Keeghan Sweeney: hi! Everybody. Thanks so much for joining our faculty, focused Webinar, hosted by the Uba Law School Foundation my name is Keegan Sweeney. I'm. A to off the law school. I'm. Originally from California, but happy to call Charlotte from my home now. given just how wonderful a place Uva is.

Keeghan Sweeney: and I recognize that it's a no small part because of our alumni. Like all of you guys, as well as a lot of the good work that the law school foundation does as well.

Keeghan Sweeney: so i'm especially excited for the opportunity to introduce Professor Ashley. Geeks, all of you today. because i'm fortunate enough to be enrolled international security. A lot class currently.

Keeghan Sweeney: the class has been absolutely fascinating, and covers a lot of issues that are only growing in importance, kind of ranging from what's going on in Ukraine right now to the legality of domestic surveillance programs, 150

Keeghan Sweeney: so as for student, I get to testify that Professor Deeks is teaching ability is really as impressive as her scholarship is and her service to the country.

Keeghan Sweeney: So Professor Deech, our Deeks joined the Law School in 2012 as an associate professor of law. After 2 years as an academic fellow at Columbia Law School, she recently took a seventeenth month hiatus to Service White House Associate Council and Deputy Legal adviser for President Joe Biden's National Security Council, her primary Research and Teaching interest or in the areas of international law, national security, intelligence, and the laws of war. But before joining the Academy she spent 10 years working in various capacities

Keeghan Sweeney: at the Us. State Department's office of legal advisor, including as assistant legal adviser for political military affairs, working on issues related to the law of armed conflict. The use of force, conventional weapons, and the legal framework for the conflict with Al. Qaeda.

Keeghan Sweeney: She's also written articles on the use of force, Executive power, secret treaties, the intersection of National security and International law and the laws of armed conflict. She's a member of the State Department's Advisory Committee on International Law and the American Law Institute, and she serves as a contributing editor to the Law Fair Blog.

Keeghan Sweeney: Professor Deeks also serves on the Board of Editors of the American Journal of International Law, the Journal of National Security Law and Policy, and the Texas National Security Review. and finally, and certainly not least She's also Senior Fellow of the Labor Institute for Law and land warfare as well as a faculty senior fellow at the Miller Center.

Keeghan Sweeney: so we're actually gonna start with Professor Beeks giving some remarks, and then she's been kind enough to take questions at the end of her presentation. At any time during that presentation. If you have any questions, please just click the Q. A. Button on the bottom of your screen, and we'll get to as many of your questions as ken as we can, and with that i'll turn it over to Professor Deeks

Ashley Deeks: great Keegan. thank you so much for being willing to take time away from your studying to moderate this.

Ashley Deeks: I know you have a number of exams coming up, and thanks also to the foundation's Alumni Relations Office for pulling this together. So i'm delighted to be able to to talk to you today, and i'm looking forward to hearing your reactions and questions. after I've made some comments.

Ashley Deeks: so I thought I would start by talking about a project that i'm currently what working on? That's about the role of artificial intelligence, or what's commonly called AI

Ashley Deeks: in us national security.

Ashley Deeks: So I want to say a little bit about how I came to the project, and what I hope to do with it. it is still a work in in progress. So the end remains to be seen. But I thought I would start with that. And then at the end, I wanted to make a few broader points about the way in which technological tools are

Ashley Deeks: changing the face of us national security, and also changing the the players who are operating within that sphere.

Ashley Deeks: So i'll start out by talking about my my book Project I'm, currently working on a project that I think is going to be called something like the Double Black Box National Security AI, and the struggle for democratic accountability.

Ashley Deeks: and I I came to this because i'd been researching and writing in 2 different areas. And and I think this project really kind of brings those areas together.

Ashley Deeks: So the first thread of work that i'd been developing had to do with the role of AI in national security.

Ashley Deeks: So I suspect that many of you have heard of AI and machine learning, I'll say just a little bit about what it is for those of you who may not be as familiar with it.

Ashley Deeks: So machine learning algorithms generate predictions by allowing the data itself rather than human programmers

Ashley Deeks: to dictate

Ashley Deeks: how the information in the inputs is assembled to forecast

Ashley Deeks: the value of an output.

Ashley Deeks: So computer scientists who are using a lot of data, we obviously have a lot more data today than we ever have before.

Ashley Deeks: and also using powerful computers. They're developing algorithms that can help make predictions about things, and they can make those predictions faster and sometimes more accurately than humans can.

Ashley Deeks: So

Ashley Deeks: you may have been. You may be familiar with algorithms that can recognize and classify things such as cat photos on the Internet, or, more seriously, things like lung cancer.

Ashley Deeks: where the algorithms reward or punish, the the the developers of the algorithms reward or punish the algorithms based on their error rates and over time the algorithms learn how to correct and improve their predictive abilities.

Ashley Deeks: So we see this in Netflix recommendations about what movies you might want to watch next. we've seen it in the game of go where computer scientists have developed an algorithmic gay game player that can actually beat the most sophisticated human players of the game.

Ashley Deeks: So I, to give you a very specific example that I think is is powerful. There are now algorithms that

Ashley Deeks: can detect lung cancer in X-rays.

Ashley Deeks: So the programmers showed the the algorithm a 1,000 slides.

Ashley Deeks: 500 with cancer, 500 without.

Ashley Deeks: and they tell the system which is which.

Ashley Deeks: The algorithm. Then extracts the relevant features of the cancer slides.

Ashley Deeks: Even if a human can't really identify what exactly it is that the algorithms are focused on.

Ashley Deeks: A computer scientist will then come in and test the machine learning, algorithm

Ashley Deeks: using 200 new slides that the system has never seen before.

Ashley Deeks: and see how well the algorithm can identify those with cancer and those without.

