EPISODE 488

[INTRODUCTION]

[00:00:00] AH: Well, thanks so much for taking the time to speak to me. It's long overdue, and I've really been looking forward to it, not least, because I feel I've beared quite a bit of my soul to you with our various interviews, Dave. I'm looking forward to you bearing some of yours.

[00:00:15] DB: Yeah, I'm looking forward to joining you. Thanks for having me.

[00:00:18] AH: Absolutely. I wondered if you could just start off by telling us what you're up to at the moment. I know that you host a number of podcasts. Can you tell our SpyCast listeners about the things that you're involved in at the moment with CyberWire?

[00:00:33] DB: I'd say, the primary thing that I do here at CyberWire is host our daily podcast, which is a daily news briefing. It's about 20 minutes every day, Monday through Friday, which we like to describe as the essential news that folks who are cybersecurity professionals, or even enthusiasts need to know, to stay up to date on the latest goings on in cybersecurity. That's a combination of a newscast. Then, we have usually a couple of interviews as well on that show. That's Monday through Friday.

I do a couple of other shows. I do a weekly show called Hacking Humans, which is focused on social engineering. I do another weekly show called Caveat, which is co-hosted with Ben Yelin, from the University of Maryland Center for Health and Homeland Security. That's focused on Law and Policy. We do a show called Research Saturday, where I talk to a different researcher every weekend, to get the details on whatever cybersecurity research they're doing. Then, I also host The Recorded Future Podcast, which is focused on threat intelligence. It's probably not fair to say I'm the hardest working man in podcasting, but I certainly – I'm certainly making an effort, doing – Maybe what I lack in quality, I make up for in volume.

[00:01:51] AH: I lost count there. Is that half a dozen, or more?

[00:01:54] DB: 10 shows a week.

[00:01:56] AH: 10 shows a week. Wow. Okay. Total. Having a different podcast, so the 10 shows a week is five of the daily, plus another five?

[00:02:05] DB: Yeah. Let's see. We've got five of the daily. We've got Caveat, Hacking Humans, Research Saturday, Recorded future. Then I do a weekly guest spot on a show called Grumpy Old Geeks, which is someone else's show. I do a weekly security segment on there. That rounds out the 10 every week.

[00:02:22] AH: Are you a grumpy old geek?

[00:02:24] DB: I can be. I have my moments. I certainly qualify – There's no more denying that I fall into the old category. No massaging that. As my wife would say, depending on how well I've been fed, I can definitely be grumpy or not. There's plenty to be grumpy about in tech, no doubt about that.

[00:02:46] AH: How do you keep on top of everything? Because that's a lot of material to triage, and in such a fluid and dynamic field. I mean, is staying on top of it, just the fact that you're doing 10 shows a week, is that so in homework? Or do you have to do additional stuff to keep up to date with what's going on?

[00:03:06] DB: It's definitely a combination of both. Yes, keeping up with all of the shows and doing all of the prep work that's required for that, that keeps me on top of things. We have a great team at the CyberWire. Our editorial staff, they prepare a daily news briefing that goes out via email. That's an invaluable source for me and the rest of our team and everyone who subscribes to it, to keep up to date with that.

We also get hundreds of incoming story ideas and pitches every day from PR people, from companies, from individuals who are reminding us what's on the top of mind for them. The news, social media, I stay pretty active on the info security groups on Twitter, places like that. You're right, it's a lot to take in, and it does require a lot of time and energy to try to keep up. One thing about cyber is that it is never boring, and it is always changing.

[00:04:06] AH: That's true. How did you first get into all the cyber stuff? Is that your background? Or is that something you stumbled into, or a little bit of both?
[00:04:14] DB: It does go way back. I was one of those kids growing up, who would always take everything apart and put it back together again and hope that I didn't end up with a few extra parts, or screws, or things like that. I think, sometimes I drove my parents nuts. I get a toy, or a tape recorder, or something for Christmas or for my birthday. First thing I do is set off on it with a screwdriver.

I was lucky enough to take a computer summer camp when I was in middle school and this was back in the days of TRS 80s and Apple 2s. I was hooked. Just something that resonated with me right away. I saved up some money. Bought my own computer. Eventually bought a modem, when those were a thing. Started poking around on BBSs, Bulletin Board Systems. Dabbled a little bit with some phone phreaking and exploring the international network of phone connections. That was an area of exploration for me as well. I suspect the statute of limitations is long gone on my exploits there.

Went off to college. I actually came out of school as a radio television film major, and rode the first wave of desktop digital video with some colleagues of mine. We started a company, ran a video and multimedia company for 20 years. Left that company. Actually, got poached away from my own company, by one of my CyberWire colleagues, Peter Kilpe. Joined him and what they were doing. We eventually spun off the CyberWire as its own company. It was previously part of a cybersecurity company in Baltimore. We've been going for about five years from there.

