**JASON MATHENY, NSCAI Q2 RECOMMENDATIONS**

**Jason:** My name is Jason Matheny. I'm a commissioner on the National Security Commission on AI. And I also work at the Center for Security and Emerging Technology at Georgetown

**Craig:** And Center for Security, that's CSET. Is that right?

**Jason:** CSET. That's right, Craig.

**Craig:** Yeah. And does CSET overlap with your work with the Commission?

**Jason:** Yeah, we do a lot of related work. CSET looks at global trends and emerging technologies. We look at the level of capability that exists in the public and private sector. We look at investment patterns, publications, patents, texts in foreign languages to try to understand how different countries are making progress in key technologies. And then we also look at the way that US policy can help to sustain leadership in different technologies, whether it's in workforce policies or technology standards or alliances with our other democratic allies.

**Craig:** Yeah. And this quarter's recommendations, these have gone a little bit deeper. Can you talk about your line of effort's recommendations?

**Jason:** Yeah, the Commission's interim report highlighted export controls and investment screening as key to protecting America's edge in security related technologies. And both export control and investment screening are much more complicated to implement for "dual use" items, that is technologies that have applications that are purely commercial but also have applications that may be in the military domain.

It's a difficult balance for the government to make. You need the policies to both prevent critical technologies from falling into the wrong hands, but not cause such harm to US industry so as to undercut US competitiveness. This requires technical expertise as well as strong regulatory bodies to effectively target the policies to specific technologies and organizations.

**Craig:** The recommendations say that the government lacks sufficient technical capability to identify new policies, and the analytical capability to enforce those policies, especially on dual use goods. And I spoke to Mignon Clyburn about the efforts to increase the digital workforce in the government, but on export controls and that sort of thing, you really need a very high level of technical expertise.

Can you talk a little bit about why there is not that technical expertise, particularly for these technologies? And how you can go about getting that technical expertise?

**Jason:** It's hard for government in general to draw in quickly the expertise that predominantly exists in the private sector either in academia or in industry. And you know, it just takes a long time to bring that kind of talent into the government. There are high opportunity costs for the people who have the technical expertise. They can be making a lot of money in the private sector. So, typically the best approach is not to require that the US government hire a ton of experts directly into the government. But that we develop mechanisms that allow the government to access technical expertise where it already exists and be able to get their advice in a way that's more agile.

One thing that we highlight in our report, is the need to be able to access talent that exists in the federally funded research and development centers, and the university affiliated research centers. So, organizations like the National Lab, or the applied physics laboratory at Johns Hopkins, or MIT's Lincoln laboratory. Those are really extraordinary concentrations of technical talent that the US government has access to, and we should be leveraging that talent and getting their advice on topics like export controls and investment screening.

**Craig:** Yeah. And we'll talk about how you draw on some of that talent in a minute, but one thing that interested me, as you say very clearly, that recommendations are weighted toward executive orders: is part of the problem that there doesn't exist sufficient technical expertise among the congressional staff to move quickly on these recommendations?

**Jason:** Congress has access to expertise that exists within the Congressional Research Service and the GAO. So, I wouldn't say that they don't have access to technical expertise. I think, with a lot of these controls, when you get down into the details, that's where you need technical experts to weigh in. And in the executive branch some of this is addressed by having external advisory committees. So, for example, I serve on one of the advisory committees for the Department of Commerce related to export controls on emerging technology.

And it's a group of experts who have a broad range of backgrounds, including AI, but also biotech, and semiconductors, and advanced manufacturing. And we're asked for our opinions about pending controls. I think that's the right sort of approach, but given the pace of technological change, you want to make sure that each of the parts of government that needs to make high consequence decisions about technology has access to expertise that exists in the private sector. Which is really why we recommended a stronger, more agile connection to the FFRDCs and UARCs.

**Craig:** You recommend executive orders to implement certain recommendations, rather than legislative language for the National Defense Authorization Act, for example. Is that simply because it's faster to work through executive orders and the legislation will catch up?

