

Ezra Vogel:

Welcome to Harvard's Critical Issues. The bad news is of course that we're not able to assemble at Harvard as we had before the coronavirus started. The good news is that since we've taken to Zoom, we now have an audience that extends beyond our local audience, and we're happy to welcome those of you from other areas who are able to join us today. Last week is the first time we tried the Critical Issues with the Zoom, and that worked great because we had a great opening speaker who was Bill Overholt. And Bill Overholt is a friend of Jim Mulvenon, and when I suggested who were some of the speakers we should get this year, is Jim Mulvenon. And so I will turn it over to Bill Overholt, and he will introduce Jim Mulvenon. Bill Overholt, it's yours.

William Overholt:

Good afternoon everyone. It's a pleasure to introduce James Mulvenon. James is Director for Intelligence Integration at SOS International's Intelligence Solutions Group. Before that, he was Vice President of Defense Group International's Intelligence Division and Director of the Center for Intelligence Analysis. If you're wondering what all that means, James teaches managers of spooks how to manage spooks. He's often ahead of his time. When we were at Rand together in 2002, he taught me about the future problems we were going to have with Huawei. He is the author of the book Chinese Industrial Espionage, which is the Bible of American research on intellectual property theft. He got his bachelor's degree from the University of Michigan, studied Communist Party history at Fudan University in Shanghai and got his PhD from UCLA. It's a pleasure to welcome James Mulvenon.

James Mulvenon:

Thank you Bill. Thank you for the kind a invitation to speak today. I'm happy to be with all of you. You're right, I work now for a company called SOS International right here on the Polo. I'd like to give a shout out to the SOSI employees around the world that may be attending today. And also a bit of a preview, we just sent to the publisher the sequel for Chinese Industrial Espionage, which is titled the same as my talk today, Beyond Espionage, and talks about many of the new phenomena.

James Mulvenon:

And now, the other interesting thing is normally at this time of year, I would be traveling around the country going to public policy schools and recruiting. I will tell you that we are hiring for all the students out there. If you speak mission-critical languages and you're eligible for us security clearance, please just DM me on Twitter because we actually hired three people in the last two weeks. So despite the pandemic, we are actively growing and looking for new people. The main theme of my talk today is continuity and change. Areas where we see continuity in our relationship with China across these very controversial areas, and in areas where we see it changing. And in my homage to Kurt Campbell, I have three points that I'd like to make today.

James Mulvenon:

The first deals with the phenomena of industrial espionage and IP theft. And despite the pandemic, which obviously has restricted our physical travel, the evolution of Chinese government sponsored behavior in this area continues a pace. Now what are my metrics for that? I will stipulate from the outset that I'm actually quite skeptical of assessments of monetary damage that people like to throw around. I think they're often self-serving and inflated. I'm much more focused on specific cases, specific damage to industries and specific companies. And I'll talk about some of that today, rather than sort of try to bowl you over with large numbers, billions of dollars here and there.

James Mulvenon:

A key indicator for me is always cases worthy of prosecution. And while I'll talk a little bit later about some of the dilemmas we've had, some of the mistakes that have been made in that area, I will tell you for many, many years of dealing with assistant US attorneys all around this country, that they are very conservative about taking cases to court, and generally don't want to go into a courtroom and be embarrassed, and generally have very high thresholds for the evidentiary standard that they use to push these cases. But why is it, frankly, let's get to the heart of the matter, why is it that we've seen this dramatic increase over the last almost 20 years in a Chinese government sponsored espionage and IP theft? Now, my good Marxist answer to that, is the economic factors of production.

James Mulvenon:

There was an interesting Chinese economic conference in December, 2004. And you have to understand, from 1978 to 2004 we had seen all of the dramatic successes of the Chinese economic modernization. They were on the covers of all the magazines, quadrupled their GDP, but there was something about the materials at this meeting that suggested a malaise. There was a reassessment, and in particular they were very focused on the fact that what had happened, as dramatic as it was, as successful as it was had nonetheless been a fairly shallow modernization. What do I mean by that? They were still largely enclaves of places in China that were importing components from abroad, assembling those components and the finished products and exporting, rather than the depth of indigenous production, indigenous innovation within China.

