The focus is on the AI algorithms and the models themselves, and it may be used within weaponized AI attacks, but when you're going after the actual algorithms and

Jennifer are taking this mindset and putting it maybe a little more subtly in terms of not necessarily just attacking the common good, but attacking supply chains. Maybe competitors are doing skunk works on each other's supply chains and stuff. Can you, Jennifer, describe some of dangers that adversarial machine learning and AI could present to an organization's supply chain.

Jen also mentioned open source so imagine this is an open source module that you're used to using, but within that module you've got in a different copy and so your module is using a module, is using a module, is using a module on that last module so it's like a butterfly wing where that impacts the code maliciously so that's a pitfall. How can we look at each element within the supply chain and software and building a AI more to the point? How can we better do that? Couple of recommendations.

One, we can take what we've learned from the cyber practices and perform zero trust audits on open source modules so hash checking is not enough, which is what's being done today. We also use which I think would be interesting is use AI programs on the software themselves, so that they become assistant software code auditors anyone too much but the idea is that you pretty much look at a, you have two models side by side and what it was originally designed to do was to help generalize them.

When they are trying to identify something they can work in harmony. That was what it was initially designed to do. The side effect of that is that they realized it's actually really perfect plug up backdoor. When they made it so that these two models are being generalized with each other and you don't minimize their accuracy and the developer has full control over what points to pick, like, how am I going to make

so they oversee the protection of our critical infrastructure, but how might these be exploited using adversarial AI? AI can provide automation to these attacks and a

social engineering platform to recruit for say terrorist organizations but also you can do the spread of misinformation. Like you said, tweaking things just a little bit I mentioned a fraud that could happen.

On a very small scale, of course, you can pretend that a dead person is still alive. You can keep saying that someone works for you and actually you can make up your own company and say that there are 200 people that work for you, but actually, none of them exist. It would require different organizations to be more cognizant of who they're going into business with because usually you just do.

I was going to mention that, yes.

This consensual universe, we're going to all participate in it's like, oh my goodness, it's a Pandora's box of like who knows. Anyway, I guess that's neither here nor there that's a whole other discussion. Obviously, we're just starting to really understand the dangers and the opportunities that all of this technology affords us. I really appreciate sitting down with both of you, Jennifer and Charles today to talk about this idea of adversarial AI.

Obviously, there's going to be a lot more to be said in the days ahead, but I really appreciate you both for your expertise and your insights. Thank you so much.

Thank you. This has been great.