National Security and Election Security: A Discussion with DOJ Assistant Attorney General John Demers

TRANSCRIPT

Discussion…………………………………………………………………………………………………………………………………………………………………………..2

- Daniel McKivergan, Hudson Institute Vice President for Government Relations
- John Demers, Assistant Attorney General for National Security at the U.S Department of Justice

Disclaimer: This transcript is based off of a recorded video conference and breaks in the stream may have resulted in mistranscriptions in the text.

A video of the event is available: https://www.hudson.org/events/1865-national-security-and-election-security-a-discussion-with-doj-assistant-attorney-general-john-demers102020

About Hudson Institute: Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings, and recommendations
Dan McKivergan:
Hello, I'm Dan McKivergan, Vice President for Government Relations at Hudson. Thank you for joining us today for a conversation with John Demers, who is the Assistant Attorney General for National Security at the Department of Justice. In this role, he leads the Department's efforts to combat terrorism and espionage, cyber crime and other threats to national security. He also leads the Department's China initiative to counter Beijing's illegal activities conducted inside the United States. Prior to joining the Department, John was vice president and assistant general counsel at the Boeing Company. John, welcome. Thank you.

John Demers:
Thanks very much. Thank you for having me on.

Dan McKivergan:
Absolutely. Before I go into the questions that I had prior to Friday, I just wanted to start off, given the news of the President's diagnosis. Have you seen any change in the scope or pace of activities by either China or Russia directed against the United States since the news broke?

John Demers:
No, I haven't. At least, not as of yet. No change, obviously they continue to pose a counterintelligence threat to us, but I haven't noticed a change.

Dan McKivergan:
Okay. And now we're going to go to questions that I think would be helpful for people [who] don't understand the Department and the division and some of the challenges that we're facing. Could you explain the national security division, why it was formed and how it works with other agencies and departments in the government to carry out its mission?

John Demers:
Sure. The National Security Division is the newest division at the Department set up in 2006 in response to the September 11th attacks and the change in the way that we were approaching terrorism and other national security threats. It's first new division at the Department, since the Civil Rights Division, back in the 1950s. The idea behind it was to bring together all of the parts of the Department that had been working on national security related issues. Both the prosecutors who at the time were in the Criminal Division, Counter-terrorism, counterespionage prosecutors, but also the folks who do foreign investment reviews and a very big group, which is the lawyers who write up the FISA applications to the Foreign Intelligence Surveillance Court to authorize foreign intelligence surveillance here in the US.

Before 9/11, the thought was that the law enforcement functions of national security, like the prosecutors, had to be kept separate from the intelligence functions of national security for civil liberties purposes. And there was what was called a wall between those two groups, both at the FBI and here at Main Justice. After 9/11, and you'll remember the failure to connect the dots and the discussion around the need to integrate the different pieces of work that the Department and that the government as a whole was doing on national security and so you had the creation of the Department of Homeland Security, for instance, at a bigger level. Here in the Department, we had a reorganization at the Bureau and then we had a reorganization here in the National Security Division to bring all these individuals who in the past have been told to not to work together, to share information only in very controlled ways and limited circumstances, to be working together and sharing information freely.
Dan McKivergan:
I know you were at the Department earlier in your career and you're obviously now there as head of the division. The division was set up in the wake of 9/11, primarily at that time focused on counter-terrorism. And now you've seen that mission expanded largely because of the activities of China who can employ a lot of national wealth and resources in the cyber realm, into intellectual property theft and other operations against us. What have been some of the challenges in terms of reorganizing or adapting the Department and the division to this now larger set of challenges that are likely to be with us for some time?