James Mulvenon:

And moreover than that, there was a real concern that there were just not enough global Chinese brands, unless you were a wine aficionado and you had a higher wine fridge. Or you're a telecoms company with Huawei equipment. In 2004 that were really not that many Chinese brands. And so they began to put together the elements of a very large strategic effort, the most important of which were a series of industrial plants. And I want to highlight the 2006 to 2020, mid to long range S&T plan, which highlighted the extent to which they needed to put greater pressure on the multinational companies that were operating in China to more aggressively and more rapidly transfer their technology to promote this indigenous innovation of Chinese companies.

James Mulvenon:

But there was also a section of that report that called for a collection by other means. Which in other sources we know was a euphemism for increasing espionage and IP theft because most of the technology that they were really interested on the high end was simply not resident in China. And the only option at that point they had to get to it, was through these elicited efforts. But there were a range of other key elements of this strategic effort. There were the state subsidies. Many of you are familiar no doubt with China's efforts to modernize its semiconductor and integrated circuit industry. And they set up the so-called IC fund with \$150 billion to go out and buy major companies, major technology around the world. The phenomenon of military civilian fusion, which used to be known as civil military integration, which was the dynamic by which defense technologies and civilian technologies could be interchanged within those two systems.

James Mulvenon:

And here I have to give a shout out to Harvard Zone, Elsa Kania, who is doing some really interesting work in that area, and I'm always happy to work with her. You have the national champion phenomena,

and here we can talk about Huawei all day long, but national champions in each industry that get generous state subsidies through bank lines of credit, tax breaks and other things in order to be portrayed to the outside world as China's global competitor in a given industry. We've seen a blizzard of laws and regulations come out in the last five or six years, including the cybersecurity law which dramatically changes the dynamic for information technology modernization and data protection within China. We've seen China use information and communication technology standards at the global level as a trade weapon in order to create openings for Chinese companies, and in some cases to distort the international market.

James Mulvenon:

We've seen in recent years, their use of overseas investment strategies through mergers and acquisitions and joint ventures and greenfield investments that then fundamentally caused the US Congress to update our committee for foreign investment in United States law to anticipate some of these new moves. Although it's a little [inaudible 00:09:53] right now, obviously one belt, one road as a mechanism in my view for creating global path dependency for Chinese companies and Chinese standards around the world. And then finally, cyber and technology espionage to facilitate a number of these dynamics. So I want you to think first and foremost about embedding that espionage within all the contours of that larger strategic effort. Now, some of you may be familiar with a study that Andrew Kim did in the Cardozo Law Review, in which he analyzed quite a few Chinese espionage and IP theft cases in the United States at the behest of the committee for 100, looking for evidence of racial bias within the department of justice prosecutions.

James Mulvenon:

I do think that there were significant methodological flaws in Mr. Kim's study, which I lay out at more length in our new book. And I'm happy to talk about it in the Q & A, but I think suffice to say, one of the comments of one of the external reviewers that was actually quoted in the report, maybe sufficient to sort of summarize my position, Dr. David Harris said, "We must recognize the limitations of these data. We cannot tell how many investigations took place during the study period, what ethnic groups the target of those investigations came from, and the rate at which those investigations actually blossomed into charged cases. The data presented in this study do not prove the existence of researching while Asian." So I have to applaud Mr. Kim for putting such a strong critique review within his report itself, but I have to agree with a lot of the findings.

James Mulvenon:

Instead, I've done a lot of my own analysis of the cases since 2004 and I'd like to offer that to you. The Department of Justice recently announced that there were over a thousand investigations currently ongoing around the United States involving IP theft with a China nexus. That either means that there is a contact with some sort of an entity in China, all the way to the point where there is an identified foreign instrumentality, which is an entity that is either part of the Chinese government or they're under the direct control of the Chinese government who is involved in the cases. And all 56 of the FBI's field offices nationwide are conducting investigations involving IP theft. Since the early 2000's, 80% of the economic espionage cases in the United States involved some level of Chinese instrumentality, and there's a nexus to China in at least 60% of the trade secret theft cases.

