incentive is to keep people on the site. Moral outrage is a great way to keep people glued to the site. You could sell lots of ads. So there's been a lot of evidence that these channels are actually propagating this stuff in what appears to be a deliberate way, because it's actually how they make money. Those are a lot of the limitations we have to deal with in this space.

Right. And we've seen that in the news recently with Facebook. Do you see any research being conducted about a trust score or data traceability inherenting these platforms? As we have Verisign for doing way back in the early days of the internet, we knew our credit card transactions were secure. Anything being done in that realm?

Well, I don't know about trust tagging. I think there has been some of that, but I don't know a lot about it. I think one of the problems we need to think about real hard in this space is how we think about online identity. And there is a lot of literature on that.

And if you go to Twitter, Twitter is very clear. They don't want to know who you are. It's wise. It's so easy to make these bots. Facebook says, we want to know who you are. LinkedIn says, we want to know who you are.

Now, in another part of my research, I have read the literature on the number of fake accounts that Facebook deletes on a weekly basis, and Twitter deletes on a-- LinkedIn deletes on a-- and the answer is we're talking about millions, not thousands. There's an interesting question, what rights of anonymous speech should be protected in social media?

Now, that, again, it's not a technical question. That's a societal question. But I think we need to think hard about that. Because one way you develop trust is through a sense that you actually can build up a model of who you're talking to. And as I say, you go into the corner store every day for your cup of coffee.

You may not know their name, and they don't know your name. But you have a sense who this person is. And if you've gone in for 100 days, and bought a cup of coffee, and went in one day and said, oh, my God, I don't have any change in my pocket. The guy behind the counter said, pay me tomorrow.

But he certainly wouldn't do that for somebody who hadn't seen before. So I think that you talked about trust scores. I think there's another knob you could turn in this space. There are specific things tech could do if they had the motivation, which means we need to think about the space of financial incentive.

You could damp the speed of certain sorts of content. And it turns out, we have some lessons for how to do this. These lessons don't necessarily come from a space, where we're very happy with what's being done. But the Chinese have really learned how to do this well.

What they're doing, of course, is controlling the flow of information, which may be right or wrong, but it's critical of the regime. But they know exactly how to take the domestic version of Twitter and slow down the propagation of retweeting or even turn it off. When a hot topic pops up that people are wanted, so they turn off retweeting. And they've learned if you turn it off for a couple of hours, people calm down.

Their outrage drains out. They go on to something else. You flood the channel with happy news, and they forget about it, and they turn retweeting back on again. If you want to change the, technology we've got worked examples. It's just that they come from a space where we're sort of uncomfortable with the objectives of the people who are doing it.

But that doesn't mean we shouldn't look at what they're doing and say, they actually know how to do it really well. How sad that is. How sad this is. But I really do think what we have to do to try to make progress here is to sort out who owns the problem. And I would just put in my own little personal plea here.

One of the things I've discovered in this space as an academic trying to do research in this space, nobody wants to fund research. The topic is so hot, for example, that the National Science Foundation doesn't want to touch it. They did some work on disinformation 10 years ago, and Congress wanted to shut them down so that they presumably could propagate disinformation.

They shut down the whole research-- they shut down a whole division of NSF to avoid having them fund research on disinformation. So even as an academic who's trying to find some traction here, you could say, I can't figure out who owns the problem from a point of view of funding, who owns the problem from an intellectual point of view. And it's so interdisciplinary. You've got to have technologists talking to psychologists, talking to sociologists, talking to economists. Boy, is it a wicked problem.

It certainly is. And I think it's interesting also that, say Donald Trump's Twitter account was shut down. So that sort of solved the problem from that perspective. And was that an overstep on Twitter as a platform and saying, well, you violated our terms of usage and things like that is that one way to curb this?

I think Twitter got so much, and Facebook are getting so much criticism in this space that they really felt they had to do something to protect the goodwill, never mind the revenue stream. And they're private actors. This is a space that's not regulated.

The private actors do not have to-- I mean, the First Amendment says the government shall not abridge free speech. A platform can do anything it wants. It'll get criticized no matter what it does. But it can do anything it want. It's a private actor. It doesn't matter.

The problem you get into in this space is the more you start curating the space, the more you run the risk of being classified not as a channel for propagation but as a publisher or an editor which gives you liability for the content. And there's a whole other conversation in this space we don't have time to get into, which is Section 230 of the Communications Act, the Communications Decency Act, which basically gives online providers channel, online for propagation of third party content protection from liability if they take some steps to curate the content.

If there is no Section 230, then either you're-- through your channel, you're common carry. You're just forward anything you're given to forward, and you have no liability. That's like the phone company.

You can be terrorists plotting over a phone call. The phone company has no liability in exchange for which they have to carry everything they're given. Or you're publisher, and you're responsible for the content. So there's now a movement, which I think is driven by the disinformation folks to repeal Section 230. So even law is entangled into this space.

Now, this is quite a bit of a departure from your usual work. What sparked your interest in online disinformation?