My combination of tech, my comfort as a public speaker, all those kinds of things combined, made being a podcast host be the ideal job for me. It's really been a combination of things I've been working on all my life. I just lucked into this situation, where all of those various talents, skills and interests combined. It was seemed to be on to something.

[00:06:21] AH: For our listeners that aren't up to date with the techs in the cyber scene, can you help us understand the landscape of tech and cyber around the Baltimore Washington area? Because when people think of cyber and tech, they immediately go to the West Coast, to Silicon Valley. Or is there quite a scene around them, the DMV? Help our listeners.

[00:06:47] DB: Well, as I'm sure you are aware of being from the Spy Museum, there's this little agency down the road from us here, called the NSA. They are located at Fort Meade, which is practically a stone's throw from our offices here. Because NSA is here, and also, because we're very close to the federal government, that makes this a large epicenter for federal cyber concerns.

Not only are there all the government agencies, like NSA, the FBI, all of the agencies that are in DC, there's also a bunch of contractors who are built up around providing those agencies with the things that they need. Because of that, this area has become a tremendous zone for innovation in cyber. There are many, many startups here looking to pursue various products and service offerings, and so on.

There are those who say that this area, the Baltimore-Washington corridor is the Silicon Valley of the East. I'll leave that up to them to say that. There's no doubt that there's a lot of activity here, a lot of venture capital money, and a lot of really interesting things going on.

[00:08:02] AH: That's for sure. We have about a dozen of the NSA museums, their top artifacts at the moment, and our special pop-up exhibit. It's a really interesting corridor. You would say that, I don't want to push this analogy too far, but it's like East Coast and West Coast rap. They're both doing the same thing, but there's a slightly different history. There's a different vibe. There’s a different piece. Here, it's more federal. On the West Coast, it's more, yeah, what people traditionally think of, social media, and so forth.

[00:08:36] DB: Yeah, I think that's right. There are definitely some rivalries. We like to tease San Francisco. We call that the city by the other bay, because we have the Chesapeake Bay here. Yeah, there's definitely some of that, and we play into that. No doubt, there's strong cyber on both coasts, for sure.

[00:08:54] AH: Do you have a beef with anyone on the West Coast?

[00:08:58] DB: That's a good question. Not that I know of. I suspect, there are plenty of people who listen to our show out of spite, rather than pleasure. Hopefully, they're few and far between.

[00:09:08] AH: Just briefly staying on that, for CyberWire, for the various podcasts that you guys push out, or use more for – or use the go-to source for people that are looking at the more East Coast concerns, the federal staff, the NSA, all of the stuff concerning the government and the stuff around the government. The West Coast deals with something different. Are you also covering that material as well?

[00:09:32] DB: No. We're covering all of it. We have a global audience. Turns out, we're big in France, big in Canada, all over the world. We try to provide a daily summary of everything that you need to know about cyber. I'll give you an example of a use case. A chief security officer from one of the big cyber companies, actually, a Silicon Valley cyber company, say that he would listen to our show on the way in to work, so that when he went into his daily staff meeting, there were no surprises.

At the very least, he was aware of the things that were going to be talked about. He may still have to get details, but he wouldn't go into a meeting saying, “Oh, I haven't heard of that. What is that?” That's a very common use case for our show. We get a lot of students who listen, that have been recommended to our stuff to get up to speed quickly. By listening every day, you get more of a general awareness of the things that are going on, and a sense for what's important.

[00:10:33] AH: Can you tell us who that was? Or what company they were from?

[00:10:36] DB: I would rather not, just because I haven't cleared it with that person, and I don't want to betray any confidences.

[00:10:42] AH: Okay. Maybe you can tell me after we stop recording.

[00:10:45] DB: Absolutely. Yeah, sure.

[00:10:49] AH: One of the things that struck me, I know that here at the Spy Museum, there are definitely some things that I know a lot about, but there's a lot of things where I'm the equivalent of an internist. You can't be a specialist in everything. The realm of cyber is huge. Do you guys get some of that, where you have someone that they put a lot of stock in being the person that knows the I's and the T's about some very niche area, then they get back to saying, “Well, you never got that straight, or whatever.” How does CyberWire deal with that being an internist and then being a specialist trade-off?

[00:11:30] DB: Yeah. I mean, it's something that we deal with every day. Yeah. I mean, we have our own internal expertise. The folks, again, on our editorial team have a lot of experience on the civilian side, and also the military side of cyber. We have that expertise to draw on. Then, we also have a broad stable of experts who we can go to. We can pick up the phone and say, “Explain this to me. I don't understand what's going on here.”

I'll share that, I think, an important realization for me, and something that was a bit of a breakthrough, probably, I don't know, six or nine months after I started doing this, I had the realization that it's not my job to be the expert on all of this stuff. It's my job to talk to the experts about all of this stuff. It's my job to represent the person in our audience who wants to know more about this stuff.