James Mulvenon:

Now, in my own research, I've looked at 147 of these cases, either what we call an 1831 case, which is economic espionage under US law, or an 1832 which is trade secret theft. Among those 147 cases, there were 33 indictments that are still pending, and there were 114 convictions. But lest anybody out there think that this is some recent phenomena associated with the current administration or with the trade war, I will tell you that that data reveal very significant spikes in cases in 2009 and 2013 during the Obama administration. I will say that in terms of the cases in the last two or three years, it's clear that the DOJ's China initiative has in fact devoted additional resources to these cases and certainly greater encouragement of these cases. One of the interesting findings though is that contrary to Mr. Kim's study that it's actually national origin, not ethnicity that is the most just positive indicator among the data set.

James Mulvenon:

That the number of either PRC citizens who were permanent residents in the United States or naturalized US citizens of PRC origin, never fell below half in any of the cases. And I would only contrast that with the recent espionage cases involving more traditional government secret stealing espionage, in which the vast majority of the people convicted in the United States, and here I'm talking about Kevin Patrick Mallory, Glenn Duffy Shriver, Fondren and Birgisson were in fact not Chinese ethnicity at all. And so we see the Chinese intelligence services perhaps trying to go against type, perhaps go against what they believe as a counterintelligence bias within the US system by recruiting Anglos as potential assets rather than recruiting ethnic Chinese. But on the IP theft and economic espionage side, it's overwhelmingly PRC citizens or naturalized US citizens of PRC origin.

James Mulvenon:

Interestingly, very few people from Taiwan, despite the linguistic and cultural affinity that they might enjoy in being able to facilitate those kinds of cases. But the other interesting thing that pops out of the data for me is who the beneficiaries are in China across these 147 cases. 57% of them are organizations that I would identify as a foreign instrumentality. Now that's not just government and military organizations, but given the nature of the Chinese political milieu, I would also include, for instance, universities in that. Why? Because Chinese universities, many of them are either directly subordinate to the State Administration for Science, Technology and Industry for National Defense, like Harbin Engineering University, or are subordinate to the Ministry of Education. But my own experience at Fudan, certainly taught me that the party secretary of Fudan University was much more powerful than the president of Fudan University.

James Mulvenon:

And so the existence of party committees throughout the university system, the ability of the ministry of education, which is itself dominated by its party committee to appoint major administrators in the university, department chiefs and so on and so forth, I do not view Chinese universities therefore, as independent educational institutions as we're accustomed to in the United States. And in fact there's plenty of evidence in the cases involving Chinese Universities, that they worked very closely with the ministries of science and technology and the ministry of industry and information technology to coordinate collection requirements, to receive funding, to open up labs that were going to exploit the technology that was being acquired from the United States through these collection channels.

James Mulvenon:

Now this is not to say that there haven't been wrongful accusations against individuals of Chinese descent here in the United States. That is certainly true, and I would only make the following a

distinction, which is... And this may be cold comfort, and there's nothing I can really do about that, but the combination of our free press and our independent judiciary in the United States has meant that many of the people, if not all of them, that were wrongly accused, have in fact avenues for relief from those wrongful accusations, and have in fact received monetary awards from the US government for those wrongful accusations. And I can only contrast that with China, which brags of it's near 100% conviction rate within its judicial system and ask whether people in fact would have the same type of relief from wrongful accusation and prosecution on the Chinese side. Just something for you to ponder.

James Mulvenon:

My second point today is that the US government, I think rightly, and this was the main theme of our book, Chinese industrial espionage, which I coauthored with two colleagues from the US government, that the US government is increasingly focused not on economic espionage and IP theft as a criminal threshold, but increasingly focused on what we call nontraditional collection. And this is collection going on among researchers in labs and universities and defense industrial based companies in the United States where people are being co-opted for technology transfer that falls below the criminal threshold of 1831 or 1832, the economic espionage and trade secret theft cases, but is nonetheless injurious to US national security. And one of the non-traditional collection, Hathaways that you've likely heard a lot about at Harvard, are the so-called Chinese government talent programs. In particular the most infamous of them, the Thousand Talents Program.

