Barclay Damon Live Presents *Cyber Sip™*
Season 4, Episode 9: "Who's Leading the AI Race, and Why It Matters," With Adam Segal

Host: Kevin Szczepanski, Barclay Damon, and
Adam Segal, Council on Foreign Relations

[Kevin Szczepanski]: Hey, everyone, Adam Segal is the Ira A. Lipman Chair in Emerging Technologies and National Security and director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations. He is an expert on security issues, as you'll hear—from April 2023 to June 2024, he was a senior advisor at the State Department where he led development of the United States international cyberspace and digital policy. His book from 2016, "The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age," describes the increasingly contentious geopolitics of cyberspace. Dr. Segal's work has appeared in the Financial Times, New York Times, Wall Street Journal, as well as Foreign Policy and Foreign Affairs magazines. And he currently writes for the blog Net Politics, which I just checked out before the podcast, and you should check it out too. Welcome to Cyber Sip, Dr. Segal.

[Adam Segal]: Thanks for having me on, Kevin.

[Kevin]: Before we get started, how did you get started in cyberspace and digital security issues?

[Adam]: So I had written a book before the one you mentioned, before "Hacked World Order," on the technological competition between China and the United States. And that book had a page and a half at the end that said, by the way, if Chinese hackers keep stealing all of our intellectual property and high tech, that's going to be really bad for us. And I finished that book and my boss at the time, Richard Haas, who was president of CFR, and I went to him, and I said, I need a new project. We don't have anyone doing cybersecurity. I should be that guy. So almost 15 years ago, the council did its first report on US foreign policy and cybersecurity. And that's how I entered this, the field.

[Kevin]: And unlike other areas of foreign policy, I imagine, the shelf life for cybersecurity and digital security issues is very short. Things change so rapidly. And I want to take you to one thing that is already evolving. And that is the DeepSeek splash that began in January of this year. So back in January, DeepSeek launches R1, which is its state-of-the-art AI model meant to compete directly with OpenEyes01. I understand that DeepSeek has already launched a newer and better version of R1 last month. What I wanted to ask you though is with the benefit of six months of hindsight, what do you make of the launch of DeepSeek in January? How has that changed the AI and perhaps even the foreign policy landscape?

[Adam]: Yeah, so the launch of DeepSeek, I think, really raised at least three big questions about AI and international relations in particular. The first was, who's winning this race? And until DeepSeek came out, US policymakers and the tech community was pretty confident that the United States was ahead. If you looked at ChatGPT, if you looked at Claude from Anthropic or Lama from Meta, their metrics on accuracy and speed and a bunch of the other things that you measure AI models on were just way ahead of what the ..where Chinese models were. And the Chinese seem to be at least two years behind. And then DeepSeek releases R1, as you said, and everybody's really surprised about how much...how well it performs and how it performs better than some models, US models on some metrics. The second area is around export controls. Because the US

government essentially wants to slow China down on artificial intelligence because of its applications, possible applications for military purposes, as well as for surveillance and repression. And so the Biden administration, well, actually starting in the first Trump administration and then continuing through the Biden administration and now continuing to the second Trump administration, the US has slowly increased the pressure on export controls, in particular around specialized chips, GPUs—general processing units—graphics, excuse me, graphic processing units, and particularly the chips sold by Nvidia. And so DeepSeek's ability to build this model, even under these very tight export controls, really raised the question about, well, what do we think they're doing and are they working? And then third is a question about the type of models we're seeing and the development models that we think are going to push AI forward. And in the United States, the argument has been AI's progress is based on three things, right? Data—huge, huge amounts of data, scraping the internet. Massive amounts of compute. So how many tens of thousands of Nvidia chips do you have? And massive amounts of energy, right? You have to drive all those things together. And DeepSeek seems to run on none of those things. There's a lot of kind of...right now inside the Beltway, debate about how many chips did they use and how much money did they spend. But the fact is they definitely spent a lot less than US companies. They relied on fewer chips and their model is open source. So that means that anyone can get it, access it, and change it... while companies like OpenAI and others are proprietary models.

[Kevin]: I was going to ask you, Dr. Segal, how is it that we were so surprised by this development? Were we not paying attention to the signs or was this utterly a shock to the generative AI platforms?