**Jason:** No, I think really, it's because many of the changes that are needed on expert controls are not changes that require legislation, but are instead changes in regulation, which fall within the executive branch.

Congress has already taken the important steps of passing the Export Control Reform Act, or ECRA as it's called, in 2018, and the Foreign Investment Risk Review Modernization Act, or FIRRMA, in 2018. But the implementation of both of those laws remains unfinished, and that really is the responsibility of the executive branch. I think the most important next step is identifying those emerging and foundational technologies to be controlled as required by ECRA. Our report calls on Commerce to complete that list and provide some timelines through the executive order.

**Craig:** The reason I ask that question is, you note that the Commerce Department has yet to identify any emerging or foundational technologies mandated by ECRA, by the Export Control Reform Act. And Commerce is a part of the executive branch, it's part of the cabinet. So, I was wondering whether there is concern about attention being paid to this through the executive, or the speed at which it's being addressed through the executive. Is there any reason why Commerce has been slow on that? Is that a question of having adequate access to technical expertise?

**Jason:** I think it's two things. First, it's a really hard problem, because you don't want to just be piling on, you know, hundreds of additional technologies that are now export controlled. I mean, the overhead, the cost that's imposed by having export-controlled technologies, is really high and there's a lot of collateral damage that's caused by export controls. So, you want to be really choosy, both in the technology that you're controlling, and in the organizations that you want to prevent from having access to that technology. And doing both of those well requires expertise. And, you know, you need more than just the expertise of an advisory committee. You really need a lot of full-time support to be helping.

The export control office within Commerce is itself already pretty small, and it, despite heroic efforts there to try to cover as many technologies as they do, they're not going to have an expert on every one of these specific technologies. So, that's why we really emphasize the need to draw on outside expertise in the private sector in places like the national labs, other FFRDCs, and UARCs.

The second thing I would say about this is, in general, we will be able to do a better job with export controls if we don't have lots and lots of technologies that we're controlling. And current export control lists are thousands and thousands of items. I liked the Bob Gates mind, that when it comes to deciding what to protect, we should have a small yard with a tall fence. That is, we should be prioritizing the things that we absolutely need to protect and investing a lot in protecting those things, rather than writing up what ends up being a relatively small amount of effort per technology to protect thousands and thousands of technologies, many of which really aren't that vital.

So, I think we need to be a little more conscientious in adding things to lists, a little more strategic in what we decide to add to lists, and think especially about technologies that are strategic choke points in our competition globally. That is, technologies where the United States and its allies have an asymmetric advantage in controlling a certain part of the supply chain that's really key to a technology that matters. That's one of the reasons why we highlighted semiconductor manufacturing equipment in our report, cause it turns out that it's a choke point in the entire semiconductor supply chain that the United States and two of its allies control more than 95% of.

**Craig:** Before we go much further, for the benefit of the listeners, we already mentioned ECRA, the Export Control Reform Act. Can you lay out the general structure of export controls for sensitive technology, since it's not something that everyone's familiar with?

**Jason:** Yeah. So, as background, there are two key technology protection tools that we addressed in our report, which are export controls and investment screening. And together those two sets of tools help prevent the transfer of strategically important technology or know-how to competitors. The export controls are governed by the Department of Commerce and the Department of State in consultation with other agencies. And these agencies have the authority to designate certain technologies as being critical to US national security, and then placing those technologies on lists that govern their exports. And most commonly, the Commerce control list for dual use goods is the most commonly, at least within the context that we discussed in our report. Companies who want to export a technology on this list have to first apply for a license to do so with the Department of Commerce.

So, that's export control. Investment screening is an entirely different process. It's governed by the Committee of Foreign Investment in the United States, or CFIUS as it's called, which is an interagency committee that's run by the Department of Treasury. CFIUS has the authority to review and to block, or even unwind, transactions or investments inside the United States that involve foreign investors. To determine whether an investment is going to harm US national security, or could threaten it in the future. And for many years, CFIUS filings were voluntary. A company itself would decide whether this was something that the government should be screening.