Ashley Deeks: And they're now at a point where these algorithms are doing better than human doctors. even though

Ashley Deeks: we don't always know how the algorithm is reaching its conclusion or prediction.

Ashley Deeks: So this is the black box that people sometimes refer to when they're talking about machine learning algorithms and deep neural nets.

Ashley Deeks: These systems have already started to appear in government decision making outside the national security spear.

Ashley Deeks: So for example, the Social Security Administration is reportedly using machine machine learning

Ashley Deeks: to adjudicate disability benefits cases.

Ashley Deeks: and the Sec. Is reportedly using machine learning to try to target enforcement efforts under the Federal Securities laws.

Ashley Deeks: So what i'm interested in is how the Government is going to start to use these systems in the national security space. So

Ashley Deeks: how is the military going to use these systems, and how our our Intelligence Agency is going to use them.

Ashley Deeks: I think it's quite clear that States, like the United States and China, and maybe to a lesser extent, Russia and Iran and Israel

Ashley Deeks: very committed to developing artificial intelligence for military uses.

Ashley Deeks: the the People's Republic of China has said that it sees AI as a race that it needs to win.

Ashley Deeks: and we can imagine why that's the case. So if we're talking about systems that can make more accurate predictions or recommendations.

Ashley Deeks: if we're talking about systems that can spot patterns in data that humans can't

Ashley Deeks: that can churn through huge quantities of data really, quickly.

Ashley Deeks: If we're talking about the ability to react with speed that can be useful. For example, in the cockpit of a fighter Jet

Ashley Deeks: if you're talking about systems that can help avoid human cognitive biases.

Ashley Deeks: or making sure that your decisions take into account all of the relevant information.

Ashley Deeks: and not take into account irrelevant information.

Ashley Deeks: Those are all really

Ashley Deeks: useful things that that machine learning that AI can do. And so I think it's easy to imagine how some of those those advantages would really enhance war, fighting and intelligence, collection, counter espionage, and things like that.

Ashley Deeks: There's been a lot of ink spilled about one particular type of artificial intelligence, and that is

Ashley Deeks: often referred to as lethal, autonomous weapons, systems

Ashley Deeks: which some now shorthand as laws so us as lawyers. We might not love that acronym. But I will refer to them as as lethal autonomous weapons systems here.

Ashley Deeks: These are machine learning systems that have been trained to identify particular types of targets

Ashley Deeks: and then be launched by States onto the battlefield.

Ashley Deeks: The idea is that the systems would be able to detect targets, either people or maybe military objects, tanks

Ashley Deeks: and so on.

Ashley Deeks: and then initiate force against them without additional direction from the military commanders or operators.

Ashley Deeks: And so you can see why Why, that would get a lot of attention. And indeed it has. It's been the subject of a lot of discussion in some international groups meetings in in places like Geneva.

Ashley Deeks: But I'm also interested in kind of pushing beyond that one case i'm interested in other situations in which

Ashley Deeks: militaries and intelligence communities might start to use AI in their systems.

Ashley Deeks: And since AI tools are, as I've said, good at making predictions and good at detecting anomalies.

Ashley Deeks: militaries, and intelligence agencies can use these tools, I think, to help determine

Ashley Deeks: who's most dangerous.

Ashley Deeks: which actors are connected to To whom.

Ashley Deeks: when, and where should a military go on patrol and so on.

Ashley Deeks: I with with a couple of other colleagues. I've also written a a piece trying to think through how States might use these tools to even predict incoming attacks before an armed conflict starts.

Ashley Deeks: So, when might other States or non-state actors

Ashley Deeks: be in a position to attack? Where might that attack come from

Ashley Deeks: what kinds of responses would be proportionate?

Ashley Deeks: I also am worried that States are going to start to use deep fakes which are systems driven by AI to try to deceive their adversaries, to try to trick them into using violence. as a result of seeing a deep fake, for example, of a

Ashley Deeks: a foreign leader ostensibly scheming about a future attack.

Ashley Deeks: I also think there's a room in cyber for for AI and cyber autonomy. I think this, in fact, might be the first area where we'll actually see one

Ashley Deeks: true autonomy in the National Security Space

Ashley Deeks: People have written about the ability of autonomous cyber tools to hunt out vulnerabilities in these in the adversaries systems.

Ashley Deeks: And of course, if we're talking about speed, cyber is a place where you really need to act with

Ashley Deeks: great haste and responding to incoming attacks.

Ashley Deeks: But of course those are all. Maybe some of the positive cases for use of AI, and some of the places where our system might see that as useful. But there are problems with AI as well.

Ashley Deeks: there's been a lot of criticisms about how companies or governments have developed AI that produce bias bias predictions, because the the data that they, the systems have been trained on reflects an earlier bias.

Ashley Deeks: Some other people talk about automation bias by the users. That is this idea that you might

Ashley Deeks: mit Ctl.

Ashley Deeks: And then, finally, and I think most importantly for my project. There's a concern about the lack of transparency, about how these pretty systems are producing their their outputs, their recommendations. it is often opaque both to the users of these systems

Ashley Deeks: and to the obviously to the subjects or targets of the systems. How exactly a particular algorithm reached its decision.

Ashley Deeks: So that's thread. One of my my thinking about national Security and AI.

Ashley Deeks: The second thread of my scholarship is interested in something slightly different, which is the challenge of government secrecy in a democracy.

Ashley Deeks: especially where that secrecy is manifested in national security, policies and actions.

Ashley Deeks: So, as many of you, I'm sure know a lot of what the Us. Government does in the national security. Space is classified

Ashley Deeks: and often classified for good reason.

Ashley Deeks: but with secrecy comes certain pathologies.

