[MUSIC PLAYING]

CHRIS DAVIS: Hello and welcome to the *Career and Academic Resource Center Podcast.* I'm Chris Davis, the associate director of the Career and Academic Resource Center and the host of the podcast. And today, it is my great pleasure to be speaking to Travis Berent, who is the director for cybersecurity policy and incident response for the National Security Council, which is part of the executive branch of government.

Travis is also a current student. He is an ALM student in the international relations program here at Harvard Extension School, and I'm really happy to have Travis here today.

TRAVIS BERENT: Thanks, Chris. I'm really happy to be here. Happy to be on the podcast and provide my perspective and insights and whatever I could do to hopefully have an engaging conversation that the listeners will enjoy.

CHRIS DAVIS: Thank you. Thank you so much, Travis. Yeah, so I wanted to have the opportunity to speak to you a little bit. Your role is certainly a unique one, both in terms of where you sit in the government, the National Security Council. I'd love to hear a little bit more about that.

For those who don't know, the National Security Council, I believe, just had its 75th anniversary. Is that correct? I read that it was created under the presidency of Harry Truman in 1947. So it's part of the White House administration, correct?

TRAVIS BERENT: Correct. The NSC is part of the Executive Office of the President. It's one of the many entities that report straight to the chief of staff up to the president. The NSC is obviously led by the national security advisor. Currently, it's Jake Sullivan.

And then I actually work in the cyber directorate, which is led by the deputy national security advisor for cyber and emerging technology, Anne Neuberger. So my portfolio is incident response mostly. So any time there's a significant cyber incident, someone needs to make sure that there's oversight and stewardship from the White House to facilitate how the US government responds.

There's a lot of different departments and agencies within the US government. They all bring to bear different authorities, capabilities, perspectives, and insights. And my role is to staff meetings and to make sure that we're driving towards response to different incidents that have the outcomes we're looking for, which is remediation, attribution, and making sure our systems are online, our networks are protected, and that we're also having policy responses to those incidents wherever they may come from.

I've been here for about six months now, so it's definitely getting my feet wet. Although in NSC years, that's, I guess, pretty seasoned because about 80% of the NSC is detailed from across the interagency. Really, there's a lot of people who are appointed, and then there's folks who are full-time government employees that make up the bulk of the nuts and bolts and really the line that is the NSC. And I represent that along with a bunch of other really fantastic folks that I work with across different portfolios and in the cybersecurity space.

CHRIS DAVIS: And so to understand a little more about your particular work, so I think when we had spoken before, you had mentioned that in terms of major cybersecurity incidents, you will coordinate responses within and between different law enforcement groups. Is that correct? The FBI. I think you had mentioned maybe the CIA, the Department of Homeland Security. These are the groups that you are typically working with. Is that right?

TRAVIS BERENT: Yeah, so when it comes to responding to a cyber incident, it's really a whole of government approach. Law enforcement absolutely is one aspect of that approach. It's definitely in the toolkit. But there's a lot of other entities that offer their unique authorities and capabilities when it comes to incident response.

Incident response is really broken down-- or any significant cyber incidents broken down into two categories. There's the asset response, and then there's the threat response. Asset response-- actually, the lead for that is DHS through their Cybersecurity and Infrastructure Security Agency, CISA. So they're sort of left of boom.

They're the ones who are making sure that the federal-- the F subnetworks are up to date with their cybersecurity procedures, and they're out there engaging with private sector and the critical infrastructure sectors, really advocating for increased cybersecurity hygiene, warning of threats, doing a lot of the net defense work. And then threat response here domestically under domestic cyber incident is-- the FBI is the lead for that.

And FBI will do the investigation, the attribution. They'll use legal process with DOJ, and they'll impose consequences on the adversaries who are responsible for that. And then in some cases, they'll also be responsible for retrieving funds, seizing assets.