In 2018, this law made it mandatory to file with CFIUS transactions that involve export-controlled technology. So, that substantially expanded the oversight of CFIUS on investments in technology. And this is really only practical if, while you expand CFIUS, you also contract export controls. Because there simply is not enough human eyeballs, within or outside of government, to both review every transaction for every expert-controlled technology. It's just impractical. So, we, again, have to prioritize, and that's something we really highlight in our report.

**Craig:** Yeah. Yeah. Well, thanks for that. That's very helpful. We talked about the need for subject matter experts. That takes a lot of time away from academics or people at the national labs. Would there be specific funding for that, or are you relying on the goodwill of these institutions to participate?

**Jason:** Well, these institutions have lots of goodwill, but they do need to be paid for doing this type of work. Now, Treasury itself received additional resources for some of the work through CFIUS, and the Department of Commerce, through BIS, has some resources, but they are unlikely to be enough to cover what both agencies have been asked to cover through ECRA and FIRRMA. So, it's very likely that it is going to require additional funding to do the kind of work that we think is necessary.

**Craig:** There's a danger, which you acknowledge, of pushing AI related research and development overseas. The controls are too strict or too blunt. How do you strike that balance between protection of free flow of ideas and ensuring that critical ideas don't flow abroad?

**Jason:** I think this is one of the most difficult balancing acts. And I think in general, we should be erring on the side of openness, in part, because that plays to our strengths. Our own innovation system has thrived because of its openness. Arguably one of our greatest strategic advantages is our ability to bring in foreign talents to the United States, have them work on projects in US universities, and then most of them want to stay here and contribute to our economy.

So, being overly aggressive in export controls really weakens one of our main strategic advantages. We do point out in our interim report that there are choke points that make a lot of sense to focus on, and then we ended up emphasizing those in our last report. Those are choke points that really wouldn't weaken our ability to draw in foreign talent. These are relatively small percentages of the total level of effort that's applied to, for example, AI. It just turns out that it's a critical resource that everything else depends on. And that, in particular, is semiconductor manufacturing equipment, and even more specifically, the photo lithography tools that are used in semiconductor manufacturing. You can't make progress at the leading edge unless you have access to the most advanced micro electronics. And producing those microelectronics requires advanced photo lithography tools that, fortunately, the United States, Japan, and the Netherlands' semiconductor industry has a decisive lead on.

**Craig:** Yeah. On that ultraviolet lithography tools. It made me think of Pakistan when it was building its nuclear weapons capability, and very famously managed to get not only blueprints, but equipment from manufacturers in the Netherlands. Is there a concern that there'll be leakage from Japan and the Netherlands on this equipment? Because there are many ways to move it to China, it doesn't have to be direct.

**Jason:** I think these are tools that would be very difficult to get diverted covertly. For one, the tools are enormous. A single EUV machine weighs 180 tons, size of a double decker bus. But even more significantly, the throughput of producing these machines takes many months and there's a backlog of orders for these machines. So, it would be very hard to keep secret the production of such a machine that would then be diverted to another country.

There's really only one company in the world that produces this leading edge extreme ultraviolet lithography equipment, and it's incredibly complex machinery. It includes components from the United States that we also track very carefully, and I think it's going to be difficult for other countries to replicate, or to acquire surreptitiously.

**Craig:** Yeah. Although, in the Pakistani example, the centrifuges and different hardware necessary for enriching uranium were not easily obtained, but A. Q. Khan, I don't know if you remember the story, but he managed to get a lot of the know-how, and then the Pakistanis were able to build that equipment domestically. And, certainly, the Chinese are well known for being able to build equipment once they have the necessary know-how. So, it's really that that I was referring to. Not so much turn key equipment.