I remind our team, it's not our job to demonstrate how smart we are. It's our job to help make our audience be smarter, by talking to people who are smarter than us. By shedding that ego of having to be the smartest person in the room, I think that's really been helpful both for me personally, and also, hopefully, for our audience that I can represent them by asking that silly question, asking that rookie question that surely, there's somebody out there who's asking that question. I bet, there are some people with higher levels of expertise, who roll their eyes when they hear me ask a silly question. I'd rather ask that question and have it answered, than leave it unanswered for the people out there who need to know.

[00:13:12] AH: What you're basically saying is that you've managed to get over yourself.

[00:13:16] DB: Yeah. I really have. I mean, Andrew, as you know, I mean, that's not easy, when you –

[00:13:22] AH: It’s not.

[00:13:23] DB: One of the things about doing a podcast, as opposed to say, live theater, or a live show, or anything where there's an audience is that there's no immediate feedback. You put something out there into the world and you hope that people enjoy it. You do get feedback. You get reviews on iTunes and things like that. You can see the numbers, and even the number of people who are downloading and hopefully, that heads in the right direction.

The flip side of that is as you know, if you make an error on the Internet, somebody is standing by to let you know, in no uncertain terms, the mistake you made. You have to have a thick skin when it comes to that thing as well. That's not easy for me. That's something I've had to adjust to. I tend to take things to heart. Having that realization has been very good for me. It's something I continue to struggle with. It's a good fight.

There are so many times when hubris has bit me in the butt over and over again, in just throughout my life and through my career. Those times when I start to take myself a little too seriously, inevitably, that comes back and I get – I learn a lesson. I learn a valuable lesson.

[00:14:35] AH: I think, for me, that's one of the things that I picked up a while ago when I was doing interviews for some research I was doing. Some people wanted me to go almost toe-to-toe with them. Then other people, I was quite happy just to part my ego to one side, and then just to try to elicit the information. If someone wanted me to go toe-to-toe, I was happy to do that. If someone needed to feel they were smarter than me, I was quite happy to let them do that. In many cases, they may well have been.

I was quite happy to be like, I used to call it just being Columbo, where I would just ask stupid questions. Actually, there was more going on underneath the hood than the person may realize. I was quite happy to subordinate myself just to get the information.

[00:15:26] DB: Yeah. I think as a host, that's an important skill is being able to sense what your guest needs, to sense where their comfort level is. If they need to be the expert, allow them to be that. If they want to be more conversational, to engage with them. You have to be able to dial that in. That's how you end up having a really comfortable, meaningful conversation.

[00:15:50] AH: Out of the various components of cyber, what are the things that you're personally most interested? What are the stories you cover, or the things that you do, that really get your juices flowing?

[00:16:02] DB: I like the psychological elements. I like the human elements. I think, that's why I'm attracted to the social engineering sides of things, the things we cover on our Hacking Human Show. Why people do what they do, the way that – How much the bad guys have refined their approaches to short-circuiting our senses, to getting us to do things against our best interests, the way they put the pressure on us and convince us to do things that we know better than to do. I find all of that fascinating.

I mean, to that end, also, the human side of the cyber defenders, that particularly as cybersecurity has grown more diverse, a diversity of thought leads to better outcomes. That when we started out, it was very homogenous, the types of people who are in this industry. As we've seen it grow, and where there more people coming into it and contributing, I think that is what leads to better outcomes.

To have contributions from people who think about things from a different point of view, that part fascinates me as well. That cyber is not just ones and zeroes, that human element. We are all humans, and we're using these machines. I think, that's the part that attracts me the most. I do love the tech stuff. I think it's interesting. The conversations I enjoy most, I think, are about that human element.

[00:17:27] AH: Give us an example of an episode of Hacking Humans, or a story that you've covered that would illustrate this point.

[00:17:33] DB: Well, I think, some of these heartbreaking scams that you see, where someone has been strung along. Let's talk about a romance scam. Someone who is lonely and vulnerable. Typically, you'll see a middle-aged woman, for example. Maybe she's divorced. She's feeling lonely, isolated. Someone will reach out on social media, and they'll have a picture of a handsome, dashing, usually a military man. Of course, it's a stock photo. Or, they've stolen the actual images from an actual military man. They'll reach out and they'll say, “Hi. I don't usually do this, but I saw your picture come by, and I just thought I'd reach out and say hello.”

They start a conversation and just meticulously, they go through and start pressing that person's buttons. Slowly over time, they build that person's confidence. It parallels a lot of the things that you all track at Spy Museum, of gaining the trust, espionage targets. Except for in this case, they are out to get that person's money. They'll say, “Oh, I really want to come see you, but I'm not financially able to do it. Could you send me some money for a plane ticket?” The person sends the money. At the end at the last minute, they cancel the trip and they say, “Oh, well. I look forward to seeing you soon.”