When it comes to the intelligence agencies and the State Department, a lot of their capabilities are brought to informing-- providing information on these incidents. The Office of the Director of National Intelligence also plays a big role in providing insights through sensitive channels on the nature of these incidents and tactics, techniques, and procedures that the adversaries are using.

And then when it comes to the international incident response, of course State Department through their embassies are really able to provide assistance and expertise to our partners and allies across the world when they themselves are hit with their own cyber incidents. So no matter what the situation is, the US government really brings to bear a whole host of different agencies that have a unique role to play. But again, the main two when it comes to domestic incident response would be CISA and then FBI when it comes to the investigation.

And of course, there are others that play their own unique roles. I didn't even mention the sector risk management agencies which supports cybersecurity across all critical infrastructure sectors. And then even on the law enforcement side, Secret Service has a very significant role in investigating cyber crime as well.

CHRIS DAVIS: So I want to pivot a little bit. What you're talking about is certainly significant, weighty work. You're doing this in your day to day, and you're also an ALM student. What has the student experience been like for someone in your role? I'm sure it's been challenging.

TRAVIS BERENT: Oh, yeah. Well, for starters, my wife hates me because the hours are absolutely brutal. And you work 10, 12 hour days, and then the work never stops. And then you just have to be very disciplined to come home and put in the time and the effort required to take the degree to take the degree seriously, to take the courses seriously because they're not easy courses.

I'm starting something where I work though, right. So I'm getting the ALM and Extension Studies with the concentration on international relations, and I just so happen to be right now at the National Security Council. And I've been working in government for some time, and I thought it would be a walk in the park at first because the curriculum was just so interesting, and it just really correlated with so much of what I do professionally. But boy, was I wrong.

And I've learned a whole lot, especially as I'm just finishing up my precapstone with Dr. Miner. It's my second course with him. He's just a fantastic professor and has just taught me so much. Just listening to his lectures and really understanding the policy process.

I've only been in the policy space for six months, so at my current role, I am really benefiting, and I'm actually applying it directly. I go to class on Tuesday nights, and Wednesday mornings, I am applying the work I learned the day before. So it's been incredible, but I would say it just takes a lot of dedication. I started in 2020. It's been a long three years, but I could see the light at the end of the tunnel.

CHRIS DAVIS: What are the kinds of things that you have studied or learned in class and then applied to your work?

TRAVIS BERENT: If anyone's listening and they want to work in government, they want to work in national security, hear me pretty clearly. The work you do in the ALM will directly result in skills that you can apply towards a career in national security. I mean, I could start all the way back with my, gosh, what's the class that everyone needs to take where you learn how to research?

CHRIS DAVIS: The Proseminar?

TRAVIS BERENT: Yes, the Proseminar.

CHRIS DAVIS: The Proseminar, yeah.

TRAVIS BERENT: The Proseminar with Dr. Orkaby-- I mean, you're learning how to research. And whether you're working in law enforcement or the intelligence community or in foreign relations or just capacity building, whatever you're doing, the fundamental skill of building an argument and substantiating that argument with proper citations is the name of the game.

I mean, it's basically intelligence analysis. They just call it research. You're substantiating an assessment. You're drawing conclusions, and you're backing all that up with research. If you're working in the national security space, instead of going on HOLLIS, you're on a classified enclave, and your citations are classified reports, but it's the same process more or less, and it's a fantastic foundational building class.

So I would say a lot of it is just process. At the ALM program, everyone gets a benefit of the doubt of being an adult, right? There's not a lot of hand-holding in a lot of these courses.

You are expected to perform at a graduate level, and that mentality just also helps build good habits when it comes to strong writing, strong researching, being able to articulate your arguments or your comments and discussion boards or alongside TAs I would say just has made me considerably more polished in my ability to communicate, to write, and to research.

And then if we're going to get more on tactical, the precapstone that I'm taking right now and some of the other courses I've taken on national security and cyber policy with Dr. Reveron or Dr. Miner, even stuff on deterrence with Mr. Nichols, like these are also-- the content is applied in every day meetings or discussions to help shape how we view problems and how we solve them.