John Demers:
Right. Now that's absolutely right. When I was here, I was here at the beginning of the division in 2006 to 2009 and it really was mainly counter-terrorism work. Not just mainly, 90% probably what we were doing, surveillance investigations, prosecutions of terrorists. Coming back to it nine years later in 2018, I think three major observations. First, the integration worked. People were working together in that had developed over time. Second, the big shift that you talked about, which is the shift from an almost exclusively counter-terrorist focus to a heavy emphasis on nation state activity. We have China, Russia, Korea, North Korea. Those are the main nation state threat actors that we talk about. And if you look back at our cases over the last several years, you'll see that most of them fall within those four countries and China being sort of the number one among those four in this area in terms of activity.

And then the related development is the rise of cyber as a means to project nation state power. Back in 2006, 2009, we were certainly focused on terrorist use of the internet, mainly for recruiting purposes. Although of course, also for communicating over email and things like that, but mainly we were focused on recruiting and that still occurs. Plenty of terrorism videos out there, if you want to go radicalize yourself. But the rise of cyber has really been a nation state story and those actors have the sophistication technologically, educationally to use cyber to steal. Theft of intellectual property, to rob banks, as we've seen the North Koreans do to get the currency and the hard reserves that they need, to as we saw the Russians do, use it for political influence activities through social media.

Across that range of activities and then of course we have sort of even the more worrisome attacks and exploration of the country's infrastructure, whether it's electric grids, water. Haven't seen significant incidents along those lines, but we see a lot of activities in preparation there. That's really been a huge development and the division responded by reorganizing itself. Now we have a group of lawyers who are focused on the cyber cases. We have built out the group of lawyers who are focused on the nation state side of things, for foreign investment reviews, telecommunications licensing reviews and then on the more traditional counterintelligence espionage prosecutions also. That's been a big change. Of course, the counter-terrorism lawyers are still doing their work and we just finished repatriating some Americans who were held by the Syrian Democratic Forces who had gone to fight for ISIS. That work continues. But the shift in adding this big nation state focus has been significant.

Dan McKivergan:
Continuing the theme that you were just discussing on nation states, you're running now the China initiative. Can you explain why that was formed? Was there a specific trigger? Or was it an accumulation of events that led to the decision that we need to have a standalone kind of focus in this area, as opposed to having it put into some other room where they're also looking at other actors?
John Demers:
Right. The China initiative really was the organic development that arose from the intelligence that the Attorney General Sessions at the time and I were seeing on a daily basis, on an almost daily basis regarding China's theft of intellectual property. And that was different in kind of course, from traditional political espionage, which we've been dealing with all the time. And obviously other nation state actors engage in plenty of that. But also in degree, when it came to China. Even before we started this China initiative, 80% of our economic espionage cases, so that's theft of intellectual property for the benefit of the nation state factor, 80% resulted back to China. 60% of all of our theft of trade secrets cases, a much bigger number there, because that includes just private disputes as well. 60% of those cases resulted back to China.

Seeing that and then of course seeing what we were seeing on the intelligence side, we decided to put together this initiative, which would one, sort of signal to the US attorney's offices around the country that these were a priority for the Attorney General, for the Department. And that we understood that these are not like drug cases or guns cases. You're not going to run up the numbers for the office and say, "Look how many cases we did this year." On the economic espionage side in particular, if you have one case that's really good. If you have two, that's fantastic. If you have none, that's not really surprising. You'll probably have one next year. We wanted a message to them, this isn't a metrics game and we understand that, but we still want you to put the resources into these cases and we are willing to prosecute those cases.

And then we wanted to arm them to with information that was not classified so that they could go out and do outreach to the private sector, to the academic community, which we do for Main Justice to, but 94 US attorney's offices around the country, they should really be doing that locally. But it's very hard if you get classified briefings to know, well, what can I say around leave this room? What can I say? We were hearing them and arming them with that material and going out and doing these briefings and developing these relationships with the Bureau so that when something happened at one of those companies, those companies, or those universities would feel comfortable coming forward, because really can't do these cases, we can't combat this problem of a Chinese economic espionage without the cooperation of the private sector and the universities. That piece was also important.

