POLITICO

Alejandro Mayorkas arrived at DHS focused on immigration, but found himself handling cybersecurity issues.

POLITICO Pro Q&A: Alejandro Mayorkas, former deputy secretary of Homeland Security

By **TIM STARKS** | 01/17/17 05:03 AM EST

Alejandro Mayorkas came to the Department of Homeland Security to run Citizenship and Immigration Services but ended his tenure as a deputy secretary focused on cybersecurity.

Before departing in October, Mayorkas, 57, threw himself into the role of DHS's international liaison, leading the department's negotiations with China over the landmark 2015 deal forbidding cyber theft of intellectual property and making frequent trips to Israel. He also worked closely with Congress.

The Cuban-American lawyer and former U.S. attorney brought a lawyer's perspective to the field and after leaving government took a job as partner at WilmerHale. He spoke with

POLITICO last week about his experience at the department and what he sees as the biggest cybersecurity challenges.

This transcript has been edited for length and clarity.

You spent a lot of time on the international side of cybersecurity. What's important about that?

I think there’s a couple different aspects that come immediately to mind when discussing the importance of international relationships. First and foremost is cooperation in the form of shared resources, information-sharing and the like. Take a look, just to give one example, at Israel, which is very advanced in the cybersecurity realm not only in terms of capabilities but quite frankly organizationally as a government. They spent a great deal of time thinking about how best they could be organized, and work with the private sector, the unified effort to secure the cyberspace domain. We were able to reach an agreement with Israel on their participation in Automated Information Sharing.

The nature of cybersecurity threats is marked, frankly, by a lack of boundaries. The information-sharing that the Department of Homeland Security focused on was not only public-private, but it needs to be and became a country-to-country information-sharing partnership. That, I, think was the most critical aspect of our work in the international domain. Then of course it’s education. We exchange information and learn about threats an individual country suffered. It's only a matter of time and circumstance until another country faces the same threat. It’s also making sure that our relationship in cyberspace is one where we are not suffering any harm. What comes immediately to mind is our negotiations with China to ensure that the Chinese government conduct comports with international norms.

How difficult was it to negotiate the cyber theft agreement with China?

That was a real team effort, I mean across the administration. We had great collaboration with the Department of State, with White House personnel, Michael Daniel and others. That was a united effort. There was great concern that China was not adhering to the international norms, specifically the norm of requirement that one not conduct a cyberattack for the commercial benefit of a private enterprise. There were different types of responses we could bring to bear for the Chinese cyber conduct that was a great concern for the federal government and the public. What we did was, we explored whether we could actually negotiate a substantial agreement that protected the U.S. in the future. I was very involved in those initial discussions internally and with Chinese authorities in anticipation of the President Xi visit to the United States. I helped lead a working group on behalf of the

United States that met with and negotiated with my counterpart in the Chinese government and his team about whether we could in fact reach agreement.

I don't think it was contentious. I wouldn't describe it in that way. I would say that there were language issues. By that I don't mean Mandarin versus English. I think our lexicon in the cyber realm didn't match with theirs, the way their government was structured. The way it operates was very different than we operate. We had to get through some of those bureaucratic challenges, as well as a willingness to recognize there was a significant problem to be addressed. In the realm of our work, it's still at an early stage. I think it is looking promising. We are continuously or should be continuously in a verification mode on that the agreement in both its letter in spirit. The indications, until at least when I left at the very end of October, were promising.

What role did you play in the DHS/director of national intelligence joint Oct. 7 statement on Russian hacking?

I'm going to decline to comment on that. It still remains the subject of concern and focus. I will say, I consider — as many others do, as all accounts indicate and public statements indicate — interfering with our electoral process in whatever way to be a red line. It is an unacceptable intrusion on the workings of our democracy.

Was there anything more you wanted from Congress that you didn't get?

First I would say I was extraordinarly grateful for the prioritization that our committees of primary jurisdiction gave to our cybersecurity work, specifically the role of the department. [Homeland Security and Governmental Affairs], under the leadership of Ron Johnson and Tom Carper, really understood the role that the department played and could play in this realm. Similarly, Homeland Security Committee Chairman [Mike] McCaul was also pivotal in prioritizing the mission set. We accomplished a great deal. We were established as the primary government portal for the public-private partnership that it at the center of our efforts in the cyber realm. One of the things when I left that I was still hoping would occur is the reorganization of the [National Protection and Programs Directorate], not only the renaming of the organization, but also some of the reorganization within it. That was one of the primary things that remained to be accomplished.

What are the biggest remaining cybersecurity challenges overall?

On the federal government side, it remains a work in progress in terms of the actual cybersecurity of the federal government and the information it's holding. That's a work in progress on the private sector side at well. There is an increasing public awareness of the challenge. We do have to level-set. We have to understand that the goal is to make the success of an attack as difficult as possible. It’s not going to be impossible. But you can do the work that prevents a cyberattack from replicating the harm because we’ve shared information after the first attack so a duplicate attack is thwarted. We can make sure that the bad actor will have to have a certain level of sophistication and a certain amount of time and resources in order to penetrate our defenses. It should be very difficult if we’re sharing information effectively and taking the cybersecurity measures available. We should be limiting the pool of hackers who can actually succeed to those who are expert and have significant resources and time. We want to constantly increase the height of the wall that a bad actor would have to climb over to get to the intended target. That obviously remains a work in progress. There's a lot more runway to cover in the information sharing domain.

And I also think that we're going to have to see how we can bring together what is becoming increasingly a patchwork of rules, guidelines and regulations that govern cyberspace. In your newsletter you just wrote about New York’s efforts in the cyber realm. There are companies, of course, that cover many jurisdictions across the country. If each state has a different set of rules and regulations it becomes increasingly difficult for a company present in multiple jurisdictions to determine how best it can comply with the patchwork of regulations, how best to guide its personnel in achieving a cybersecurity footprint that comports with that patchwork. It would be great if we could bring some cohesiveness to the landscape.

How much was the trust relationship with the private sector affected by regulatory agencies bringing actions against companies?

It’s a really important question. Let me table-set by saying this: This issue has been growing steadily and one can take a look at the AIS platform that NPPD established and the growth in the number of companies in sharing of information as a key indication of how much I think we are improving in the public private realm. There’s still a lot of work to be done. There are barriers to greater growth. Key amongst those barriers is some residue of distrust. What is in it for a private company to share information with the government? there’s still some skepticism. At the outset of the effort, we were battling the distrust that was born of the Snowden revelations. As I observed when I spoke at DEFCON and the Black Hat conferences, that distrust was continued or renewed a bit in some corners the of private sector as a result of the disagreement around encryption. And then there were the challenges of the Wassenaar Arrangement, and then government regulatory action against private entities for cybersecurity failures.

What that last phenomenon did was, it chilled at least some companies from sharing information for fear that the government would turn around and investigate those companies to determine whether the breach they had suffered or that was attempted were part of inadequate measures on their part, instead of viewing them as victims of a harm that's ever-present. I expressed concern in public remarks and otherwise that at least some actions taken were taken, I felt, too speedily, that the standard of care in the cybersecurity arena is not well defined. I have difficulty with that standard being defined through the crucible of the courtroom rather than a cooperative exchange of ideas and information and the more orderly development of policies.