[Adam]: I think some people who are very deep in the woods and were reading the scientific articles that are being published about breakthroughs in AI were not completely surprised. But I think one of the reasons why we were surprised is that DeepSeek was not a company that people expected to see the breakthrough. When we were talking about the tech giants in China, people talk about Alibaba, they talk about Tencent. They talk about Huawei, the telecom company. And the interesting thing about DeepSeek is that it actually is a spinoff of a hedge fund. It's a quantitative hedge fund. The CEO of that hedge fund, Liang Wenfeng, really kind of as a side project said, well, I'm interested in AI and I'm going to create this organization and I'm going to basically fund them to do what they want and experiment and break through. So I think that's why it was off the radar of a lot of people...

[Kevin]: Dr. Segal, I was mildly surprised that the R1 model was open source, but I'm not sure if I should have been surprised. Were you surprised? And if not, what is it about the Chinese, either DeepSeek itself or the Chinese system that led DeepSeek to make that an open-source model?

[Adam]: Yeah, I wasn't that surprised. I think there are two reasons why I wasn't surprised. The first is, in a lot of technologies, the Chinese are looking at open source, in particular to get around some of the export controls we were talking about earlier. Because when they're not proprietary, when they're widely used, then the Chinese think, well, it's... be much harder for the United States to control and be able to use export policy to slow Chinese growth. And we see that open source being used around operating systems for computers and cell phones. We see it around chip design. So I'm not surprised we see it for artificial intelligence as well. The second reason is that the debate in China around AI is slightly different than it is in the US. In the US and in Western Europe, in the EU, there's been a lot of focus on safety, right? And in particular on existential risk, right? Are we creating the Terminator or Skynet that's going to create a computer system that's going to come and eventually kill us or no longer need us? The Chinese are really not very focused on that—the threat of artificial AGI, artificial general intelligence. They're much more focused on... what's the impact going to be on the economy? And in particular, how do we diffuse it as quickly as possible to as many different sectors of the economy? And open source will do that much faster, right? If you're not worried about licensing, if you're not worried about paying for the use of it, then that's, I think, the other reason why they've been really focused on open source.

[Kevin]: So I know it's difficult to predict because we're only a few months into the new administration here. But what does that say, Dr. Segal, about our assumptions about the US and Chinese approach to approaches to AI? It sounds like there may be some common ground between the current administration, which seems to be concerned about over-regulation. Arguably of the sort we see in EU though I'm not questioning the need for some regulation. There seems to be some common ground between the US and Chinese approaches now. Do you see that and how do you see that playing out?

[Adam]: Yeah, so the Trump administration came in essentially arguing, as you said, that there was too much regulation and that there was too much fear about the security and safety of the systems. And one of the first things the president did was overturn the Biden executive order on AI saying that it was slowing innovation. The second thing that the administration has done—and we saw this on the president's trip to the Middle East was make these huge deals with Saudi Arabia and the United Arab Emirates, the UAE, for them to be able to gain access to chips. So the US could diffuse its technologies. The Biden administration, right before it left office, created some controls on chips again. It was called the AI Diffusion Controls. And it essentially divided the world into three tiers. Tier one were our friends, countries that were going to get everything for the most part. Tier three were enemies or potential enemies, China, Russia, North Korea, Iran, that would never get hopefully any chips. And then tier two was the rest of the world. Now, tier two was a very confusing space because lots of close friends of the US were in that space, the Poles, the Israelis, Indians. So they were all pretty unhappy with it. And so the Trump administration also overturned that executive order. And we saw the kind of outcome of that in the trip, the president's trip to the Middle East. And so the, the White House has really been promoting what was accomplished there by saying, yes, we're focused on diffusing. And in particular, we want other countries to use American technology. We don't want them to rely on Chinese technology, and so this is a good way to do that, to beat the Chinese into that space. There's still a lot of differences. China is much more actually heavily regulatory on AI than in the United States. Part of that has to do about the Communist Party and political controls, right? So anyone who creates a generative AI has to make sure that it upholds socialist culture and socialist values. So I don't know if anyone listening to the podcast has ever played around with DeepSeek, but if you ask it about...for example, the Tiananmen protest in 1989, it'll refuse to answer. It'll say that that's too politically sensitive, I can't answer that question. If you ask it about Tibet, it'll say Tibetans are all very happy and China is really engaged in developing it. So we see these controls around those spaces. I think the big issue is are we going to find any places to have convergence around common interest internationally, right? Can we talk about international controls on the AI? And that is going to be very hard. We've had one very narrow agreement that happened under the Biden administration around applying AI to nuclear command and control, right? So you don't want these systems making decisions about launching nuclear weapons. But other than that, it's been very hard to find any common ground.