And we're just pulling together all these pieces of what we were doing with regard to China foreign investment reviews, as I've mentioned, telecommunications licensing reviews. Those are mainly done here at Main Justice, but we needed to be sure that they were properly resourced. And so that those are areas where we have added attorneys over the last few years. And then more generally in this counter-intelligence space.

Dan McKivergan:
Continuing with China, the House Intelligence Committee released an interesting report recently on the strategic challenge of China to the United States. And I just wanted to read a brief quote to you and then I have a question about it. It states quote, "Chinese influence operations in the United States intentionally obscure the line between typical civil society engagements and malign influence activities. Within the United States, Chinese influence operations that targeted cultural institutions, state municipal level of government offices, media organizations, educational institutions, businesses, think tanks and policy communities." My question, if you're outside the beltway and you read articles and you see media reports on this, could you explain what the difference is between malign influence activities, what they look like and how they differ from traditional espionage?
John Demers:

Malign influence activities, and I think one of the examples they cite there, take for instance, that Confucius Institutes. On the surface, these institutes are educational programs. They're I think more than a 1,000 K through 12 schools around the country. Continue to be up at a hundred or so campuses, although the numbers are coming down because of some changes in federal law to combat this. And on the surface, they look like, well, this is great. They're teaching Chinese language to students who want to learn Chinese language. They're teaching Chinese history, they're teaching Chinese culture. Those are all positives, of course and on the surface kind of politically neutral. But when you look more deeply at those programs, especially as they existed previously, you'll see that the institutes controlled who was doing the teaching and even how they were teaching. The Chinese map of areas around China is different than the State Department map of areas around China and the map that maybe the Philippines uses or Vietnam uses, et cetera.

They lay claim to territory into waters that our State Department doesn't recognize. And so you would be taught, using that material that reflected the politics and the policy priorities of the Chinese government. That's just one example. You would not be taught for instance, if you were doing a history of China, you're really not going to be taught about Tienanmen Square. And so it's about what's in there. It's also about, what's not in these curricula. That's an example of when folks talk about malign influence activity, it's generally covert. It can be coarser depending on the activity that's involved.

Open foreign influence activity is, and we have that all the time, especially here in DC. Those are folks from the embassy going out and saying, "Hey, I represent the Chinese government. Here's what the Chinese government thinks." And that's totally fine because countries get to express their views here and Americans can consider them and weigh them in the balance. What we worry a lot of times is when ideas are expressed, but the authorship of those ideas is not identified. And so we have things like the Foreign Agents Registration Act, for instance, that says, you can say whatever you want, but if you're saying it on behalf of China, you have to say that you're saying it on behalf of China, so that an American audience can appreciate that and then that will help them to assess how much weight they want to give to those statements. That's a concern in that House intelligence report among other things, there are lots of examples that the Chinese are very sophisticated in terms of their foreign influence activities.

Think the FBI director said they are the number one counterintelligence threat. Part of that is the sophistication. And the other part of that is just the resourcing. It's a tremendous economy, as well as having the will to influence us and to sell its viewpoints on a variety of policy issues. It has the resources to do so. We see, for instance, the Chinese developing relationships not just at the federal level, but at the state and local level. That's very unusual for a nation state. Really takes a lot of sophistication and resources to pull that off. But they're targeting either individuals who they think politically have a bright future ahead of them or who are influential with figures who have political power here in DC. All to the goal of supporting their policy priorities.

For instance, not wanting folks to criticize them about Hong Kong. Not wanting politicians to criticize them about their treatment of the Uyghurs and Muslim minority populations in China. On those issues and many others, Taiwan, Tibet, et cetera, they'll use their economic levers of power, as well as these political connections to try to keep criticism of them to a minimum so they can continue to do those activities undisturbed.
Dan McKivergan:
Yeah. It sounds like what you're describing, they've kind of sharpening the art of using non-traditional collectors to both to gather intelligence, but also to put out a message that benefits their view of history. Do you believe that, getting back to universities just for one second, that there's a deep enough understanding of how the Chinese may be using our freedoms and our system to advance their ideology? And to the extent that universities may be unwitting because it just conflicts with academic freedom and an exchange of ideas that makes American universities very, very important and tops of the world, in terms of that kind of philosophy, if that makes sense.