These poor folks get strung along. There are countless stories of people losing their life savings. Tens of thousands of dollars, hundreds of thousands of dollars. All because they went along with what they thought was the hope for love, or companionship. At the other end, it's really just a scammer, a heartless scammer who's out to get their money. There's a whole lot going on there. They're heartbreaking. Part of what we try to do is help inoculate people against those kinds of stories. The more you are aware of how they're done and the things to be aware of, so that those red flags can be raised. The little voice in your head can say, “Hold on. I've heard about this. This is a scam.” Hopefully, we can save some people from having to go through those sorts of things.

[00:19:44] AH: CyberWire is like the Moderna for cyber security, basically. Is that what you’re saying?

[00:19:51] DB: If only it were that easy. I have to say, I mean, it's something that does make me feel good about what we do is that we are trying to help people make the world a little bit safer. We get letters from people. People write in and say, “Thank you, because of what I heard on this show. Here's an example of someone who tried to scam me. I knew better. Thank you for what you do.” That feels good. It's very gratifying.

[00:20:15] AH: For our listeners that haven't listened to your shows, is there anything to feed? Are there high barriers to entry? Do you need to know all of the acronyms and all of the jargon? Help us understand how they can approach it and start to learn about this stuff.

[00:20:29] DB: This is approachable as possible. Like I said earlier, many of our listeners are students. Something that I remind our editorial team is that it's okay to have things in the show that people who have a higher level of understanding will benefit from, or will feel included by knowing that thing. We never want to be exclusive. We never want someone to feel left out, because they don't understand what something is.

As much as possible, as much as time permits, we try to just briefly explain what we're talking about, or put things into context. That said, the CyberWire Daily Podcast is a bit more focused on professionals. There is more jargon in there. That show is so concise, that it's harder for us to take as much time to explain things. Some of our weekly shows, like Hacking Humans in particular, and also Caveat, those are more focused, or targeting more a general consumer audience. There's more explaining that goes on there. We've gotten feedback that those audiences are made up more of people who are just interested in the stories, and not so much cybersecurity professionals themselves.

[00:21:45] AH: You mentioned espionage not long ago. I want to get a sense of with what you guys are doing. Where does the world of intelligence and espionage – where does it stop in terms of what you're doing? Because there's obviously, quite strong overlaps, and there's a struggle that's going on out there between malevolent forces and benevolent forces and states and individuals and institutions. Help us understand, how much of an overlap? Is that 50% of what you're covering? Or is it 10%? Or is it 90%? Give us a sense of that.

[00:22:23] DB: Like you say, there's so much overlap now. I mean, it's funny. I was thinking, as I was prepping for our conversation today, and I was trying to put some things into context with many of the things that I know you all are interested in and cover there at the Spy Museum, imagine if you could go back to the 1950s and tell some officer who is interested in espionage, that in the future, everyone would be carrying around a device on their body that tracked their location with extreme precision. Not only did it track their location, but it also tracked everything they purchased. It kept track of who they were nearby, their goings, their comings, their conversations, their photographs, their relationships, their intimate moments, everything on this one device that is with them almost all the time.

When they don't have it with them, it's on their nightstand while they sleep. If you told that to someone back, then they would say, "Are you crazy? Why would anyone do that?" Yet, here we are, and we all do that. That collection of our data, I think, is fascinating from an espionage point of view.

We've heard the stories where the espionage agencies, they don't necessarily have to put a tail on someone. They can put a request in with the service providers and say, “Tell us every cellphone tower this person hit,” and have a good idea of where someone was traveling. I think, that changes the game when it comes to espionage, don't you think?

[00:23:59] AH: Yeah, absolutely. I mean, I think, that there's a brave, scary new world that we're still marching into, and we don't quite know the ramifications. I think, the institutions and the other things that we take for granted, they're increasingly struggling to keep up with exponential technological change, right?

[00:24:20] DB: Yeah. I think, that's exactly right. One of the things I wonder about is, are the foundations on which our societies are built. For example, here in the US, our constitution, our systems of government. Are they properly equipped to deal with the velocity of online life? How much more quickly everything happens? I think, many would say, one of the features of our system is that it is slow and plodding, that it's hard to get things through and that's good. At the same time, does that make it difficult to react to things that are changing so quickly in cyber, in social media, in our online connected lives, are we left being in a constant state of being reactive to things, rather than being able to get in front of things? That's something I think about quite a lot.

[00:25:14] AH: You mentioned a thought experiment. Imagine a spy from the Cold War and telling them about the modern iPhone, or the Android. I mean, can you imagine telling the founders about the type of world their descendants would be living in? I mean, the constitution is yeah. I don't know. It's from a particular place in time. It obviously stood the test of time. There are these changes that are going on, though, that are very difficult to deal with.

[00:25:44] DB: The context is important, I think. These are people who as progressive as they were, as brilliant as they were, and careful as they were in putting together the foundations of this experiment, that is the United States of America. These are also people who did not have indoor plumbing. They went from point A to point B on horseback. They did not have antibiotics. All of these things of modern life that we take for granted, they did not enjoy.