[Kevin]: So it makes me think of something we were talking about earlier in the context of DeepSeek, the notion that one of the things it told us or may have told many looking from a very high level is that the folks—the nations that lead the generative AI race today—may not be leading it tomorrow. My question for you, Dr. Segal, is what does it mean to lead the AI race? I think we all assume we know what that means, but what does it really mean, particularly in the context of foreign policy?

[Adam]: I don't we really do know what it means. I think for a long point in time, there was a lot of focus on the metrics, right? Which models do the best? And that was the lead. Then we saw this shift, especially in the foreign policy and in the policy-making world about, well, that matters, but diffusion matters even more, right? It matters how you use the technology, and how many companies are using it, which sectors you use it in. It's like electricity, right? It's not a question about who got to electricity first. It's who used it for industrial purposes more dramatically. My sense is that the lead on the metrics is going to go back and forth and back and forth. The people who think there's a race seem to think that there's a moment where one side wins and locks out the other side from all the benefits.

[Kevin]: Mm-hmm. Right.

[Adam]: I have a nuclear weapon. You don't have a nuclear weapon. But I don't think that's how it's going to be with AI. And I think we're going to have to learn to live with lots of different competing models. And then the arguments are going to be about: why would you use a US model versus Chinese model?

[Kevin]: Mm-hmm. No, that makes sense. And so what are there... or is it too early to tell, what are the foreign policy implications of all this? We're dealing with innovation with obvious economic implications. And that's probably what everyone's thinking about. That's what I'm thinking about anyway these days. But are there foreign policy implications? Does the growth of generative AI have the potential to exacerbate tensions between the United States, China or China and the West or are there other implications that most people aren't thinking of?

[Adam]: There going to be lots of foreign policy implications. We talked about some around just how do you shape the race for AIs. We talked about export controls, but trade policy is going to have an effect on it, immigration policy, because many of the experts in AI are actually Chinese and they used to come to the States. They used to train in the States. They used to start companies in the States. So immigration policy, visa policy all has an impact on that. We're clearly seeing it around the questions about influence and disinformation operations, right? So Chinese operators on TikTok or Facebook or X are using generative AI to engage with Americans and other people internationally to try to make their propaganda sound better and be more engaging. So we're definitely seeing it there. It's being applied in weapons systems. So it's definitely going to have a military... impact on the military balance, right? With the Ukrainian operations two weeks ago, not a huge amount of artificial intelligence was being applied in the drones, but a little bit, right? When they get close to the target, they were trained to identify certain types of Russian bombers. And so at the end, especially because as drones become more susceptible to lots of electronic countermeasures, and they might be cut off from the operator, artificial intelligence helps them in the last kind of set before they hit the target. So we're seeing that application now as well and then as just broadly whose economy is going to do best. So it has just a range of really big impacts on US foreign policy.

[Kevin]: You mentioned Russia-Ukraine conflict. Before we pivot, I wanted to ask you about the Israeli-Iran conflict. Is it too early to tell, or are you able to see any AI implications, any technologies employing AI in that conflict so far?

[Adam]: I don't think we've seen any reporting about it. Again, in the first day of the attacks, the Israelis launched some drones from inside Iran. And I don't know if the targeting at the final stages was done by an operator or if they used some target identifications software or not. I mean, certainly we know there's a huge cyber component to Israel-Iran competition. The two sides have hacked each other multiple times, gotten into each other's critical infrastructure. We know that Israel leads the world with cybersecurity technology. So I suspect on the defense side and probably on the offense side, we're seeing AI there as well.