Ashley Deeks: You don't have to test out your ideas or your policies as publicly as you do when they are going to be open, and out there ex ante.

Ashley Deeks: You can use secrecy to conceal legal violations or embarrassing mistakes that you've made.

Ashley Deeks: So when we're thinking about

Ashley Deeks: government secrecy, and we're evaluating it. I think what we're really worried about is trying to make sure that the Government is complying with

Ashley Deeks: what

Ashley Deeks: what we might call public law values.

Ashley Deeks: So these are things like legality and efficiency

Ashley Deeks: and accountability for mistakes

Ashley Deeks: and competence and fairness.

Ashley Deeks: And so how do we check the executive branch today. On those, how do we figure out whether it's complying with public law values? Well, we rely heavily on

Ashley Deeks: mit ctl and parts of Congress and parts of the courts. For that we rely on certain Congressional committees like the Intelligence Committees or the Armed Services Committees

Ashley Deeks: to look behind the the secret curtain that the Executive has.

Ashley Deeks: and in terms of courts we have a body called the Foreign Intelligence Surveillance Court.

Ashley Deeks: which evaluates government applications for electronic surveillance which are obviously sensitive

Ashley Deeks: and the Fisk serves as our surrogate there to check, to make sure that the Executive is complying with those public law values.

Ashley Deeks: I'm. Also, though interested in how those primary checks that is, the courts in Congress are insufficient.

Ashley Deeks: it is often hard for Congress to oversee and regulate

Ashley Deeks: a wide range of intelligence and military actions. Sometimes this is because of their lack of capacity or their lack of interest. Sometimes it's because the executive may withhold certain information from Congress

Ashley Deeks: and the courts.

Ashley Deeks: tend to be quite deferential to the Executive.

Ashley Deeks: So these are important checks, but they're not

Ashley Deeks: always hugely robust checks. So I think this means we also we we end up relying on other less obvious actors that interact with the executive, and that can actually also check it

Ashley Deeks: behind this veil of secrecy.

Ashley Deeks: So, for example, corporations, I think, are serving as checks today, especially in

Ashley Deeks: the cyber setting.

Ashley Deeks: These corporations are basically gathering what we would call intelligence if it were a government agency that was collecting the information

Ashley Deeks: mit Ctl, and they share that information with the Government. The Government shares information with them. They can check whether they agree with the analysis that the Government is providing them. So think Microsoft and Google, these really sophisticated companies, 150.

Ashley Deeks: We also have actors, like our allies, especially NATO allies, allies from from Europe.

Ashley Deeks: who impose constraints on us

Ashley Deeks: in the military and intelligence space. When, for example, we are engaged in classified joint operations.

Ashley Deeks: they actually sometimes impose an additional layer of laws on top of the laws that our own officials have to comply with.

Ashley Deeks: and they can call us out if our officials are doing something that seems improper.

Ashley Deeks: and I found a number of cases historically where that's happened.

Ashley Deeks: maybe counterintuitively, I think executive branch lawyers themselves can serve as a kind of non traditional check on what's happening in secret and interagency Negotiations among lawyers really serve as their own kind of check

Ashley Deeks: that helps the executive sharp and its legal arguments, and make sure that it's complying with the law.

Ashley Deeks: And interestingly, I think states and localities are also starting to serve as if not active checks, at least players in this space. So, as we all know, states have a huge role to play in elections.

Ashley Deeks: and they have a big role to play in cyber because they're often the ones that are controlling these more regional electrical power grids or water systems, and so on.

Ashley Deeks: They can share intelligence with the Federal Government. The Federal Government can share intelligence and operational plans with them.

Ashley Deeks: and then, finally, I I should just mention leakers, which are, of course, not a kind of constitutional actor who checks, but have long been in the system as a way to check the executive branch.

Ashley Deeks: So, even with these additional kind of nontraditional checks. It is a highly imperfect system.

Ashley Deeks: And yet, as I was stepping back, I realized that there's a really, I think, an important overlap between these 2 areas of scholarship that I had been thinking about in writing it.

Ashley Deeks: So if you were already worried

Ashley Deeks: about governments doing things in secret

Ashley Deeks: that are hard for you as a citizen to know about and to evaluate

Ashley Deeks: what happens when those national Security decision-makers start using new sets of tools that you

Ashley Deeks: and they may not be able to interpret or understand very well.

Ashley Deeks: So I think that this is potentially going to double down on this public law values problem.

Ashley Deeks: So the goal of my project is to really explore how bringing machine learning other types of AI into the national Security ecosystem are going to exacerbate or double the existing black box problems.

Ashley Deeks: So machine learning may exacerbate the citizens inability to know what the government's doing in our name.

Ashley Deeks: It may exacerbate the ability of our usual proxies to know and understand what the Executive is doing. That is.

Ashley Deeks: Congress in the courts may have a harder time.

Ashley Deeks: and it might even make it harder for the executive branch itself. The actors within the Executive to explain why they made certain decisions.

Ashley Deeks: and I think it could potentially undercut some of the strengths of these alternative checks that I mentioned

Ashley Deeks: the the poll, the the I think, helpful interagency disputes that you sometimes hear about really produce, I think, a useful push poll that tries to get the Executive to the right policy place.

Ashley Deeks: and if you have some agencies that are much more sophisticated in things like AI and Ml. Than others. That push poll is going to break down a little bit.

Ashley Deeks: Think about leaks, too. Leaking an algorithm is so different from leaking a memo that anybody who can open the the the New York Times Could read.

Ashley Deeks: and from the legal perspective people in these General Councils offices may have a harder time understanding the tech, or be able to get involved in the front end development of these systems where it would be really useful to make sure that legal issues and legal parameters are taken into account. As you are building these tools.