James Mulvenon:

Now what are these talent programs? Well, these are very robustly funded programs by the Chinese government to attract foreign talent from abroad to either do research for or research in China. In other words, to find a mechanism to get access to the know-how and the innovation and the scientific expertise that is resident outside of China, to bring it back to China in order to improve indigenous innovation in China and its own R&D base. Now the thousand talents program, of which I said is one of the largest and most famous of these, according to the global times, one of the Chinese propaganda outlets has funded 7,000 researchers around the globe since 2008. Now the Thousand Talents Program is only one of many programs within the Chinese system. In fact, we're doing a lot of research on the over 590 other talent programs as well as the 100 startup contests and the 500 supporting offices that exist in China in order to attract this kind of talent from abroad.

James Mulvenon:

Now, I'll talk more about this in a little while, but what is the importance of these talent programs? In my view, it actually is trying to fill a major gap that has been revealed in the Chinese innovation system by the economic espionage and trade secret theft, which is to say we see time and time again in these cases where Chinese entities are stealing the first generation of a technology, bringing it back to China, and then the army of... And here we often hear about China graduating huge numbers of engineers every year, 500,000 engineers. I wouldn't call all of them engineers in the sense that we would say someone from MIT is an engineer. I think many of them are better described as technicians. And these technicians have a remarkable track record through the decades of being able to reverse engineer products from abroad.

James Mulvenon:

There's a particular talent there. But reverse engineering is not the same as understanding the organic know-how in innovation. It's at the heart of these technologies. And time and time again, we see

Chinese entities having to come back and stealing the second generation of the technology rather than being able to learn enough from the first stolen generation to be able to then innovate and create the second generation. The talent programs in my view exist in part to bring the people back to China who can provide the missing intangible context, the mortar between the bricks, the organic [Foreign language 00:21:54] in Chinese that is at the heart of these technologies, that is not contained in the stolen blueprints. When these individuals come back and they have these two-week espionage vacations in China and they go to The Great Wall and they visit the Terracotta Warriors, but they also spend a week with peers from their industry being debriefed on various technologies, that these are the very fora in which many of these key contextual and intangible innovation questions can be asked about some of these stolen technologies.

James Mulvenon:

But these talent programs feed into an enormous tech transfer system on the Chinese side. There are over two dozen laws that we've identified in China creating this transfer apparatus. It is managed by a professional cadre of hundreds, if not thousands of Chinese government S&T transfer specialists. These talent programs feed into over 300 so-called pioneering parks for overseas Chinese scholars and 500 incubators, 160 innovation centers, 276 national model transfer organizations, even including 90 plus nonprofit organizations located in the United States who are partnered with a Chinese communist party and Chinese local and national government organizations in order to spot and assess US technical personnel and bring those people into the talent programs so that they can then participate in this tech transfer apparatus. And when you read Chinese material, and I've always been struck frankly as a Sinologist by the extent to which the Chinese government regards its languages, its first layer of crypto, because so much of the material, the thousands of primary source footnotes in our first book on Chinese industrial espionage were overwhelmingly Chinese government documents that had never been translated.

James Mulvenon:

And one of the consistent themes in these documents is with the so called the concept of operating from two basis, jidi, liang ge jidi. And what they mean by that is rather than trying to lure scientific and research personnel to China permanently, that they would prefer that those personnel stay in the United States and in Western Europe and other places because that's where the innovation is occurring. And so while they want them to travel to China at Chinese government expense, they want them to divulge technical knowledge through scripted venues. They want to be briefed, they want to brief these individuals on Chinese technology interests. They also then want them to return to this foreign base, this foreign GD, so that they can maintain their access to the information. Now, some of you are familiar in the last year or two that both the National Institute of health and the National Science Foundation in the United States have begun to crack down on what they regard as inappropriate behavior by scientists and researchers in the United States who have been receiving NIH and NSF grant money.

James Mulvenon:

And what they're charging them with, again, to continue this theme, my second theme of non traditional collection, they are not charging these researchers and scientists with criminal economic espionage or IP theft in almost all cases, but instead charging them with fraud and with lack of disclosure of conflicts of interest. And perhaps most seriously in an academic context, charging people who have been sharing embargoed peer review proposals that have been sent to them as part of the peer review process, and violating their peer review contract by sharing those proposals with colleagues

abroad particularly in China. And we have evidence that then those colleagues in China have been setting up companies and conducting that research and stealing those ideas before they've even been approved in the United States, which is a gross violation of academic rules and academic norms and standards.