John Demers:
Yeah. I think there's increasing understanding of the threats posed by China to academic freedom and to research integrity, and on the academic freedom side, it was very interesting especially as a lot of schools went back online recently, instead of in person, a number of schools saw the need to anonymize their students' online participation in the classes. And in particular, it's to protect Chinese students who are studying here from being retaliated against either here or back home for expressing opinions that diverge with those of the Chinese government. And so that's an area that we have been thinking about and talking to universities about too. It's Chinese students on American campuses are often the subject of pressure and surveillance. And we saw one case where a student went back and he was jailed, I think for six months for some comments he had made about the Chinese premier.

They're being watched here and I think schools have become more attentive to that, especially with the passage of the new national security law that was passed in reaction to the protests in Hong Kong. That's an area I think where schools have been focusing on and we have as well. The other is in terms of research integrity and our cases that have focused on transparency in terms of disclosing to the US grant making agencies, really to your college, so that they disclose it to the grant making agency, your foreign funding sources, including anything you're getting from the Chinese Thousand Talents Program. What we've seen as we've begun to bring these cases is that there were many professors out there, many researchers out there who are getting Chinese money, but hiding that fact from their university and hiding that fact from the US grant making agencies. That runs counter to the university philosophy and culture of transparency.

Whatever area you're researching, if you're getting a significant amount of funding from a particular source, you're expected to disclose it again, so that people can assess that when they're assessing your conclusions or your views. And here, all we're asking is, disclose your affiliations with the Chinese Thousand Talents Program or other foreign funding so that the school can decide for itself whether that's consistent with your receiving that money is consistent with where the school wants to be. And so that the federal government can consider that when they're giving out money, because of course, for every grant that's given to one person, somebody else is not getting a grant. And so we don't want people double dipping.

I think, over time and I think a number of our indictments in these areas have helped. The universities have become more sensitive to those threats, but that's definitely an area where we want to continue to work with them. And on the government side, simplify and make more clean for instance, the process of disclosures of funding so you don't have a lot of different disclosure requirements for different entities. We make that simple and easy, but then on the enforcement side, continue to bring cases where people are hiding their foreign funding, or even worse, stealing intellectual property that doesn't belong to them.

Dan McKivergan:
We'll move on to Russia. And I guess the first question I have would be, have you seen any active operational cooperation or sharing information in other ways between China and Russia as opposed to both operating against the United States in somewhat similar ways, but without any active coordination?

John Demers:
Obviously can't talk about what I see on that intelligence side, but in terms of what I can say publicly, there is more alignment between those two countries than there has been historically. Some tensions, no doubt remain and distrust remain between the two of them, but we see an alignment of interest that drive similar behavior. We certainly saw that on coronavirus, for instance, and a lot of the messaging we were seeing on social media, where there was a real sort of coincidence of interest, even if I'm not saying that they were talking to each other about what their message was going to be, but the message of that, America and other democratic countries, including in Europe did a poor job of responding to coronavirus. And that's a reflection of their system and that shows that these alternative systems, whether they're Russian or they're Chinese, are superior at protecting the lives of their citizens. We saw a lot of that message sort of coalesce, even some blaming the US for the development or the spread of the coronavirus around the world. We saw some of that coalescing.

Again, I'm not saying there was a coordinated campaign, but their interests are aligning in a space like that in a way that we really hadn't seen before. And that's just one example here of what we're doing. And in other ways, they do have different tactics and approaches. We don't see, for instance, in Russia, the level of intellectual property theft that we see from China. The Russians in terms of thefts of intellectual property, are more focused on military and dual use equipment. The Chinese are focused on that, but also focused on the commercial side. Differences certainly remain, but I think we're seeing an alignment that we hadn't seen before.