It's valuable to try to put some of the decisions they made in that context. Could they imagine communications happening at the pace that they do? When word had to come from overseas, and it would take six weeks for a letter to come by ship from Europe. Now, you and I are speaking instantaneously. We could be on opposite sides of the world, and it wouldn't be any burden to our communication.

I guess, what I'm saying is that the work that they put into those founding documents, could they have imagined the place where we are right now? To their credit, they put in – To some degree, they knew this. That's why we can have things, like amendments. Again, it's not easy. Those things happen slowly. I guess, that is both a bug and a feature.

[00:27:07] AH: The next couple of questions, I want to leverage some of your expertise for SpyCast listeners. I guess, the first one is, what book, or books would you recommend people read to get up to speed with cyber? What are some of the things that have really had a lasting effect on you?

[00:27:25] DB: One of my favorite books of all time, not just with tech, but it just in general, it's a book called *Hackers: Heroes of the Computer Revolution*, I believe, is this subtext. It's written by Steven Levy, who's a well-known author and journalist. It really chronicles the early years of tech, the Steve Wozniaks of the world, the Steve Jobs of the world, the foundation of these companies, how they got their start.

Not only is it a real page turner, but it gives you a good idea of where we came from. Because many of the things that are happening now came from decisions that were made, either intentionally, or just the way things worked out back then. From a history point of view, I think, that's a really interesting book.

There are lots of books available today. I get new books, practically, every day, from folks who want us to interview their authors on our shows. *Countdown to Zero Day* is a good book. Thomas Reid's books are quite good. *A Sandworm* book is quite good. *Cuckoo's Egg*, I can't remember. There's quite a few of them. I wish, I had more time to read them than I do. Those are just a couple that I've enjoyed.

[00:28:42] AH: If you're hosting half a dozen podcasts, your time is rather limited. Well, the next question was, say someone who can give you advice about health and they say, make sure that you exercise three times a week, make sure you eat vegetables, try to get an eight-hour sleep, etc. Someone that knows about how to look after yourself. Help our listeners understand about how to look after themselves digitally in a cyber sense. Are there particular things that you do? Do you have a routine? Do you always use a VPN? Do you always use **[inaudible 00:29:21]**? Do you use particular browsers, particular emails? Help us understand how you keep healthy digitally and your own life.

The bits of advice that I will share with our listeners that will get you most of the way there in terms of your cybersecurity, two main things. First of all, use a password manager. There are many of them out there. LastPass 1Password. There are open source ones, there are free ones. Use a password manager. What a password manager does for you, is it makes it so that number one, you don't know what your passwords are, because now you can start using random strings of characters for your passwords. A good password manager will remind you and badger you, when it sees that you're using the same password for multiple sites. You should never ever, ever use the same password for multiple sites. By using a password manager, that's an easy way to get around doing that.

In fact, I think, the only password that I have memorized is the master password for my password manager. That leads us to the second thing, which is to use multi-factor authentication. A username and a password for anything that's important to you is simply not enough. You should have multi-factor authentication. That can be an SMS message that gets sent to you, when you log in somewhere from a new computer, or a new location. Many people will rightly point out that an SMS isn't the most secure way to send you a message. That is absolutely right. It is way better than nothing at all.

Other ways are there are password generators you can get for your devices. Most of the password manager companies have their own. Google has one. There are many of them out there. Then also, security tokens, security keys, like a YubiKey, that sort of thing. That is highly secure as well. For things like your bank account, any account that's dealing with money, your credit cards, again, if it's important to you, it deserves to have more than just a username and password. The data proves this. The reports that Google has put out, say that if you're using multi-factor authentication on an account, it almost never gets compromised.

Also, I'll point out that one of your most important accounts, if not the most important account is your email account. Because that's where everything else flows through. When people are trying to do password resets on some of your other accounts, let's say, I'm trying to reset the – I'm a bad guy, and I'm trying to reset the password on your bank account. Well, that's going to flow through your email account. If I have control of your email account, and I trigger a password reset, I'm going to get that email. I'm going to say, "Yes, this is Andrew, and I would absolutely like you to change my password." Don't think your email isn't important. You absolutely should have multi-factor on your email as well.

Just doing those few little things will get you most of the way there. I understand, it is really hard. Almost everybody reuses passwords, but you just got to break yourself of the habit. You have to approach it in a different way. Also, you're not nearly as clever as you think you are. If you're using the same password and appending a couple of letters to it, or a couple of numbers to it, believe me, the bad guys are on to you. Those little, simple patterns are not going to stop anyone from figuring out how to get into your stuff.

[00:33:01] AH: For browsing the Internet and so forth, what would you advise there? Do you always use Tor? Do you always use a VPN? Do you use a particular browser?