James Mulvenon:

Now, that being said, NIH has only singled out 61 research institutions in the United States out of the hundreds if not thousands of research institutes and only 16 cases for legal action. I think that the mainstream media would give you the impression that there is a gigantic dragnet against thousands of ethnic Chinese researchers all over the country, and it's simply not born out by the facts. In fact, NSF recently came out and said that while 6,000 plus ethnic Chinese researchers have received grants over the years, they only can identify 180 or so cases of wrongdoing. And again, this wrongdoing is very much along the lines of fraud. In particular researchers and scientists who have not disclosed to their home research institution the money that they are receiving from foreign universities, the foreign appointments that they have been receiving, and in the case of NIH and NSF, incorrectly filling out US government paperwork to the extent to which they are double dipping and receiving money from two different organizations, one US government, one PRC government for the same research, which is a violation of the contracts that they would have with the US government.

James Mulvenon:

Now I am unable for a variety of reasons to comment on the Professor Libor case. So any of you that have questions about that, I'm going to have to mute on that. But I would say that the details of that case, while at the high end in terms of the money involved, are very similar to many of the cases we have around the country. And professor Libor is not alone in being of non-ethnic Chinese descent who is nonetheless being investigated for these types of academic violations. Good examples, for instance Professor Percival Zhang at Virginia Tech who was a full time professor there and yet was also claiming that he had a full time job at the Tianjin Institute of Industrial Biology. Can't be in two places at once. I'm not a quantum physicist, but clearly trying to charge the same hours to two different institutions.

James Mulvenon:

Similarly, Franklin Tao at the University of Kansas, similar charge that he had accepted a position at Fuzhou University, which simply violated the laws of physics in terms of being able to be at two places at once and to receive two sources of unreported income. And Chunzai Wang from the Government National Oceanic and Atmospheric Agency, who had also accepted a Chinese position. In all cases, these transgressions had gone on for a long time, and it is fair to say that the US government had not been as perspicacious as it could have in the past. But the rules are the rules, and so I think going forward there's going to be much greater scrutiny of these kinds of activities involving research collaboration with China.

James Mulvenon:

That being said, the sunshine policy of being completely transparent, no one is being persecuted or investigated for their overt relationships with Chinese research organizations, unless those overt relationships have some other reason to be investigated such as violation of export controls, violations of deemed exports or ITR, that fall within those rules systems. And so maybe it's just because I've spent my life having to live transparently with US government reporting requirements, but I think increasingly that's going to be de rigueur for academic research that involves US government grants and funding.

James Mulvenon:

My third and final point today deals with Chinese cyber espionage and perhaps more recently the digital disinformation operations that we see coming out of China, particularly during COVID-19. Now cyber espionage has long been China's preferred mode of conducting espionage. It has numerous advantages. Because of social media, it is now possible to do targeting against all of us at distance because of oversharing that we do on LinkedIn and on Facebook and other things that frankly are a targeter's dream from a human intelligence perspective. The logistics of doing cyber espionage versus having to use human assets and the potential signatures and vulnerabilities that creates, it's much preferable, for instance, in the intelligence game to be able to do plausibly deniable cyber espionage as opposed to using a human asset who could potentially then be caught, and perp-walked on the steps of the federal courthouse in Los Angeles much to the embarrassment of the Chinese government.

James Mulvenon:

Now this is still very current. In fact, I would argue that under COVID-19, because of the travel restrictions that are preventing the kind of non traditional collection and talent program travel that we saw before, that cyber espionage is now more relevant than ever. Recently, the US government called out APT 10, Advanced Persistent Threat Group 10, which had targeted 45 US companies across banking, finance, telecoms, biotech, auto healthcare and mining, as well as US government agencies stealing a hundred thousand records from the personnel records in the US Navy, the Jet Propulsion Lab, and the NASA Goddard Space Center. And the attribution of this activity was a contractor company in China that was operating at the behest of the Ministry of State Security's, Tianjin State Security Bureau in order to carry out these kinds of activities.