Dan McKivergan:
At this point in 2016, the Russians were very active in the wake of the DNC hack and such. In this election, how would you characterize their involvement? And have they changed their tactics? I know recently the government identified a website where they were hiring American writers who didn't know who the website was being run by, but it was identified, I guess this just happened last week.

John Demers:
Yeah. Certainly, the Russians are still active on social media. Although I have to say that I think the efforts that the Bureau has made together with the social media companies to try to take down these Russian government controlled accounts to share information about them has really done a very good job in lessening the impact of their social media activity. But they're still added on social media. You saw the reports, as you said about that sort of newspaper, online newspaper.

Dan McKivergan:
Peace Data.

John Demers:
Yeah, that was being funded by the Russian government. That's another influence activity. That's newer. We didn't really see that in 2016, but we're seeing it now. But you're right. At this time in 2016, we were well into the Russian hacking and dumping efforts. Obviously we still have a month to go and so we have to remain vigilant on that front and really work to try to make sure that doesn't happen again. But I
think the work again at the Bureau that the Department of Homeland Security has been doing, that the intelligence community has been doing, we are so much aware of this threat than we were four years ago, attuned to it. And the work that they're doing with the campaigns, with the parties to help secure the infrastructure of those organizations, has made them harder targets. Doesn't mean it's impossible. Everything has vulnerabilities to it, but a lot of work and focus has gone into it. And I'm hopeful that for the next 30 days, we won't see a significant incident, but there's certainly no guarantees on this front.

Dan McKivergan:

Well what concerns you the most leading up to November 3rd and maybe the days that follow in terms of election security?

John Demers:

Well, in terms of election security, the kind of influence operation that has always concerned me the most is the hack and dump operation because individuals' personal email accounts, even their work email accounts and there's a lot of bleed over between those two category of email accounts, are a vulnerable target. And what's in them is true, even if embarrassing, et cetera. A hack and dump, they get somebody's personal emails and then releases them is, very difficult for the news folks to resist, even if they do resist it at this point, the internet will have it all out on there. And it's very difficult for Americans to resist. It's true facts, even if they're sort of illegitimately obtained. That's worried me, I think that's a more, if that can be pulled off. And we saw that by the way, not just in the political context, but one of the first uses here in the US was the Sony Media hack and dump that was done by North Korea in retaliation for the movie that they considered to be offensive to their leader.

And it's very effective. Sony suffered for that hack and dump, its relationships with other businesses with the individual actors suffered. And so that's the one that worries me on that front. On the other front, which is more of the election infrastructure, I think as we've said repeatedly, and this is more of a DHS focus than ours, it's going to be nearly impossible for anybody to change votes in a meaningful way without the US government knowing it. It's not about worrying that people are going to be able to change enough votes, but if you can mess around just a little bit, it undermines people's faith in the process.

And if this election's close and some states are contested, if you can just suggest that, look here were 10 ballots that weren't counted or 10 votes that were counted twice. And then say from that, "Who knows what else happened? Who knows what we didn't see? We know this, but we didn't see that." That can undermine Americans' faith in the system overall and then their faith that the outcome actually reflects the votes that were counted. Those are the two things that concern me the most as we go through this election soon.

Dan McKivergan:

Okay. Before we end, I know we started on the National Security Division which was formed in the wake of 9/11. Looking forward, do you have concerns about as memories fade, people becoming too comfortable that another major attack could not occur? And secondly, how does the division's approach to violent domestic extremism differ from its approach to international terrorism?

John Demers:
On the first question, not yet. The FBI and the other investigative agencies continue to be very focused on international terrorism. There is a challenge these days because of the use of encryption, to communicate encrypted apps, that makes it harder to track terrorist communications, but they remain very focused on this threat as do the prosecutors around the country. I think, what we're seeing now is the same that we've seen for several years at this point, which is continued radical, what we call a homegrown, violent extremists. They're individuals who are being radicalized on the internet. They're generally already here in the country. They're not traveling here to do an attack, but they're here. They get radicalized. They tend to attack close to home with materials that are readily available. Sometimes, just driving a car right through a bike lane as we saw in New York a few years ago. Those are hard to detect because they're not talking to a lot of people and then hard to stop because they're moving quickly from idea to fruition. That will, I think, continue to be our threat going forward on that side.