Ashley Deeks: And yet right. And yet we are still going to come under pressure to adopt these tools, I think, especially because Russia and China are very committed to them.

Ashley Deeks: So how do we strike this balance. How do we ensure that the Executive continues to pursue the public love values that we want it to?

Ashley Deeks: without leaving the us behind?

Ashley Deeks: So that's really the thrust of the book.

Ashley Deeks: and the project really mostly focuses on the double black box in the United States.

Ashley Deeks: But I think the challenge that i'm hoping to describe is one that's probably going to hold true for a range of democratic states. and NATO allies, and I think our allies can be useful here in helping us think through the costs and benefits of using certain types of national security, AI.

Ashley Deeks: And joining with us to condemn other States if we see them using these tools in unacceptable ways.

Ashley Deeks: I think it's unlikely that we're gonna see a new treaty emerge that purports to regulate national security. AI: so I think it's really going to be important to get our own checks and balances and our own values clear in our mind on the domestic side.

Ashley Deeks: And finally, I just think it's important that lawyers, including those who are working in the national security space.

Ashley Deeks: understand, or at least are willing to try to learn the basics of tech

Ashley Deeks: related to machine learning related to cyber.

Ashley Deeks: and also maybe tools like encryption.

Ashley Deeks: So I want to just quickly shift in the last couple of minutes. Say something about

Ashley Deeks: what I think we're starting to see is a broader shift within national Security law.

Ashley Deeks: So AI, I think, is just one example of how novel tech tools present both challenges and opportunities

Ashley Deeks: for governments that are concerned about their national security.

Ashley Deeks: So, as as Keegan knows, because he has been in my class. This semester AI is not the only area in which tech tools that we use to connect with others.

Ashley Deeks: Cyber Telephony apps are really changing the face of national security.

Ashley Deeks: So we do current events. in my national security law class at the beginning of class, and in almost every class this semester there was a news event related to tech threats to the Us. Government or to us citizens

Ashley Deeks: studying national security used to mean really focused on? What are the domestic laws related to going to war? What is the international law related to war?

Ashley Deeks: What about espionage? How does covert action work.

Ashley Deeks: Those were kind of the Core national security issues.

Ashley Deeks: but many, many of the national security developments in the Us. In the past few years have really been focused on tech threats and particular threats from China.

Ashley Deeks: So

Ashley Deeks: this includes China's use of both its own legal system and technologies inside China.

Ashley Deeks: right to build new AI tools

Ashley Deeks: to demand access to data from us companies that are doing business inside China.

Ashley Deeks: I think. Google

Ashley Deeks: we're also seeing the sale of Chinese, Chinese sourced technology inside the United States.

Ashley Deeks: Huawei inside state and local fiveg networks

Ashley Deeks: drones produced by Dji, a Chinese company being used by hobbyists and being flown in places that worry us a little bit, including

Ashley Deeks: over the national capital region.

Ashley Deeks: We're starting to see reports about self-driving cars manufactured in China being sold here, and a concern about the kinds of data they might be collecting and sending back 150

Ashley Deeks: into China.

Ashley Deeks: We also have issues related to the acquisition of us source components by Chinese companies, meaning things that Us. Companies are making here that could be exported to China. So we've seen past administrations basically say no more sales to Huawei or Zte

Ashley Deeks: limits on selling semiconductors to China semiconductor chips.

Ashley Deeks: We're also we've been thinking about acquisition by Chinese companies of assets inside the United States. Right? The the sfiest process. Sophia is actively reviewing Tik Tok.

Ashley Deeks: and news reports suggest that even though it seemed like maybe there was going to be an agreement.

Ashley Deeks: There are still national security concerns that the Us. Feels haven't been addressed.

Ashley Deeks: and then, of course, we have the steady diet of cyber operations and espionage. So these are all thought to pose serious national security threats. So how do we think about these threats. The us has a huge surface area for other countries to target.

Ashley Deeks: We have tons of high, you know. High-tech us companies here.

Ashley Deeks: Some of them have offices overseas. We have a large defense industrial base.

Ashley Deeks: We have many us citizens who spend huge amounts of time on their devices, producing data

Ashley Deeks: and the target surface

Ashley Deeks: for foreign adversaries, I think, is only going to grow right as we continue to adopt the Internet of things in our houses, houses, and elsewhere.

Ashley Deeks: I think there's a really interesting, significant role for new actors to help the Federal Government detect and address the threats.

Ashley Deeks: I've already mentioned companies as a possible check.

Ashley Deeks: I've mentioned that not just to check, but I guess also a an ally to sort of help us push forward to protect our security

Ashley Deeks: and states and localities. We're seeing that Maryland just banned the use of tik tok in its own Maryland Government systems and banned Huawei in those systems as Well.

Ashley Deeks: we're seeing different parts of the executive branch than we're used to helping advance our national security right? So we usually think about Dod, the Intelligence Community.

Ashley Deeks: We're now really talking more about commerce. The Commerce Department, the Treasury Department, the State Department for Export controls, for sanctions for Sophia's.

Ashley Deeks: Many of these systems have dual uses, right? So we're not just going to ban the systems. We can't just make them unusable because civilians get a huge amount of benefits out of a lot of this technology.

Ashley Deeks: and because of our interconnectedness, technologically with our allies, we need them to be on the same page as we are.

Ashley Deeks: so otherwise, our adversaries are just going to penetrate our systems, this by going through our adversary systems.

Ashley Deeks: So there are lots of existing legal tools out there for the Executive to use statutes like Iipa, the Export Control Act, Sophia and Fermat

Ashley Deeks: but I think it's useful to really think about whether the overall legal framework we have is sufficient. Is it appropriate? Are there things we could be doing

Ashley Deeks: better?