James Mulvenon:

Now this activity has become more sophisticated over time. There's a lot of interesting empirical challenges in analyzing this activity, particularly after Xi Jinping's supposed promise in the Rose Garden in 2015 that commercial cyber espionage was going to decline. What instead we saw was a dramatic increase in the quality of Chinese government tradecraft, and a dramatic increase in the attribution problems associated with that tradecraft as they move their command and control of the US cloud and increased their use of virtual machines and other things in order to obfuscate what they were doing.

James Mulvenon:

But just this morning in the New York Times there are some very interesting articles about China's growing use of digital disinformation operations in the United States. Here I would draw some important distinctions with the Russians. The Russians, whether we're looking at their activities in Ukraine or the near abroad in Transdniestria or the Baltics or in Belarus or even the United States, we see a clear, sophisticated pattern of them pitting left against right, right against left, both ends against the middle, and really seeking to de legitimize political and social institutions inside those countries. Historically, China's more timid efforts at information operations had exclusively fallen into two buckets. One was to refute quite loudly Chinese criticism from abroad. For instance, it's activities in Xinjiang, it's activities in suppressing the protests in Hong Kong, or to present China in the best possible positive light abroad.

James Mulvenon:

But we are increasingly seeing a real edge to Chinese information operations and more of a subversion element. This was certainly true in what we saw in the Taiwan presidential election where the Chinese military's 311 Base, otherwise known as the voice of the Strait, was conducting operations on Facebook,

which is very popular in Taiwan, particularly pro Han Kuo-yu sites. And certainly seeking to defame and lower the support for the DPP candidate, Tsai Ing-wen. And even doing information operations inside of digital channels that we don't have here in the United States like the Telnet based PTT forums, particularly the #Hatepolitics forum, in order to push the pro Han message. Certainly as we began to see the initial use of so-called deep-fake videos, which I think is a harbinger of things that we might see in the 2020 presidential election here in the United States.

James Mulvenon:

And then finally we've seen this very aggressive, so-called Wolf Warrior Diplomacy, where dozens of Chinese diplomatic officials have set up accounts on Twitter. Which in my view is pretty cowardly considering that it's a platform that the majority of their own population can't see. So it's clearly directed information operations outside of China. But these are extremely popular on Chinese social media right now, and there is no incentive for the leadership to rein it in. We unfortunately now live under pandemic and in a period of increased tribalism in my view, where there's a reduced penalty for othering outsiders, popularism, and in-group rallying is all the rage. And I can't think of any reason why a Chinese political leader would want to step in front of that train. And I think Xi Jinping frankly has a great deal of fear from a Bushy-like kind of character or Cheranovsky kind of character that decides to play to the crowds and push a very anti foreign, pro-China populous message. And so we're certainly looking for that bubbling up in the Chinese system.

James Mulvenon:

So let me conclude, um by talking about some of the effects, I think, that COVID-19 in particular is having upon the phenomena that I've described and where we might be going from here as we continue to try and flatten the curve and recover but still confronting perhaps a world that will never be the same post COVID-19. I would say that the business community and Bill Overholt is keenly aware of this, had been the last sustained pillar supporting strategic Sino-US cooperation and collaboration. But in the last five or six years, we certainly saw that pillar began to get shaky and break, as it became increasingly difficult for some companies to make money in China as IP theft and economic espionage became more rampant.

James Mulvenon:

And so it was already shaky before the trade war. The trade war certainly made that shakier. We also saw Xi Jinping and the Chinese system regressing to greater focus on central planning. Um, greater privilege being given to state-owned enterprises, greater focus on state-directed R&D, and frankly the playing field was becoming less and less level even though 30 years after reform and opening, many of us had believed that the playing field would become more level. And for me, one of my metrics of this, is the fleeing American expatriates from China who I thought would never leave, but have begun leaving because of their perception that the system was never going to give them a fair shake, and the pollution and all of the other things that had made life there less than hospitable.