We're still seeing some individuals who want to travel abroad to commit acts of terrorism, to join various terrorist groups. Not as many as we're seeing. Just recently, we repatriated the last Americans in Syrian Democratic Forces' custody that we had charges against. We continue to focus on that. I'm not too worried about individuals in government kind of letting down their guard on the terrorism front. The big challenge going forward is we need to continue that resource while we resource the increasing threat from the nation state actors. And I think that that's going to be a difficulty going forward.

Then moving to the domestic terrorism front, I would say our approaches are to domestic terrorism, international terrorism are increasingly coming together. The big difference here is there is no domestic terrorism organization statute. The main statute that we use on the international terrorism side is material support to a foreign terrorist organization and those foreign terrorist organizations are designated by the State Department through an inter-agency process. We don't designate domestic groups as terrorist groups. And a big part of that is because we're concerned about the First Amendment implications of taking that approach to domestic terrorism.

That said, we charge plenty of cases of domestic terrorists. Some of them are charged under state law, murder, assault, et cetera. Others under federal law. And what organizationally and tactically the approach we've been taking is, the first is to call a spade a spade. If it's terrorism, let's call it terrorism even if we don't have a terrorism charge, because the way our laws is. The second is, we're taking a more proactive, disruptive approach to domestic terrorism. And that's the same approach that was the shift after 9/11. Most crimes, the crime occurs and then the police or the FBI come in and they investigate the crime, figure out who did it, charge them and prosecute them.

With terrorism, President Bush's famous line to Director Mueller was, "You need to make sure this never happens again." And so changing the Bureau on counter-terrorism matters to be more proactive into disrupting a terrorist activity before it happens. That's the approach we're now applying on the domestic terrorism side. That means sometimes charging someone who we think as domestic terrorism has been plotting or talking, maybe buying weapons, but charging them early, not waiting to see how that plot develops, but going in, maybe they are felons in possession of a firearm, at least you've disrupted that plot. And so that's something.

And then organizationally we're using, and that's something we did on the international terrorism side, organizationally, we're also using more and more what we call our joint terrorism task forces, which are the local task forces that include the various federal agencies that have law enforcement responsibilities in that area, as well as the state and local police departments so that there's information sharing and people are coordinating their law enforcement activities. Using those to target not just the international terrorists, but also the domestic terrorism. And that's very helpful because of course those organizations exist so you don't have to reinvent the wheel. You just give them this additional responsibility.
Dan McKivergan:
Thank you. I know our time is coming to an end here. Welcome any kind of concluding remarks you'd like to make before we end. Anything that comes to mind, maybe a surprise, something that surprised you taking this job that you didn't anticipate. I guess there's a lot in 2020, but anything, the floor is yours.

John Demers:
Yeah. Look, the big surprise for me coming back, I kept track of the division while I was gone, but the biggest surprise is just how much of the nation state threat occupies my time and how we're really just talking about the four countries that we've been talking about. But how really the lessons that we learn, the organizations that we set up to fight the terrorism threat, the integration of those individuals can very usefully be directed against the nation state threat as well. And so while there's a lot to do and a lot to focus on in these areas, I think these lessons of the intelligence side and the law enforcement side working closely together to fight the threat is equally useful on that side of things. And that that's been a very pleasant surprise for me.

Dan McKivergan:
All right. Well with that, I want to thank Assistant Attorney General Demers for joining us today. We really appreciate it. And everyone thank you for viewing. Goodbye.

John Demers:
Great. Thanks very much.

Dan McKivergan:
Thanks.