A lot of the content has served as a fantastic foundation to the work I've done before the National Security Council, the work I'm doing now at the National Security Council. I'm sure it will continue to inform how I build my opinions with whatever comes next.

CHRIS DAVIS: Is there a favorite from the courses that you've taken?

TRAVIS BERENT: There are so many unique aspects about the Harvard Extension School, and so picking a favorite probably not. But why do I like more certain things, like I'll tell you. Some classes I like, some I didn't.

But the professors themselves, like the cadre is so impressive. I took one class by a guy named Chuck Freilich. The guy was a former national security advisor for the state of Israel. I mean, talk about his perspective. The stories he tells are incredible.

The guy has seen some like historic national security hallmark pieces of Middle Eastern history that we talk about in textbooks, and you have the opportunity to spend a summer with this guy or a fall semester, whatever it is. And he's over here, giving lectures, and he sprinkles in all these anecdotes about his time working in the national security staff in Israel, and it was just fantastic. That was one of my first classes.

But then there are other courses where, like I said before, where the content is just incredible. Dr. Miner's intelligence class, Dr. Reveron's cyber course, and Dr. Orkaby's research class, those three really stick out.

But some of the more unique things about Harvard Extension-- so I guess any college or any university could have a fantastic cadre and professors. It's really just the gambit of your cohort. I have former CEOs of Fortune 500 companies. We have newscasters, we have celebrities from foreign countries.

There's people who I work with professionally, and then there's people who are just grinding. People that work at coffee shops that are doing their best to grind and switch careers. Or there's people who are older who finally have some time in life to learn. And man, hearing them talking about building a PowerPoint, and they're over here, giving you the keys to life and just based on the life that they lived.

I would say that outside of the cadre and the courses, just the general cohort has been such a joy to get to know and work with. It's definitely one of the, I have to say, probably one of the more unique parts of the Harvard Extension School experience.

CHRIS DAVIS: So when you were presumably looking at different programs, what stood out to you about the ALM? I'm curious to hear.

TRAVIS BERENT: Yeah, well I'll be candid. There is a program that I was applying to where my home agency before I got to the NSC was funding my college or grad school. And so I was looking. I was putting in for this program, and I was looking at different programs, and it had to meet criteria that it had to somehow benefit the job I was in then.

So I saw that Harvard had a program specifically for working professionals, or that's where it was marketed towards, and of course it caught my caught my eye. So I did some work and spoke to some-- yeah, I guess admissions folks and just learned about the program. It actually seemed this is a legitimate program. This is one of the many schools under Harvard itself, under the Harvard banner, and these are legitimate professors, and this is not going to be an easy program.

What I like most-- there were two things I loved most about the Harvard Extension School admissions process was, one, it was based entirely on merit. If you do well, welcome. If you don't do well, I'm not sure what happens because I did well. But I thought that was a great concept, and it definitely relieved a lot of pressure.

I'm working full-time here. I was working in the National Security space, and I didn't have time to start studying for the I guess GRE or whatever entry or whatever entry program would have been required. I knew I was dedicated, and I thought that was a great sort of way to make admissions based more on merit than anything else.

The second thing that drove me to put in for Harvard Extension School was the pandemic. I had a lot of time. When the cities are closed, I was in New York City, there's less crime. There's less national security risk. We were working, but there was definitely a bit more time.

CHRIS DAVIS: I was wondering-- you don't have to share any kind of identifying details of course, but could you talk a little bit about what your experience with Derek Reveron's course and how that applied to a real situation in the White House, because I think that's just an amazing experience to hear about.

TRAVIS BERENT: Derek Reveron has a portion in his course where you write something called a strategic options memo (SOM), and I know this is something that Dr. Miner uses, and I think a lot of this comes from some of the HKS faculty, including, I think, Graham Allison is really one of the ones along with Dr. Reveron and Dr. Miner that sort of championed this exercise.