I've worked on the design of the internet, mostly not at the application level but at the packet carriage level, this platform that moves packets around and supports apps. I've worked on the design of the internet for 50 years. And I think starting 20 years ago, it became clear to me that the drivers of the character of the internet were not primarily technological, which is why I started collaborating with lawyers, and economists, and political scientists, and so forth.

What I'm concerned with all the forces that are shaping the future internet, and this is a very powerful driver, if you look at what other nations are doing, I talked about China, information control as a tool of regime stability, what we see there is an erosion of any sort of global internet. And that's a point that I'm both concerned about but also want to pay a lot of attention to. I can still send a packet from my computer to a computer in China. We haven't lost the ability for two people to exchange packets.

But China is clearly reshaping the internet experience in China completely. Russia is reshaping the internet experience in Russia completely. And they're more interested in cutting off some of the connectivity. They see, why don't my citizens need global connectivity? Well, that's a fundamental change in the character of the internet.

The other reason I'm interested in this is that this conversation does lead to some proposals to change the parts of the internet that I work on. An obvious example is there are calls for concepts of identity to be embedded in the packet layer of the internet. And I think that's a terrible idea for a whole bunch of reasons.

I think it's a terrible idea for social reasons. It would eliminate any possibility of anonymous action on the internet. And I think that's worth preserving up to the point. But also, I know that any mechanism that's put into the layers of the internet that I work on will immediately itself be attacked.

And I don't know how to build a system that provides global validation of identity that cannot be attacked. Look at the border routing protocols in the internet, the border gateway protocol. I study that a lot. It's constantly attacked by parts of the internet.

Look at the domain name system. It's constantly attacked by malicious actors. Look at the certificate authority system. It's constantly attacked. And that is a lot of my research is trying to understand and mitigate these problems. And people say, oh, let's add a new mechanism at that layer, which carries global human identity.

No, I just don't want to think about that. The other issue, of course, is hardening of sovereign boundaries through changes in the technical design. People are saying, why doesn't the internet have sovereign boundaries in it. I hope you change the protocol so we can find the sovereign boundaries. And that way, China can have the Chinese internet.

These things impact on the part of the internet that I work on. So that's why I'm concerned about these forces, which are arising at higher levels but really can change the character of the internet, including the lyric which I live. I've also been interested in problems with a multidisciplinary character.

And this is a prime example. There's economics, there's law, there's political science, there's sociology, there's psychology. There's a set of collaborating with a behavioral psychologist in this space. There are also some other interesting technical specialties. I don't know whether you've done a podcast with Una-May O'Reilly here in CSAIL.

But her specialty is adversarial AI. And without trying to explain what adversarial AI is, you should get her to explain what it is. You can imagine, well, that could be a tool in combating disinformation, so let's go study this space. So there's just a sort of, wow, this problem brings in almost every field. And we just have to shift the paradigm by embracing cross-disciplinary research. So that's another reason I'm interested in this.

We are interviewing Una-May in an upcoming podcast. So we'll be talking with her about that for sure. Is there any other research or insights that you're excited to share with us?

Well, as I said, my long term interest in the design of the internet, I'd say at least for 20 years, it's been focused on security at the packet transport layer. And I'm very concerned with the fact that almost all of the systems that builds the basic packet transport layer are deeply flawed or at least deeply vulnerable at the foundational layer.

So the border gateway protocol allows malicious parts of the internet to try to hijack address blocks and take traffic that should be going to you and go to them instead. That's one of the strategies that's used by fishers. It's not the only strategy that's involved in phishing email, but it's a component of it.

If I can send you to the wrong place, I can then put up a fake website, steal your credentials, and you could say, well, doesn't the certificate authority system give us a cryptographic protection? That's why the certificate authority system is always under attack. I'm deeply offended at all of the abuse of the domain name systems.

There are thousands of names registered every day that clearly are only intended to support phishing, or scams, or things like this. So a lot of the research that I'm doing right now is really trying to understand and basically figure out how to mitigate some of these security challenges at the packet transport layer.

And where could people go to find out more about your research?

Well, the standard thing I tell them is through casual interest. Go to the CSAIL website. I mean, we try to keep it up to date. Of course, we know where the current repository of all scholarly knowledge is today, it's in scholar.google.com.

And you can obviously go look for me there and see all the papers I've written. And obviously, for serious interest in this space, I'm always happy to talk to people. But start with the CSAIL website. I should go look at it, make sure it's up to date.

It has actually been updated fairly recently. So we just did an update on it and would encourage people to go to csail.mit.edu for information on David, and all our other principal investigators, and what's in the latest research at CSAIL. David, this been a fascinating topic.

I would definitely like to have a follow up with you at some point in the future to talk about this, because it's so multifaceted, and there's so many areas that I'm sure our listeners would be interested in finding more about. But thank you very much for your time. We appreciate it.

You're very welcome. It's fun.

If you're interested in learning more about the CSAIL Alliance program and the latest research at CSAIL, please visit our website at cap.csail.mit.edu. And listen to our podcast series on Spotify, Apple Music, or wherever you listen to your podcasts. Tune in next month for a brand new edition of the CSAIL Alliance's podcast, and stay ahead of the curve.