Ashley Deeks: So I think it's a fascinating time to be a national Security lawyer and a scholar, and the stakes feel pretty high to me, so i'm i'm happy to be doing this.

Ashley Deeks: I'm going to hand it off now to Keegan, who will help collect and

Ashley Deeks: and and ask your questions. so with that i'll turn it over to Keith.

Keeghan Sweeney: Yeah. So Professor Deeks thanks so much for for that presentation. Obviously fascinating stuff, and can't wait to hear more about what you find after you're further along in the research project. but just as a reminder to all of you. you can submit questions if you just look at the Q. A button at the bottom of your screen. we've got a bunch already, but we'd love to take more and hear what you guys are curious about. but let's start with a question from John White, Professor

Keeghan Sweeney: And John asked the People's Republic of China has put very few limits on the development of artificial intelligence as well as big data management systems. And so the question is would implementing an extremely conservative approach within the Us. on the development of artificial intelligence

Keeghan Sweeney: put us at a strategic disadvantage in the near future. and kind of the flip side of that question. If if I can just add something would be. Does pressure from competition with China make us pay less attention to those public law values that you described earlier.

Ashley Deeks: Yeah. So that's a great question, and it really kind of goes to the heart of my project. So

Ashley Deeks: I think. In short, the answer is.

Ashley Deeks: yes,

Ashley Deeks: concerns about

Ashley Deeks: exactly the kinds of tools that the Prc. Is going to be able to develop

Ashley Deeks: are are certainly relevant to the kinds of tools that we're going to face pressure to to deploy

Ashley Deeks: and and so whenever you're in a kind of competitive posture you know, it's more likely that your values will be tested.

Ashley Deeks: But I think where I've landed on this and again, the last parts of the book have not been written. But I think my take is really going to be that we need to to decide on our own

Ashley Deeks: kind of apart from what any other

Ashley Deeks: adversary is doing.

Ashley Deeks: where our own values and limits leave us, and that should really be our our guide star.

Ashley Deeks: And so, to some extent the Us. Government has already started to do this. The Defense Department and the Intelligence Community have put out principles related to ethical use of of AI

Ashley Deeks: that put out documents that try to help those who are developing a. I ask the right questions in in thinking about it.

Ashley Deeks: I think we need to go down a level of detail. I think that there's a fair amount of agreement

Ashley Deeks: within within Western States about kind of what the

Ashley Deeks: the basics we should all follow in AI accountability, transparency reliability, those kinds of things. But it gets once you once you get below that it gets harder. And so I think where the work really needs to be done right now is that that slightly more granular level of analysis

Ashley Deeks: and thinking about what we do, and Don't want our Government to deploy in our name. And so, you know, I think part of this is just having public start to think about this stuff and be able to talk about

Ashley Deeks: erez agmoni to journalists or to you know, in public for it to their congressperson what kinds of things they they think do, and don't make sense 150.

Ashley Deeks: I think the Government should try to be as transparent as possible about the kind of challenges that it's confronting, so that we can kind of react and say, Yes, this is a tool we, of course, think the Government should use and know. This is when they shouldn't. But I think at the end of the day, while while countries like China will be putting pressure on where we want to go. With this.

Ashley Deeks: I think we ultimately need to stand on our own. with regard to what values we wanted to represent.

Keeghan Sweeney: All right. So next question, coming from Harvey binds

Keeghan Sweeney: and I think you mentioned this briefly. Maybe we could dive into a little bit more detail. But could you address if there are any AI connections to Fermi or Cfius oversight and compliance generally. So you know to what extent is artificial intelligence already being used in those processes. What is the potential use?

Keeghan Sweeney: I'm curious if you could discuss that, and maybe just to find Cypius for the group, too.

Ashley Deeks: I'm sure. So Sophia is the Committee on Foreign Investment in the United States.

Ashley Deeks: and it's basically a group of actors from different government agencies, the Treasury Department and State and Justice and defense that are trying to evaluate whether a potential acquisition

Ashley Deeks: from a foreign actor of part of a Us. Company, or in some cases us real estate

Ashley Deeks: would implicate national security concerns in a way that would

Ashley Deeks: cause us to either block the deal, or more likely try to impose certain regulations on the deal To minimize those national security concerns. and i'm sure there are people on this call who who practice in this area who will know it better than I do.

Ashley Deeks: but I so I think it's an interesting question. I'll just say

Ashley Deeks: I should say i'm speaking only in my personal capacity, not in reliance on anything that I did in the government. But in this case I have no information about whether, there are

Ashley Deeks: considerations being given to using machine learning tools in the space, but I

Ashley Deeks: I guess I can imagine that just like the Sec. Is starting to try to use machine learning to

Ashley Deeks: detect potentially

Ashley Deeks: concerning transactions that they might want to pursue in an Enforcement matter. You could imagine, trying to use machine learning to look at the whole bucket of potential acquisitions that are out there about which there is some public information.

Ashley Deeks: to try to detect whether there are some deals that we're worried about that haven't been brought before Sophia right? It is effectively a a voluntary process to bring yourself before Sophia. If the Government hasn't, I guess the Government can also identify an issue of concerns to a spontane. But

Ashley Deeks: you know the the place where where AI and machine learning function best is where there's a lot of data. So I guess you'd really want to know how many transactions there are every year that could potentially implicate Cypius. And if there are a ton. Then that might be an area where you might want to think about trying to develop some machine learning tools.

Ashley Deeks: If there are 20 or 30, then it's probably just easier to kind of do it. Do it manually

Keeghan Sweeney: great. Okay. So next question from Mike Gowdy. So, Professor Geeks, you recommended that national security lawyers get smart on technology. AI and Ml: issues. Do you have any recommendations for good places to start?

Ashley Deeks: Hi, Mike?