And it's where you look at an incident. There's a scenario where there's an incident going on with national security ramifications, some sort of geopolitical incident with-- however it's written, and then you're tasked to provide strategic options, response options and short-term options and talking points for whoever your principal is. And you sort of put it all together, and that's the assignment.

I think there's a page limit, and the whole point is to keep the bottom line up front. Keep it brief, but make a strong assessment and sort of lay out the pros and cons for each option and then sort of choose one and why you're choosing it and what the expected outcomes are and what are the talking points.

So I actually early on in the job, there was a cyber incident. And I was trying to figure out, well, what are the options? What are the response options here? It's like, I am not kidding you, on some of these SOMs that Dr. Reveron had written out were so close to being real, I almost I almost emailed the guy to be like, I don't know what's going on over there, but you guys are definitely just hitting the nail on the head.

And yeah, I wrote out a-- the SOM was really for my own personal trying to frame everything up, and I actually ended up walking down the hall and delivering it to my senior director, who was fantastic. He looked at it and looked at it for a second, and then he looked at me, and he went, what the hell is this?

And I was like, it's a SOM. He's like, well, long story short, it doesn't necessarily work exactly the way it does in-- the SOM is not necessarily a known vehicle to deliver policy recommendations.

So I ended up-- and this was not how that particular individual wanted to receive information in general. However, it was a great way for me personally to frame up where I'm thinking the response should be for this incident and how we're going to use the departments and agencies to see if these are tenable options to discuss what comes next.

So it was extremely helpful, and it felt really cool to be writing one of these in the White House. But it definitely did not have the storybook ending where I thought, oh my god, this is amazing. Everyone, look at what Travis did. He wrote this amazing product. No, that did not happen, but it was still a pretty cool moment nonetheless.

CHRIS DAVIS: So it sounds like it was a learning opportunity in many ways.

TRAVIS BERENT: Oh, yeah, because I was able to frame my mind, organize my thoughts, write everything down in a way that I was trained at HES to do. And then when it came time to actually working on what their response will be, I had a good framing in my mind, and we were able to engage with our interagency partners to see if any of these options were feasible or tenable, and it definitely had positive outcomes in that regard.

CHRIS DAVIS: So if you don't mind my asking, what comes next? Do you see yourself longer term in the cybersecurity world?

TRAVIS BERENT: Yeah, I think so. I'm getting my degree in international relations, but when it comes to actually working in cybersecurity, that's almost the cost of admission is understanding geopolitics and the intentions of other countries and understanding just how the world order works. And just so much of it is almost required more and more as we look at the different threats that we're facing in the cybersecurity space, whether it's in a national security position or even in the private sector. Cyber threat intelligence is extremely valuable part of the role here.

And so many of these threats are coming from places outside of the US. So many of these adversaries have maybe agendas or intentions that are more aligned with the foreign policy goals of the adversaries that we're facing.

So I think no matter where I work, and I hope it will be in cybersecurity, and I plan to continue to serve the country hopefully at my home office, I do think that understanding the great game and the political implications of cyber incidents will only strengthen our ability to not only mitigate them but also establish effective deterrence so that we're able to move the needle on stopping some of these.

CHRIS DAVIS: Well, that's good to hear. And on that note, I know you're a busy guy, and I don't want to keep you so much. I want to say, Travis, thank you so much for joining us, for sharing your experiences, your observations, your insights. I know it'll be of interest to other students, incoming students, future students, so thank you so much.

TRAVIS BERENT: Yeah, no, of course. Definitely happy that you had me on.

CHRIS DAVIS: Thank you. Thank you so much.

[MUSIC PLAYING]

You have been listening to the *CARC Podcast,* a podcast of the Career and Academic Research Center. The views and opinions expressed in this podcast are those of the speaker and host and do not necessarily reflect the views or positions of any entities or organizations they represent.

[MUSIC PLAYING]