James Mulvenon:

And the trade war was already breaking the WTO and the multilateral trade system. COVID-19 in my view was only accelerating those trends. I believe that we're going to come out of COVID-19 with a permanently changed global economy. Many of the multinational companies that I talked to that had feared that they needed to diversify their global supply chains because of the trade war, are now using global pandemic as a non-trade war related rationale for diversifying those global supply chains. I think

the era of extreme clustering of industrial clusters inside of China will be over. But China's strategic plans have not changed. The go-out strategy has not changed. BRI, One Belt, One Road has not changed, and Xi Jinping's aspirations for the Chinese dream have not changed.

James Mulvenon:

And therefore, I think this puts even more pressure on using economic espionage and recruiting talent from abroad as potentially some of the multinational enterprises that had been the target of domestic technology transfer, seek to do that production and innovation elsewhere. Going forward also, I think we should not expect to see some changes in some major thrusts in US policy. In particular, executive orders that seek to impose sanctions on state-owned enterprise executives who benefit from cyber espionage. There was an executive order to that effect under the Obama administration, I wouldn't be surprised to see it again in the current administration. Obviously we've already reformed the law and the committee for foreign investment in the United States with the so-called FIRRMA, which made it less voluntary, which gave the US government the opportunity to initiate investigations of Chinese merger and acquisition and investment activity.

James Mulvenon:

I would expect a greater strengthening of the Foreign Agent Registration Act, and less leniency about people acting as agents of the Chinese government who have not registered under FARA. And for many of the universities that I talked to, I would expect a deemed export reform. In other words, deemed export is when, for instance, an individual at a lab that a US company might run in China if they had a PRC national working on an instrument in that lab in China that would have required an export license to sell that piece of instrument to a Chinese company or Institute, they have to get a deemed export license for that. I wouldn't be surprised in the near term for a foreign national using that instrument at a lab in a US university, that that US university would also be required to get a deemed export license.

James Mulvenon:

I would expect greater scrutiny of the student visa system under SEVIS, and I would even expect that we're going to see major changes in Hong Kong's custom status which had been a separate custom zone post reversion as a way of protecting Hong Kong's economic and political rights, but as this has instead become the major trans-shipment point for illicit tech transfer to China because of the difference in those customs regulations. I would expect to see in the near future that those special Hong Kong exemptions would be repealed, and Hong Kong would increasingly be treated as part of a PRC custom zone. And none of those trends I think would be decelerated or changed because of COVID. So let me stop right there, Bill, and I'm happy to take any of the questions that may have popped up in the chat that you could help me moderate.

William Overholt:

Let me lead off with one question. All of these bad things are happening and we're trying to prevent that. There are a lot of good things happening too, scholarly conferences. When I was at Harvard's Ash Center before the season being here, we always had three vice ministers from China who would typically spend a semester. And they got to understand how the US worked. It facilitated my research a lot to be able to walk across the hall and say, "What's this China 2030 all about?" An awful lot of that has been shut down. Actually the guy who wrote four books within China promoting the idea of thousand talents was my colleague there for a year, and he was very idealistic. So what we found is bad things

that weren't being addressed are being addressed, but on both sides, the good exchanges which I think are very necessary for both our countries to understand each other are being shut down too.

William Overholt:

There are no vice ministers coming to spend a year anymore. That's a decision, big decision. So do you see a way that we can encourage and restore some of the good exchanges while we deal with the bad things that everybody, at least in America, acknowledges are happening?

James Mulvenon:

I can only be fair and say that for the first 10 years of my career at Rand that a great deal of my professional activity involved participating in precisely the kind of venues and fora that you're talking about, Bill. Whether it was Track Twos, pure academic, although there were really no such thing as Track Twos with China, right? Particularly when you're dealing with organizations like Kicker and others. But Track 1.5s, because most of my research over the years has focused on areas that are pretty sensitive. Cyber, nuclear, intellectual property theft, things along those lines, space. And the Chinese always prefer to have so-called Track 1.5 dialogues, where non-governmental institutions are technically the host. And then we can each invite government officials from both sides who can make non statements, issue non papers, signal each other, socialize with each other. And I have certainly seen the value of that over the years.