Ashley Deeks: There, that's a that's a really good question. So

Ashley Deeks: one place you could start is

Ashley Deeks: looking at a couple of the recent reports from the National Security

Ashley Deeks: Commission on AI

Ashley Deeks: this is a a a hardy assignment, because the reports are hundreds of pages. But even just looking at the executive summary is a good place to start. This was a commission set up by Congress

Ashley Deeks: mit ctl and sort of to mirror the Cyber Solarium Commission, really stepping back and taking a holistic look about where the country is on a AI, and where it needs to go 150.

Ashley Deeks: and it was. It was led by people like Bob Work, who really tried to get the Defense Department smarter and faster on a AI, while he was there.

Ashley Deeks: That Commission actually

Ashley Deeks: takes a pretty forward-leaning approach to AI. With this taking taking the the approach that

Ashley Deeks: we're going to fall behind china on current pace, and we really need to to be pushing harder and and doing more in this space. so it's a little bit, I think, leaning a little bit more forward than than I am, but it's a very helpful primer.

Ashley Deeks: and there are also there are people at the center for New American security who are doing excellent work on this Paul Shah has written a book called Army of none where he's really thinking about the kind of lethal autonomous weapons system use of tools. So that's a great book. And and Cnn. Has done a lot of reports on this

Keeghan Sweeney: mit ctl and Alrighty. So Kimberly Cobb asks how concerned should we be as a society about the risk to us, national security associated with the rise of AI globally 150

Keeghan Sweeney: so not necessarily just being employed by, say it actors, but also non state actors. and she's particularly thinking about the consequences of acquiring generalized intelligence. And maybe, Professor, if you could just distinguish between the algorithms that you're talking about here, and what generalized AI is

Ashley Deeks: sure. So so the algorithms I've been talking about are generally thought of as kind of narrow AI, where the algorithms have a pretty specific purpose. A pretty specific question that they're trying to answer

Ashley Deeks: General AI, or artificial general intelligence, as it's sometimes called, is

Ashley Deeks: the idea that we will be able to develop systems that can effectively think like reason like, make decisions about detect causation in the same way that humans can.

Ashley Deeks: So this is a little bit more the sort of terminator future.

Ashley Deeks: and there is an active debate among people who are much smarter than I am on the the tech on this about whether this is

Ashley Deeks: never going to happen

Ashley Deeks: might happen in 20 years might happen faster, we might have a sudden breakthrough about it.

Ashley Deeks: My, my project is basically working off the assumption that we're not gonna arrive at General

Ashley Deeks: General AI, or artificial General AI in

Ashley Deeks: the next decade. if ever I think once, if that happens, I think all bets are off, and and

Ashley Deeks: it's really hard to predict what the world looks like.

Ashley Deeks: but so maybe more specifically sort of the associated rise of AI. Generally.

Ashley Deeks: I think 1 one thing I haven't really talked much about, but

Ashley Deeks: will be an issue is

Ashley Deeks: the use of AI by non-state actors.

Ashley Deeks: even in this narrow AI, you can imagine non-state actors

Ashley Deeks: being able to get a hold of

Ashley Deeks: you know advanced sort of autonomous drones, small drones

Ashley Deeks: that are extremely precise

Ashley Deeks: and

Ashley Deeks: able to deploy those i'm thinking like the hutis in yemen, they've been able to use large drones to fly into Saudi and cause an explosion basically on the door. The palace in in the Saudi Government

Ashley Deeks: enhancing those drones and the sophistication thereof with AI

Ashley Deeks: in the hands of non-state actors is pretty pretty scary

Ashley Deeks: as of now. That really really advanced AI is largely in the hands of governments, I think, but

Ashley Deeks: we might expect that that won't last that long. So

Ashley Deeks: I do think as the as it proliferates, including to non

Ashley Deeks: non-responsible states are non-responsible State actors.

Ashley Deeks: It increases the the the global risk.

Keeghan Sweeney: Okay, so Melissa, and apologies in advance. If if I mispronounce this, but Melissa Riley asks, what do you think Congress can do to help improve the legal framework surrounding these types of technologies.

Keeghan Sweeney: So, beyond just trying to prohibit certain actions or imports and exports, is there space for a statutory structure to ensure ethical use of AI? Or does it belong in regulation or other more flexible regulatory spaces?

Ashley Deeks: hey, Melissa, I think.

Ashley Deeks: so. That's an excellent question, and I do think there is

Ashley Deeks: more room for Congress

Ashley Deeks: to weigh in here.

Ashley Deeks: I think in general, one of the challenges that Congress is going to confront is.

Ashley Deeks: the same general challenge that it confronts in national security already is

Ashley Deeks: having to do with the amount of time that staffers can spend getting smart on these particular technologies.

Ashley Deeks: really being able to extract from the executive agencies what exactly is happening and what's right around the corner.

Ashley Deeks: so that's a kind of a challenge coming in. But if there are

Ashley Deeks: if you get to a point where Congress can

Ashley Deeks: has the will and ability to act in this space. I I do think you could imagine a like a framework statute here.

Ashley Deeks: we have a lot of framework statutes in the national security space things like fisa and the covert action statutes. where Congress really

Ashley Deeks: sets out like these are the kinds of systems that we're okay with. Here are the

Ashley Deeks: the levels of human oversight that we might want to insist on. These are the context in which we don't want you to be able to use this. So, for example, the they could legislate to say that the Defense Department should not allow

Ashley Deeks: AI into its command and control systems for nuclear weapons.

Ashley Deeks: So taking certain things off the table, and then you know, kind of building in thoughtful values on the on the side without going too too detailed. Right? The If you get really detailed on a lot of things the statute becomes outdated pretty quickly. so I need to. I i'm gonna

Ashley Deeks: in the book project spend spend a bit of time thinking more coherently about what an actual statutory intervention could look like

Keeghan Sweeney: Hmm.