**Jason:** Yeah. I think there is a dis-analogy in that, you know, the centrifuges are really sort of 1940s era technology. And while it was challenging for people to hit upon the right solution independently, and there's many instances of tracing back to Khan's network for the centrifuge know-how, it's pretty different compared to what really is 21st century technology that involves a complicated set of components that have very narrow supply chains. The know-how is highly distributed among hundreds of people who are involved in developing individual components. So, I think it is fundamentally different than the example of centrifuges.

**Craig:** China has tremendous economic influence right now, as we all know. Is there concern that the Dutch or the Japanese would not play a long on these export controls if China brings enough pressure to bear?

**Jason:** I think multi-lateral export controls are always easier said than done, and economic incentives can help address some of the financial concerns of allies when they're going to lose money on exports. There's a couple of things that help here. One is that ASML is already oversubscribed. That is, when they decided not to send a machine to China, they could simply move to the next customer down the list. And there are lots and lots of customers on the waiting list. So, it is unlikely that it actually means a loss of net revenue for the Netherlands.

But allies do need to have a shared understanding of the risks of a specific technology going to a specific actor. I think the good news is that our allies today generally see the risks posed, for example, by China's attempts to become self-sufficient in leading edge microelectronics, so I'm relatively optimistic that we'll be able to sustain agreements among Japan, Netherlands, and US semiconductor industries. But this shouldn't be our only strategy, and it's very likely that in the next several years we'll see alternative approaches to advanced semiconductor manufacturing, some of which may not require extreme ultraviolet. And we may also see advances in micro-electronics that don't require semiconductors. So, we really need to do as much on the promote-side of technology development as we do on the protect-side, to control that technology development. That is, we need to be investing in research and development, in commercialization so that US companies and the companies of allies remain at the leading edge.

**Craig:** You talk about the AI stack, hardware algorithms and data, and that they should be treated separately. You mentioned that some algorithms are controlled. Can you give me an example? And realistically, how do you control their transfer when that can be done, you know, with a click of a button and an encrypted file?

**Jason:** So, many algorithms are open source, which makes them impossible to control. Commerce has imposed restrictions on specific algorithms, a recent licensing restriction on geospatial imagery software that uses deep neural networks. And this type of algorithm has important national security implications for military targeting. I personally am skeptical that that control is going to do much in the case of China, which already has a pretty sophisticated research infrastructure for training computer vision models. But, I think the Department of Commerce was trying to identify what are fairly specific algorithms that might make sense for controls. I think there was generally a sigh of relief that the controls were not broader. The vast majority of AI algorithms are dual use, so their availability to the general public makes it extremely difficult to control. And, you know, realistically, even proprietary code could still be transmitted illegally. So, I'm not very optimistic about controls that are placed on algorithms.

**Craig:** Yeah. And the example you mentioned, what was that algorithm?

**Jason:** These were deep neural networks for geospatial imagery software. And these controls are on the entire class of geospatial imagery software.

**Craig:** I see. Yeah. Well, that's interesting. So, in the flow of business, you're depending on private companies. Is there a way to ensure that they're not transferring something that falls under a control? Because it's not like shipping stuff through customs where anyone sees it. How do you track what algorithms are being sent over the internet to another country?

**Jason:** You don't. The enforcement mechanism for this really relies that, you know, one party or another, or somebody along the line is going to report that there's been a violation of an export control.

Now, the violation could involve large fines or even jail time, so I don't think that companies or universities will be casual about export controls. But at the same time, there are lots of export controls, it becomes quite confusing as to which ones might apply to a particular piece of technology. And I think that that is an argument for being especially frugal in the way that we use export controls. Having worked on the university side, when a university office is trying to determine whether a technology that they're developing in a laboratory in the university is export controlled, whether it represents fundamental research, whether they can have foreign nationals work on that technology, which in many fields is the bulk of students within the lab, all of that is incredibly difficult, and putting the burden on universities or small businesses to comply with thousands of export control requirements, just creates huge overhead and a pretty significant likelihood of making mistakes unintentionally. So, it's one of the reasons that we in our report suggest that we not place a large number of items on export control lists. And we have said, "Be very targeted."