[00:33:12] DB: I don't. I like to use the Brave browser, which is a privacy-focused browser. I use iOS devices, so I use Safari there. I think, that's enough. If I were doing something where security was important, or if I was in a place where I thought perhaps, there was a heightened risk, I would use a VPN. For example, I would never use public Wi Fi. Let's say, I'm in an airport or something, that's a place where I would use a VPN.

At home, at work where I have a pretty good idea what's going on here, I generally don't feel the need to use a VPN. Again, using a privacy-focused browser seems to be enough for me. I think, you can go overboard with this stuff. An important part of it is understanding what your risk profile is. The flip side of that is you should not think that no one is interested in your stuff, because someone is interested in your stuff.

Your stuff has value. Even your name, address, phone number, social security number, your basic information, somebody can sell that, even if it's for 10 cents. If they gather up enough of them, we're talking real money. Don't think that you're not interesting. At the same time, most people who are at risk are aware of that and either know themselves, or they have a team who helps them address the particular risks that they may face.

I think, it's like general hygiene. You wash your hands. Try not to cough on anybody else. You cover your mouth when you cough, all those sorts of things. You shower and bathe regularly. Try to eat right, stay relatively healthy. That gets you most of the way there. Is it foolproof? No. Nothing is foolproof to a talented fool. Just doing the basics. I don't think you have to go overboard.

[00:34:56] AH: You spoke about the bad guys there. I just wondered if we could focus on that briefly, because out there for the people that are not, again up on cyber, to hear of black hats, white hats, lots of different terminology. I just wondered if you could tell our listeners a little bit more about that. Who are the bad guys out there? Are we talking about states with these forums of hackers? Are we talking about very sophisticated, organized crime? Or are we just talking about the cyber equivalent of the person who goes to the gas store with the barn tillers tattoo and pulls out a gun in front of the camera and says, "Give me your money?" What are the people that are out there, that our listeners need to think about?

[00:35:47] DB: There is a whole spectrum of actors out there who engage at all those different levels. It really does parallel traditional crime. You do have low level actors, and they can be out there, everything from folks who are crypto mining, which is you're using your computer. They'll get unauthorized access to your computer, and they'll just use your computer's processing power to mine cryptocurrencies, things like Bitcoin, or Ethereum. You may not even be aware that they're there, but they're using your computer, they're using your electricity to do the things they do. They try to fly under the radar, because they don't want to be detected. They want to be able to use your system and have you not notice. Some of them will even just operate at night, or they'll sense when you're not using the computer, and that's when they'll do their thing.

Then, you get into ransomware operators. You get the low-level ransomware operators, which is a ransomware started. Those are folks who will get access to your computer, and they will lock it down and then start encrypting things. They'll say to you, “If you want your stuff back, give me a 100 bucks, or give me 500 bucks, or something like that.” Ransomware is grown much more sophisticated. There are folks out there who are targeting businesses with laser precision, and demanding millions of dollars and getting it.

Those folks do their homework, both from a technical point of view and studying the companies that they're going after, to make sure that they have the resources that they're after. That's more like, organized crime.

Then you get up to the nation states, that's where they're primarily interested in espionage. There are some exceptions to that. The North Koreans, for example, because of their own unique situation of being shut out from the rest of the world, they do actually need to generate revenue based on their state sponsored cybercrime. They do. Most of the other nation states, the Russians, the Chinese, they're mostly interested in espionage.

You have situations, for example, with the Russians, where you may have some of their actors who are moonlighting. They're off the clock. They're doing things like ransomware. The government looks the other way. This was one of the topics when President Biden met with President Putin recently, to say – Biden said to Putin, you got to knock this off. You can't keep turning a blind eye to this stuff. This is serious. We had the shutdown of a pipeline here in the US, because of a cyber-attack. That's serious stuff. We're getting to the point where we can say, there has been loss of life.

I saw some folks comment that the conversations we're having about cyber, at the nation state level, are conversations that we used to have about things like nuclear weapons, that it's been elevated to that level. We're talking about critical infrastructure and so forth. Yeah, there's all sorts of folks from the highest level nation state actors, down to the smash and grab criminals who are trying to skim from credit card machines and ATMs and everything in between.

[00:38:52] AH: For the organized crime, who are some of the stories that you guys may have covered? Who are the types of people that we're talking about here? Are we talking about traditional mafia? Are we talking about something else? How do they recruit? Where do they get this skill set from? I guess, just to be slightly flippant for a second. For many of our listeners that know some of the stuff that are popular culture, it's difficult for them to imagine someone with a tracksuit and they wear sleeveless vest, then a meatball parm sandwich in one hand and setting, hacking on the other. Is there a particular skill set that goes along with that?