Keeghan Sweeney: And maybe if I could take students prerogative just to ask a follow up question kind of related to that. But so my understanding is. During the Cold War a lot of the critical technologies were developed largely by government investments in R&D. but in today's world I think private Sector R. And D, especially in artificial intelligence. But a lot of these other kind of core technology areas pretty drastically outpaces Government investment.

Keeghan Sweeney: and also, I think the private sector is a lot more competent and cutting edge on developing a lot of this. So what challenges are generated by the fact that a lot of this stuff is being developed outside of kind of the government space.

Ashley Deeks: And

Ashley Deeks: yeah, so

Ashley Deeks: I think they're right. They're both benefits and and burdens to this fact, right? Our Our tech community is incredibly creative.

Ashley Deeks: It can move fast, it can break things, and it can to develop really neat stuff

Ashley Deeks: in a way that it's hard for the Government to do right because of

Ashley Deeks: hiring restrictions because of acquisition restrictions, the government just moves slower. That's not to say that there aren't really smart.

Ashley Deeks: fabulous computer scientists inside the government. But I think your premise is right. That that a lot of the the kind of

Ashley Deeks: advanced stuff is coming out of the the private sector. So

Ashley Deeks: One thing the Government has tried to do to harness. The power of the private sector is through tools like in hotel, which is basically like a CIA venture capital firm that

Ashley Deeks: can identify things that it wants, and and try to invest in companies that might be able to deliver that. So that's a way in which the government's tried to be a little bit more creative and harnessing the power of Silicon Valley.

Ashley Deeks: One of the challenges you could see

Ashley Deeks: depends where you sit. If you think of this as a challenge or a benefit

Ashley Deeks: is that the companies might resist pursuing

Ashley Deeks: certain technologies or areas to to dive into.

Ashley Deeks: because

Ashley Deeks: they object to how it could be used. so we're already starting to see some companies that are

Ashley Deeks: refusing to sell facial recognition software to certain police departments without

Ashley Deeks: certain commitments about how it'll be used.

Ashley Deeks: A couple of years ago we had Google decide not to try to re up a contract with Dod called Project maven because they were worried that they're

Ashley Deeks: machine learning ish tools. We're gonna be used to engage in targeted killings that it, I guess, concluded as a company where.

Ashley Deeks: inconsistent with international law.

Ashley Deeks: So that is one of the challenges of of relying on companies where they're

Ashley Deeks: their corporate

Ashley Deeks: values. Don't align with the with the government.

Ashley Deeks: but it is I. I know that the the government.

Ashley Deeks: I, from a variety of agencies, are

Ashley Deeks: interested in making sure that there are good open relationships with these companies, not just for acquiring tools, AI type tools, but also in the cyber setting. the the interactions between those companies now become incredibly important, as I think the Ukraine conflict shows.

Keeghan Sweeney: Yeah, it's really interesting. okay. So next question kind of returns to reoccurring and probably predictably. So theme here. China. So Richard Engel asks.

Keeghan Sweeney: You know what legal means are available to punish those States like China that might go beyond.

Keeghan Sweeney: You know some of the limits we as a society, might place having those public law values. Are there any means that

Keeghan Sweeney: the United States and kind of like-minded countries might

Keeghan Sweeney: use to to enforce or get other countries to adopt limits that that might make this technology better for the world.

Ashley Deeks: yeah, thinking about the tools from one powerful state to punish another state is can be a frustrating exercise. obviously this is kind of come up in the in the Russia Ukraine situation.

Ashley Deeks: one tool that the Government has that the Us. Government has used in the cyber setting, where it has suffered cyber attacks from countries that the Us. Thinks transgress

Ashley Deeks: appropriate norms is through criminal indictments.

Ashley Deeks: there' been examples of the Justice Department indicting Chinese officials, Russian officials, Iranian officials for cyber attacks on dams and elections, and so on.

Ashley Deeks: It's not entirely satisfactory, because the chance that you will actually get a person who you've indicted here in the us to to hold them to put them on trial is pretty low.

Ashley Deeks: but it is a signal for sure that this behavior that someone's been indicted for is something that the Us. And and often its allies think is

Ashley Deeks: a problem. Another tool that we and and friends have used in the cyber setting to say, we don't like this is through public attribution, which is basically you trying to rely on a name and shame approach. So

Ashley Deeks: we have done that with, you know, countries ranging from the Netherlands to Japan to the Uk. Where we've come together and said, we are accusing X country of why activity, and it's inappropriate that they did. That

Ashley Deeks: is that really a punishment? Not in the sense that we think about it in the domestic law sense. but that is one means that States are trying to use, I think, to shape

Ashley Deeks: not just the the club. Of what does NATO think, but also what are countries that are really

Ashley Deeks: not within China's

Ashley Deeks: orbit or not within Russia's, but not within ours. Either can we persuade them.

Ashley Deeks: through the strength of our values that that we're actually defining the right kinds of uses of cyber. I think all of those potential tools are relevant to AI as Well,

Ashley Deeks: So

Ashley Deeks: you know, sanctions are also another tool in the book. The only other thing that I've really been able to think of is, if you were to

Ashley Deeks: capture a system

Ashley Deeks: another State's autonomous system.

Ashley Deeks: and you knew that it had been used in an autonomous way that you thought was problematic. You could potentially leak the code.

Ashley Deeks: so we might start to see some things that are more trying to turn the tech back on the user.

Keeghan Sweeney: Mit. Ctl. And so Dennis Kelly asks, and I think you mentioned in your initial remarks, you reference deepfix which you're obviously a big concern. But Are there any plans to use AI on the flip side of that to help diffuse misinformation? 150

Keeghan Sweeney: and disinformation?