[Kevin]: Yeah, something that I'm sure you and others will be following. I do want to pivot back to something you touched on earlier, and this may be too high level to be useful, but in my reading before I knew we would be talking today, I got the impression that the perspective of the US when it comes to AI is on innovation. The perspective of the EU, and this may be a gross oversimplification, may be more on regulation, based on concerns about safety. And from what you suggested earlier, it sounds like the Chinese are a hybrid of those two. Innovation, but also wrought of a fairly thick regulatory framework. Are those assumptions true? And—putting you on the spot a little bit here—what does that imply about the long-term trend for AI development and leadership in the world?

[Adam]: Yeah, I mean, that is definitely the kind of shorthand for the systems, right, is that the US hands off bottom-up innovation driven by the private sector with support from universities. China is kind of a mix controlling, but also has a very vibrant tech environment, or at least it did until the backlash against technology inside of China. But, you know, it has lots of state support and very focused on the state's desires and needs. And Europe regulates, right? It has the... first it had the GDPR, the general directive on privacy

regulation. Now it has the digital services act and the digital markets act, which regulate and the AI act. And so the argument has always been, well, Europe doesn't really have the innovative environment. And so its impact is through regulation. And this is a Columbia professor up the street from me... Anu Bradford, called the Brussels effect, right? The EU gets its international influence through regulation. So I think what we're seeing now is some kind of, the Europeans are questioning that. I mean, there's still a strong desire to regulate and that's not going to change, right? We have to remember that the desire for regulation around privacy and other things didn't come out of the desire to kneecap American firms, right? It came out of World War II and a reaction to Nazism, right? And fascism and the desire to protect people's privacy, right? How do you protect people's privacy? And that's not going to change. Europeans just have a very different perspective on who they're willing to give their data to. But there is definitely some questioning that's been going on. There was a very influential report written about three or four months ago by a former prime minister of Italy, the Draghi Report, that basically said, look, we can't regulate our way out of this problem. We need to really start supporting small firms and innovation. And the Europeans have slowed the implementation of the EU AI Act because of the impact on some small firms there. And so they're beginning to think about how they can kind of find a more golden mean between regulating and innovating...

[Kevin]: Mm-hmm. The "Goldilocks zone." But that leads me to a question for you. There's an emphasis on regulating businesses and individuals—the developers and the operators of AI—but I wonder whether we may be too late. We're focused on regulating the individuals and the operators, but we're not as focused on regulating the AI. So with all this talk of agentic AI, which for our viewers and listeners is a much more autonomous AI than a simple generative AI product like ChatGPT or DeepSeek. Are we going to reach a point where the regulation is too late because the technology has outstripped the ability to regulate the conduct and the use of that technology?

[Adam]: I mean, we certainly look to be on that trajectory, right? I mean, that's kind of what happened with internet technologies and social media. They all raced out the door and that was in part because both because of the US's willingness to basically say, all right, we want these sectors to grow and also the mindset of Silicon Valley, "move fast and break things" and we'll deal with those problems later. And I think people are afraid we're going to recreate that model with some strong negative effects with AI. There have been attempts and there are growing attempts at the state level to regulate AI. California had tried to pass a bill over the last summer, and I think Connecticut and Virginia and a couple of other places have started. I think, you know, the "one big, beautiful bill," one of the things that is in contained in that bill basically is a 10-year moratorium on state regulation of AI, which doesn't make a lot of sense to me. It also seems to go against what the federal, our federal system is designed to do. But I can understand why the AI companies don't want to have to deal with 50 different types of regulation. So I suspect we'll, I was on a panel this weekend and somebody basically asked, are we going to get there in time? Because you could regulate a lot of these things with existing regulations, right? You could figure out, as you said, liabilities, but we just haven't made any decisions yet. And the question was, are we going to get there in time, or is it going to take something terrible to happen? And then we'll rush. And unfortunately, I'm afraid probably something bad is going to happen, and then we'll rush legislation up.

[Kevin]: Yeah, I get concerned about that too. I think DeepSeek is a kind of metaphor for that. When it comes to emerging technologies, there's a zero-day effect. We often don't know about the problem until it rears its ugly head. And by then, it may be too late. So it'll be interesting to see. And that leads me to, we're almost out of time, but it leads me to this. And I know your area of expertise is broad, but I'm going to draw it over to the business side. So, for those of our listeners and viewers that are sitting here as businesses, particularly small and medium-sized businesses, Dr. Segal, and they're thinking, well, this is all very interesting. What does this mean for me? What should I be thinking about? What should I be doing in response to all of this frenetic AI development? Are there guidelines that small and medium-sized businesses should follow?