James Mulvenon:

All I can say is that there's probably going to be greater scrutiny of who specifically those individuals are. As we learn more and more about influence organizations and the actual providence and origins of individuals that might not have been scrutinized in the past, may achieve more scrutiny. But God knows there were plenty of times when I would have to contact people in the US government, and try and put people on must fly lists so that they could get through the visa process to be able to come to various conferences.

James Mulvenon:

So certainly the answer is not to completely close all of our sphincters and not have those levels of dialogue. We even had those levels of dialogue during the worst periods of the cold war, and they certainly have their purpose. The pendulum may have swung over-corrected the wrong way. That being said, as someone who has been PNG-ed from China since the publication of Chinese industrial espionage, I would tell current and future scholars that we live in a boon age in terms of being able to still conduct research that doesn't involve interviewing, that our access while being increasingly restricted to vast amounts of materials available online... The one time in my career that I've been to Fairbank last year, I insisted on being taken down into the vaunted library so that I could get access, so I could see some of those materials.

James Mulvenon:

China is very unique in the extent to which, particularly on issues that I research on, military and other things, to have such a vast publishing enterprise. So it's not like we're reverting in my view back to the era where all we had was People's Daily and Beijing Review and a couple of other propaganda rags to be able to try and divine what was going on in China. But I would also make the argument that it's the absence of our Track One dialogues under the previous security dialogues we used to have with the Chinese, that those were absolutely essential that the Obama administration ran. You can have those

dialogues even when you strongly disagree with people. I embrace the dialectic, and I think that we should embrace the dialectic. If we can't defend our positions and policies with our Chinese counterparts, then maybe they're not worth defending.

James Mulvenon:

And so I just think that there's been an unfortunate retrenchment, and a lot of the ill will on both sides related to expelling of reporters, which I labor on the Chinese side because I think that having US journalists in China is as good for China as it is for the United States. And so I do believe that post COVID-19, we're going to have to restore some of these mechanisms. But if you saw the Pew polling yesterday, there has been a major shift in American attitudes about China because of the progression of this pandemic. And it's going to take a long time for the relationship to heal from this.

Ezra Vogel:

I think we are all indebted to you for this very thoughtful, detailed analysis. The question we have I think in universities is that there are a lot of good reasons for cooperation and a lot of good reasons for our study that are open. How do you draw the line between what is good research that should be encouraged, mutual learning, if we were working on something that would reduce the problems of the virus now, and we can put some joint results that's obviously good for everybody. So how do you draw the line as national policy for what we should be doing to encourage a global research and where it becomes a national problem where it's a stealing and is a real issue?

James Mulvenon:

Well, I mean, I think the most obvious candidates are areas in which our mutual research is mutually beneficial. And number one on the list is climate change. Number two on the list is global bio health. If anything, the last five to 10 years has cast into stark relief the importance of both of those. Now, that's not to say that within those, like for instance in global bio health, there are certainly things where there are national security implications where things can be weaponized. But we have mechanisms under the Biological Warfare Convention which the US and China are both signatories for dealing with that. And frankly I think that that collaboration should also focus on raising certain standards. I think that one of the dilemmas we have with China on global public health rate in the last decade has been the extent to which the difference in the Chinese regulations and rules and norms have meant that they become the place of choice for various types of genomic research and human subject testing that frankly doesn't meet our ethical and regulatory standards.

James Mulvenon:

I'm particularly concerned about Chinese research involving things like CRISPR. But we can't alter that by cutting ourselves off from it, but instead there has to be an incentive-based system where the Chinese side sees the value in collaborating with us, and an exchange has to meet certain regulatory and ethical thresholds that we're comfortable with. And that's one of the values. As you know from your many exchanges, one of the many things that come out of that are greater understanding of each other's systems as well as greater socialization about those kinds of standards. And that certainly won't happen if we're doing that research in isolation from one another.

Ezra Vogel:

I want to thank the speaker again for spending the time and giving us such an informative presentation.

This transcript was exported on May 01, 2020 - view latest version [here](#).

James Mulvenon:

Oh, well thank you Ezra and Bill for the invitation, and I look forward to seeing you guys in some of my favorite patriot bars in Southie when all this recent unpleasantness is over.

Ezra Vogel:

I guess on that note, we will conclude. Thank you all. And a recording of this will be made available on our website and across our social media channels. Thank you again.