[00:39:32] DB: There is. To talk about the organized crime component of this, one of the things that we've seen, for example, is ransomware as a service. There are organizations out there, where if you don't have the technical capabilities, you can hire someone who does. they have an affiliate model. It’s like opening your own McDonald's. You have a franchise, but the McDonald's mothership provides you everything you need, all the equipment you need, all of the branding you need. They'll send you leads. You can purchase all of that stuff, run your own criminal organization, but all of the technical side of it, you're jobbing out. You're paying someone else to do that. That could be the criminal masterminds.
In exchange for that, they get a cut of everything you take. They've got this broad, high-level business model, where they're making more money that way, and I suppose, less effort, than if they were out doing it themselves. It's also interesting to ponder, does that put them at more, or less risk for running afoul of law enforcement? It's hard to say, but I think that's a component of it as well. I'm not actually the one out there stealing things. I'm the one providing the tools for the people who steal things.

They find each other on dark web forums. There are hacker underground forums, where these people meet and exchange information and trade their wares. Of course, cryptocurrency has made so much of this possible, because that's the way that the money gets sent around internationally, as a way to send money around that’s separate from the banking system, the global banking system. There's been a lot of call from folks saying that we need to put better controls on that, because that's been a real enabler for these folks, to be able to pay for things.

[00:41:27] AH: Can you give us an example? What would be an example of one of these motherships that sends out hired guns to other organizations? Is there one that you have covered on any of your shows that our listeners could maybe Google and find out a little bit more about? When you were talking, it almost reminded me of some of the organizations and the James Bond novels and movies, where you have a non-state, almost enterprise that is happy to hire out their services to bad guys.

[00:42:02] DB: Here's a good example from recent news. We had the colonial pipeline shutdown here in the US. That was identified by the US FBI as being the responsibility of the Dark Side ransomware group. It's an organization called Dark Side. Yes, it is a very James Bond-sounding organization. These groups love to – Well, either the groups, or the people who study them give them interesting names. That's a whole another conversation. In cybersecurity, we can't seem to settle on one name for any organization.

However, the Dark Side group was an affiliate – They had an affiliate program. What's interesting about the colonial pipeline incident is that it seems as though, it was one of their affiliates who hit colonial pipeline, perhaps unintentionally. They were out just seeing who they could hit and doesn't seem like they were targeting the pipelines specifically. It was not their intention to shut down critical infrastructure.

They were just looking for businesses with money. They happened upon colonial pipeline. Took down almost half of the fuel supply to the east coast of the United States for a few days. People who run Dark Side started backpedaling and saying, "Oh, okay. Ha, ha. Well, this was one of our affiliates. We did not intend to do this. Here are the keys to unlock everything." It seems as though, they sensed that they had gone a little too far, and that their affiliate had gone too far. That this could bring undue attention on them from the powers that be, which it absolutely did. To have our president talking to their president about this specific incident, and saying, "Knock it off," that turns the heat on. That's not what they want.

There's stories and speculation that the Dark Side folks shut down that affiliate. Sometimes, what you'll see happen is when the heat gets put on these organizations, they'll shut down for a little while. They'll rename themselves. They'll rebrand themselves and come back under a different name to try to let the heat blow over. That's probably the most well-known recent example of an organization running under an affiliate program and how inadvertently, it caused harm and also, brought the heat on them.

[00:44:29] AH: Just to track that down a little bit more and give it a human face, where are we talking here is Dark Side, are they based in Russia? Are they a group of people? Are they affiliated with the state? Or is it a Russian mafia that hire a bunch of people out of college to do certain things? Yeah, how does it all shake out?

[00:44:51] DB: Yes. Dark Side is suspected to be Russian. Most of these organized crime style, the ones who are after money, the vast majority of them are Russian organized ones. The high-functioning, highly skilled ones. Russia seems to be where they come out of. Again, the Russian government turns a blind eye on them, as long as they don't go after Russians.

One of the interesting things about that is you'll see in many of these ransomware packages, for example, it will check to see if your computer's primary language is Russian. It will check to see if you're using a Cyrillic keyboard. If you are, yeah, if you are, it leaves you alone. It moves on, because they don't want to mess with the homeland. That's how they get the hammer brought down on them.

In this case, yes, almost certainly, Russia. Again, it's hard to know how many of these people are folks who are working for the state, and are moonlighting, doing jobs on the side. How many of them for which this is their primary job? Do they sometimes help the government when the government needs help with things? There's a lot of crossover with the Russians, in particular. It's pretty fuzzy as to who is sponsored – who is state sponsored, who is state tolerated, that sort of thing.

[00:46:19] AH: That sounds a little bit like, when you're talking about Biden's conversation with Putin. It's a little bit like, drug cartels. They realize that there's no mileage and killing an FBI agent, or a DEA agent. They're left off limits. If they do, then they know the heats coming on them. I mean, for some listeners, they will be thinking, I mean, does Russia even have a sense of what's too far? Why would this be considered too far, given some of the other things that they're up to?