**Craig:** And to add to the complexity, you have Google and Microsoft, with some substantial research operations in China. You have Baidu and Tencent with substantial research operations in the US. A lot of it's simply to provide convenience to the researchers, there are researchers that have families in China that want to stay there. There are those that have families in California that want to stay there.

But there's, daily, an exchange of algorithms between the research offices in California and the research offices in Beijing. How do you capture that? Or do you just accept that that's within a multinational corporation and they have the right to transfer information across borders within their corporation?

**Jason:** So, this is another reason why we recommend in general against applying expert controls to algorithms. Because, as you rightly point out, the development of those algorithms is an international enterprise, even within single companies. Now, fortunately, to my knowledge, there is only one export control that applies to AI algorithms. But I think there has been some temptation to explore, you know, what more expansive controls on algorithms would look like. In general, we think that's the wrong place to focus. We think we should be focused more on some of the key pieces of hardware and the semiconductor supply chain, and in some cases, datasets that have particular, easily significant military value.

**Craig:** So, the one algorithmic export control that you're aware of is this geospatial satellite class of neural networks, that analyzed geospatial satellite imagery, is that right?

**Jason:** That's correct.

**Craig:** But you talk also about prohibiting the export of facial recognition surveillance technology. And there, I mean, isn't it essentially algorithms that you're talking about? Because the hardware is off the shelf, really. And the data is in the population that you're surveilling.

**Jason:** Yeah, the commission doesn't make any specific recommendations about export controlling facial recognition technology. That's certainly the type of thing that could be considered in applying end-use or end-user controls. That is, one might try to prevent a specific end-use of an algorithm that has been trained on a large database of faces that we think would represent a special risk. But I agree that it probably doesn't make sense to try to place a control on facial recognition algorithms generally. I think that that's too broad and I think it's very unlikely to be effective.

**Craig:** I see, yeah. And then on data sets, can you give an example of a data set that is controlled? And how would you evaluate whether a data set that's not currently controlled should be?

**Jason:** Yeah. So, there's certain technical data that's controlled by the International Traffic and Arms Regulations, or ITAR. And ITAR-controlled datasets are controlled because of their relevance to manipulate, needing inputs to defense platforms.

So right now, there are datasets that are ITR controlled because they're relevant for ballistic tracking for missile defense and other applications that are relevant to the design or maintenance of weapon systems. Separately, there's categories of data sets that might warrant controls if it includes personally identifiable information of national security personnel, genetic information, or other sensitive details about US persons. What we think is that, broadly, if the bulk transfer of data out of the US poses a national security threat, that that data set should be worthy of consideration. It's really difficult to categorize in advance which data sets one needs to be especially worried about.

**Craig:** There's a reference to protecting AI enabling data, in other words, weights in neural networks, and AI enriched data as potential future targets of export control. It's hard enough to regulate algorithms, but when you get into regulating the weights in neural networks, I just can't imagine having a system that could, or a cohort that's qualified to even know what is in a file of weights. You know what I mean?

**Jason:** I think in general, most of these controls don't really have a foolproof enforcement or verification scheme, right? Like, having somebody look at a file that's actually full of, geospatial data, you wouldn't necessarily know that. Right? I mean, fundamentally it's just a bunch of ones and zeros. The same thing for model weights. You could have, you know, a 1 billion parameter model that's been trained on some data set and seeing 1 billion weights in a file, it's going to be hard for somebody to interpret that for the purpose of enforcement.