Keeghan Sweeney: on the Internet

Ashley Deeks: boy. I hope so. I I I don't really study misinformation, and so I don't think I have a great answer to that.

Ashley Deeks: But if we think about where AI can do best. It's when it has a lot of data.

Ashley Deeks: And

Ashley Deeks: you know, we, if there's one place, it's got a lot of data. It's the Internet. So so maybe some

Ashley Deeks: people on this on the screen could help

Ashley Deeks: think about ways in which AI can be used for that. It may already be in train. I don't know. I don't know for sure. Unfortunately.

Keeghan Sweeney: Okay. So Krista rapport asks: Are you concerned about the hacking of electronic locks, such as those on the launchers that the Us. Sold to Ukraine, those locks supposedly blocked long ranks, launching and missiles into Russia, and just kind of building off that question. Maybe i'll. I'll add general observations about the role. Artificial intelligence is going to play in cyber security

Keeghan Sweeney: writ large, so broad question. Take it, however, you'd like.

Ashley Deeks: Okay,

Ashley Deeks: So your middle question was

Ashley Deeks: role for AI in

Ashley Deeks: Russia. Ukraine.

Ashley Deeks: I don't know the answer to that. I wish I did. I do think it

Ashley Deeks: highlights one

Ashley Deeks: challenge moving forward, which is that we can see weapons, systems.

Ashley Deeks: be used in real life, and we may not always know what mode they're in. We don't know if they're in fully autonomous mode or not.

Ashley Deeks: This is actually a challenge that happened. I think, with a Turkish drone that was used maybe in Syria, where reporters

Ashley Deeks: speculated that it had been in fully autonomous mode, but it was difficult to confirm. So

Ashley Deeks: of the Us. Russia Ukraine I don't know. I wish I did know

Ashley Deeks: Haven't seen reports that there has been a lot of autonomy in those systems.

Ashley Deeks: hacking is, of course, a real concern with AI. It is easy to

Ashley Deeks: to deceive the system. If you don't, I think, created correctly.

Ashley Deeks: they're real dangers that it could be hacked and misused. and some of these systems are frankly, even without the the hacking are kind of brittle, easy to trick, right. You've heard about a system being able to detect a stop sign. But if you put a sticker on part of the stop sign. It starts to think it's a panda right? It really kind of goes sideways.

Ashley Deeks: And so with all of these tech tools, I think the answer is, Yes, we're really always concerned about hacking, and so yes, if we had. As a country, I don't know whether we did this, but if we had

Ashley Deeks: tried to put particular locks on weapons that we were sending to Ukraine. we would, of course, be worried that those could be UN unlocked and used in ways that that we didn't intend

Ashley Deeks: and then, Keegan, your your kind of broader question about the interaction between AI and Cyber

Ashley Deeks: I mean, I think that this, I think cyber is the area where we are going to see the most autonomy fastest.

Ashley Deeks: and I know that in a recent

Ashley Deeks: NATO cyber exercise. The news report suggested that there were some autonomous tools or AI AI based tools that were used in that in that scenario. So it makes me think that that's almost here.

Ashley Deeks: and so

Ashley Deeks: I think that

Ashley Deeks: I think a AI. And cyber is a good place also to kind of, if we could just circle back and think about the Democratic accountability piece of it.

Ashley Deeks: Congress, for example, has a, I think, a a hard time kind of tracking cyber. It has legislated in particular areas to require that the Government

Ashley Deeks: give it 48 h notice within a after a cyber attack has occurred.

Ashley Deeks: If we, if we start talking about autonomous cyber systems and the attacks are are flying fast and furious, and there's a possibility for unintended escalation between 2 different autonomous cyber systems, almost like the reverse of a stock market crash. Then you can imagine how the role for Congress in helping

Ashley Deeks: moderate and be aware of and make smart choices about, the kinds of conflicts that we're getting into overseas is diminished by the the an introduction of AI into these cyber tools.

Keeghan Sweeney: Alright. So we're coming up on one o'clock. So maybe time for just one more question and we'll circle back in and on on potentially, the most important aspect of this question, which is the people who are going to make this happen so, Richard Glenn, and asked, how difficult is it for affected us agencies the Federal Government, with large to find and hire a qualified people who are going to develop the AI in the responsible way that you're describing.

Ashley Deeks: Yeah, it's hard.

Ashley Deeks: I. The Government knows it's hard, though, right, including Dod and and the Intelligence community.

Ashley Deeks: It is. It takes a long time to bring people on to intelligence agencies, including in particular the CIA.

Ashley Deeks: you have to have a pretty clean background.

Ashley Deeks: and there are a lot of people who are really good tech people who might have done some things in the past. That

Ashley Deeks: would be a challenge to get them into the government. so maybe the Government needs to think a little bit about

Ashley Deeks: changing. Its its clearance process.

Ashley Deeks: I do think one advantage that the government has is that there is a real mission here. And

Ashley Deeks: you know, if you want to serve your country

Ashley Deeks: in a way that is very direct and very tangible. then the Government, I think, can offer that in a way that that some of the companies in Silicon Valley can't.

Ashley Deeks: But it is a persistent challenge, and

Ashley Deeks: my only comfort is that the Government is very keenly aware of this, and is, is, I think, trying to think hard about how to make sure that it's it's person power remains strong.

Ashley Deeks: Okay, so thank you all very much for taking the time to to join me in Keegan and the foundation today.

Ashley Deeks: If you have any questions about upcoming programming, please feel free to reach out to the alumni Relations team at alumni relations at law dot Virginia Edu.

Ashley Deeks: So thanks again very much, and I hope everybody has a good day.