[00:46:49] DB: Well, I think the too far is that it attracts the attention of the highest levels of the US government. That could bring down things like sanctions and non-cyber responses. The code for that is a kinetic response, which is guns and missiles. That's happened. There was the incident, where the Israelis took out a building that was hosting folks who they felt were coming after them from a cyber point of view. There's the whole Stuxnet thing, where the legend is, and the pretty strongly supported story is that we took out the Iranian centrifuges using malware, so they couldn't enrich uranium.

When you get to the point where your adversaries are going beyond cyber to respond to the things you're doing in the cyber domain, that gets the attention of the highest levels of your own government. That is not the attention you want as, even an organized criminal. You want to just be able to do your thing, not cause any trouble, make your money, tip the appropriate people you have to tip to get them to leave you alone and go about your business. As with the colonial pipeline incident, I think inadvertently, they went somewhere they didn't intend to go and it went too far, and the hammer came down.

[00:48:15] AH: Just a couple of final questions to wrap up, Dave, one of them was, with you guys at CyberWire doing the “Lord's work.” Do you use over the focus of any of these malevolent actors out there who are thinking, they're out there evangelizing and keeping people safe? We're going to bring them down a peg or two. I mean, are these discussions that US have internally? Or are you just part of that game as well, user civilians, and you don't go after them? Help us understand that.

[00:48:47] DB: It is a conversation that we have had. It is something that's on our radar, that we could put a bull's eye on our backs by reporting on things. We try to be fair. We try to be as accurate as possible. We don't deal in gossip, or speculation, or innuendo as much as possible. I think, that keeps those folks away from us.

Sure, it's a concern. We take appropriate security measures here to try to keep ourselves safe and prevent them from coming at us. At the same time, I don't think we should take ourselves too seriously, that we would be a specific target, or I don't want to be paranoid, or have any undue worry about that. It's definitely something that we think about. It's part of the planning that we do to keep ourselves safe here.

[00:49:41] AH: Having listened to your show, it's quite a matter of factual. It's not strongly editorialized, one way or another. Yeah, it's not sensational. It's more just, here's information that you need to operate in the world.

[00:49:55] DB: Yeah. We try to be respectful of people's time. That is more and more, I'm coming to believe, that's the most valuable resource, because nobody's making more of it. We'll try to give people what they need in a very concise way.

[00:50:11] AH: Final question. Just when you were talking there, it made me think about international relations has been amongst great powers, it's been a carefully choreographed performance, where there are certain rules, and you do this, and we do that, and involving espionage, or the military. With cyber, it's like, the old drill book has been wrapped up. I'm sure, there are some listeners to SpyCast who are thinking, "What in hell are the Russians doing that this is going to provoke a war, interfering in the US election, shutting down a pipeline on the East Coast." I mean, you could set off a chain of events that could easily escalate out of control. In the past, that may have had certain consequences.

When you're talking about nuclear armed great powers that are engaged across the world, I mean, the stakes are really high. What's your read on the rules of that game, as it's been played out, or the lack of rules?

[00:51:14] DB: I think you're right on. I think, the thing about cyber is that there's a lack of proportionality there. In other words, if I want to exert my power in the real world, building an aircraft carrier is a great way to do that, because I can take my military anywhere I want it to be, and I can exert my force remotely. To do that in the cyber realm, I don't need to build an aircraft carrier. I don't need to have the resources, the know how, the engineering, the time, the money, all those sorts of things to build an aircraft carrier. Don't need any of that.

Smaller countries have access to the same sorts of tools. Since we have connected the entire world via the Internet, they have access to all the same systems. That's how a poor country, like North Korea can be so active in cybercrime. It's how a country like Russia, who if you look at Russia's GDP compared to other nations of the world, they're small, but they have an outsized influence when it comes to cyber. Let's not discount the fact that, yes, they have nuclear weapons, and so they're a military force to be reckoned with as well.

In the cyber realm, I think, the big change, as you say, is that it's disproportional. It doesn't take a huge investment to stand up a capable cyber team that's able to have influence and power around the world. I think, we've yet to see what the capabilities of some nation states are. I think, the United States has been very effective in limiting the view of what our true cyber capabilities are.

Could we turn the lights off in another nation if we wanted to? I suspect we probably could. I suspect for many reasons, we choose not to do that. One of them is that we don't want the other folks to know what our capabilities are. To not have them revealed is a type of power all in itself. Yeah, I think it's a different world. I think, we are slowly but surely adjusting to that world. I think, as we see the next generation come up and take their place in our governments, in our societies, the people for whom these things are reflexive, the digital natives, hopefully, will see a better understanding. We'll see how society changes because of it, with people who come up with different attitudes towards things like privacy and collaboration and communication. It's all going to be different. It's going to be different than it is for folks like you and me, right?

[00:54:01] AH: Absolutely. Well, thanks so much for your time. I feel like, I could speak to you for hours. Yeah, time is the most important commodity. Let's wrap it up there.

[END]