The reason why we really highlight semiconductor manufacturing equipment is it is in such a separate category from data or weights. The controls that one would apply to algorithms, or the weights that come from training, those controls are going to be very difficult to know when to apply, how to apply them, how to enforce them once they've been applied. I mean, just for completeness, to explain why it is that you might think about these models' weights as being controlled, the idea is that in many cases, the key enabler for an AI model isn't the full dataset. But rather, the model weights that are the output of a network that's taken a lot of effort to train on a dataset. Possibly a lot of compute. And so, the logic is, maybe you don't need to protect the data set as much as you need to protect the trained model or the model weights that are part of the trained model. There is a logic to that. But again, I think the difficulty of enforcing these kinds of export controls is immense.

**Craig:** I had a question in here, I don't know if I'll keep it in, but it just occurred to me in reading the recommendations that you require all transnational sharing of data to be done through federated learning, so the data never leaves the US. Or it never leaves to its home country. But, the models are sent out trained and the weights are sent back, update the model, you know, that sort of thing. I don't know if that's relevant at all.

**Jason:** It is. And I mean, thank you for bringing up the topic. I mean, I think federated learning, which is one class of approaches to dealing with this issue of how to train models on data sets that you might not want to centralize, it's a really exciting area for research and development and there's lots of interesting opportunities to apply it right now in some cases of AI. Right now, the computational cost of using federated learning rather than learning on centralized data, it's about a tenfold penalty that you pay. So, you'd want to use that in cases where you really don't want to centralize data for some reason. And, you'd still want to be able to control how the data are exported by you and your allies. But I do think that investments in federated learning, other sort of approaches to privacy, preserving computing, partially homomorphic encryption, the crypto networks that Microsoft has done. Those are really exciting areas for investment and they would solve a range of problems related to privacy and security that are important.

**Craig:** Just on foreign investment into the US companies that produce sensitive technology: how do you ensure that you're distinguishing between investments from friendly foreign countries, and countries of special concern? There's already a problem of China hiding behind front companies in friendly countries in order to make investments in the US. It's not always easy to untangle who the ultimate benefactor of an investment is.

**Jason:** It's a really good point. You know, our recommendations focus on increasing scrutiny on investors from countries like Russia and China, while speeding up the process for countries that are allies and that have solid investment screening regimes. But our legislative proposal that we include in our report is flexible and permits Treasury to designate additional countries of special concern through the regular notice and comment period that Treasury uses. This flexibility allows CFIUS to adapt as tactics change, and especially if investors in China begin moving money through third party nations. And, I think this is a cat and mouse game and that for every defense that we develop, a few years later, you're going to see some way of circumventing that defense. No system is perfect. And of course, investors are going to find ways around any system we put in place. But we should make it difficult, in order to impose additional costs, additional burdens, additional risks. And we need to continue to monitor on the creativity of our competitors and coming up with new investment strategies that work around the defenses that we've put in place. Which means that we will probably need to adapt those defenses. I think FIRRMA, in a way, was sort of the first adaptation of a defensive strategy, and there will need to be successors.

**Craig:** These recommendations address a very difficult problem and one that will never be solved completely or for the long term. Can you put these recommendations in the overall context of the Commission's second quarter recommendations? This is intended, really, to slow adversaries or, in this case, China in its development. But no one expects any sort of export control to stop other countries from developing similar technologies. But while we're slowing China through these kinds of measures, there are other things happening to keep the US at the forefront. Can you just give us a few lines about that?

**Jason:** I think that we view export controls and investment screening as part of a portfolio of policies that the United States should pursue to sustain its leadership in key technologies like AI. But it is certainly not the only part of that portfolio, or even the most important part of that portfolio. In fact, I'd say its value is maybe 10%, compared to the investments that we need to be making in promoting technology development, increasing our investments in research and then being able to attract and retain global talent, being much savvier about international standards, and working with our allies to collaborate in key areas of technology development. So, I don't think we should neglect that 10% where we're working on the protect-side through export controls and investments screening, but it's certainly not sufficient. And we should be doing much more than we are already to ensure that we're investing on the development side.