[Adam]: Well, I think that the guidelines are being developed. There's two issues for small and medium-sized businesses that are coming up. One is, at the same panel I was on, there was a kind of very unscientific survey of people. Do they have any idea of the liabilities involved in deploying the AI systems that they're using right now? And nobody did. So I would suspect that that's real high priority is that if you are starting to use AI in your businesses, which most of us are in some cases kind of even unconsciously is to kind of like we did with cybersecurity in the first kind of after the first wave, we're like, let's do a kind of figuring out what we're using, where we're using it, what's important, what will you do if things systems went down? Do we have backups? All the things we did in a cybersecurity audit, let's similar do, I would imagine do something similar with AI, right? Where have we applied the system? What is it? What do we think the system is doing? What are the bad outcomes that we're concerned about? The second is probably, you know, in the next five, 10 years, if that long, you're going to have to choose if you're going to use a system from China or India or some, or Europe or some other place, right? It's not just going to be a US system. And we, you know, we've seen that a little bit, right? We had a debate about TikTok, which is, you know, and maybe some of the people listening to the podcast, do business in China and they use WeChat. So they have to be worried about some cybersecurity concerns. But a lot of people are using DeepSeek, right? And are they downloading it to their work computers or are they running it in a sandbox or some other safer environment? So I would be... start thinking about that. What do we think about using these systems? Do we know where the data is going? Do we know what's being trained? Those types of questions.

[Kevin]: Yeah, I agree. I think I see both sides. Up until about six months ago, my instinct was caution and security. And I think that's an important instinct. But I was having a conversation with one of my colleagues, it was at a weekend conference, and he said to me, you know, if we in the legal industry don't figure out how to incorporate AI into what we do best and become more efficient, we're going to die. And it hit me because I think there's a lot of merit to that. Whether, whether we personally like it or not, or you like it as a, as a business or in a sector, if everyone else is doing it, it's counterintuitive not to do it. And so I think we're going to be seeing it more and more. I, I encourage everyone to develop a use case for AI. It's good to experiment with it initially, but eventually you have to figure out what is it that I'm going to use this platform for to make my business more efficient? And I wonder, this is a sort of broad question, maybe we can close with this. You look at these issues on a micro and a macro level, Dr. Segal, do you ever feel as though there is a kind of rush to embrace new technology, damn the consequences, without a really careful assessment of the implications? And does that concern you at all?

[Adam]: Totally. You know, I think again, looking at the whole social media experience—and my children are now in their 20s. So they've kind of, I'm not as concerned about their impact on their well-being, but certainly when they were younger, you know, was like we've lost control, you know, even as somebody who did cyber and digital. I had very little, when I realized that both of my children had figured out workarounds for the controls I had put on their phones, even though eventually I discovered them, but they had a month there where they had a workaround. So with AI, I think the impact is going to be even larger in many ways on what the jobs of the future are, how we make decisions, impact on people's health is just huge. Unfortunately, the debate in the US is very much shaped by the, you know, we have to get to this super intelligence as fast as possible because if we don't get there, the Chinese will and then who knows what will happen. And in that environment, people are more willing to say, all right, well, let's rush the product out and regulation is not great for us. And I don't think that's the right framing. We definitely need to be mindful of what China is doing. We need to race as quickly as possible, but we also need to think about what the impact is going to be.

[Kevin]: That is a sobering and insightful thought, and I think that's the perfect place to leave it. Dr. Segal, thank you so much for joining us on Cyber Sip. This was a terrific conversation. I wish it could be longer, but I encourage those of our listeners and viewers, if you haven't had a chance to hear from Dr. Segal or read him before, go on Audible. If you're on, you can pick up "The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age." That is a great baseline book. I have purchased it myself and started to listen. Of course, I'm listening, so I find that I have to listen twice as opposed to reading. I think it's a more active process. You are contributing very impressively and invaluably to this space, and I appreciate it.

[Adam]: Thanks so much for the kind words and thanks for having me on.

[Kevin]: And thank you. Thanks to all of you for joining us on Cyber Sip. We're back soon with another episode.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, and Spotify. Like, follow, share, and continue to listen.