Transcript

DAVID LEDGERWOOD: Chris, it's great to you have on, man. Thanks for joining us.

CHRIS SHORT: Thank you. I appreciate you having me.

LEDGE: Can you give just a little background story of yourself and your work just so the audience can get to know you a little bit?

CHRIS: Sure! Currently, my job is part of marketing for the Ansible team at Red Hat but like any job I've ever had, there's so much more to it than just marketing.

I started out in tech working at a textile manufacturing in the mid-nineties. I remember seeing the big coaxial cables that used to run the network at that company.

So bringing them aboard, I used to run ISP. I used to dial up ISP in North Carolina. Then I joined the Air Force and did big networks for the Air Force, deployed for OIF, came back home, got hurt doing a field exercise after getting back from Iraq so that was super awesome.

I got medically discharged in 2010 and I've kind of been in the WebOps and DevOps space ever since 2011.

I have a broad spectrum of events and history to pull from — from communications, some work in the intelligence field, and then deployed overseas type work all within kind of the IT realm the whole time. So it's been a super interesting dichotomy going back and forth between public and private sectors.

Personally, I'm super excited about Ansible operators specifically taking Ansible code and using it as operators in Kubernetes or OpenShift as opposed to having it. So it's a super cool thing that that we're working on collaboratively as Red Hat does.

LEDGE: Absolutely! Before we get too far, I want to make sure everybody knows about your newsletter because that's actually how I —

CHRIS: I write the newsletter DevOps'ish. It's a weekly newsletter covering DevOps, cloud native technologies, and open-source software.

LEDGE: Make sure you sign up for that. There's super broad coverage there. Off-mike, you and I got to talking a little bit about how current research topics. You have to read everything when you write a newsletter like that. It's really interesting.

You had some thoughts on the emergence of China from that technology and DevOps and business perspective. You had some things to say that I haven't heard a lot about.

CHRIS: I think there are a lot of stories in the media right now and you're seeing it from both sides because I read a lot of Chinese news sources and I read about American news sources. I read a lot of other news sources as well.

Especially in the last couple of weeks, I've seen a lot from both sides, the U.S. side and the Chinese side talking about Huawei — that offensive Huawei and, from the Chinese, the kind of public criminalization of Huawei the U.S. government is trying to do.

It all ties back to, essentially, intelligence services and some of the work I've done with that. It's interesting in the light of Huawei We can kind of talk about some of these things that we wouldn't have even known about as society until recently.

The U.S. and the Chinese have intelligence services. Those intelligence services surveille the Internet. Obviously, the Chinese government has the Great Firewall of China and that's how they manage their Internet access. It's very restrictive.

A U.S. company can't just walk into China and do an Internet connection and start up a service.

They have walls in place. The Chinese government has walls in place that only Chinese companies can certify to work on their telecom industries which are typically government-owned companies. They have a license to operate and there are all these regulatory

requirements to get that; and there's only a handful of U.S. companies or international companies, in general, that have a license to operate in China.

They usually have to participate with a subsidiary of a Chinese company to actually get access to the Internet for the services they're trying to provide inside China.

So somebody like Cloudfare, a few years ago, did a great blogpost about all the hoops they had to jump through technologically, legally, contractually, the whole nine yards, just to get a point presence in China.

And keep in mind that the Internet in China is a very different Internet than it is in the U.S.: a) It's Chinese based; b) Because of it's kind of separation from the rest of the Internet, they have services that are similar to Twitter or whatever, Facebook, the whole nine yards. They have comparative services on the Chinese side of things that are 100% run and owned by the Chinese company that maintains them.

So Twitter use in China is very minimal. LinkedIn use is pretty good. I have no idea about Facebook use is in China. I'm sure Twitter and Facebook are trying to break into the Chinese market because of the massive population and growth of Internet users there. It only makes sense.

Just to give you an idea of the kind of landscape, it's not like operating anywhere else in the northern hemisphere or Australia. Some countries in Africa, New Zealand, typically, they're pretty easy to work with. China is a whole another regulatory ballgame.

So the U.S. government argues that Huawei is owned and run by the Chinese government and there's some truth to that; there's some falsehoods to that to an extent like what percentage is unknown; whether it's wholly a subsidiary of the Chinese government is unknown. But even Huawei is like, "No, we're not."

And they've admitted to some percentage — I forget what the current number is — of ownership by companies that are owned by the Chinese government.

So it's a lot of sleight of hand behind the scenes; it's a lot of jostling politically for essentially who makes the stuff that runs the Internet.

Now, we've already kind of seen that China has the separate Internet but what they're trying to do now is the New Silk Road; I think it's called "Belt and Road." They have a **bigger** name for it in China. But it's essentially creating this Pacific to Europe trade zone that's Chinese influence. It will be natural gas, oil — two way kind of sales and trade.

Belt and road is designed to bring China into the full-blown industrialized modern era.

So what's that doing is putting pressure on Huawei and other companies in China to expand just like, we, being the rest of everybody not China, have been pressuring ourselves to get into China. So it's a two-way street.

The main concern from the U.S. government's part is they can't verify what every chip does in a Huawei device. They don't know. The device complexity has gotten so bad that it would take forever to do this.

We've been doing this since forever. We did it with the Soviets. If we could get our hands on some Soviet technology, we would take it apart and figure it out and, eventually, a couple of years later, we would have it in ours and all is well.

Same thing with the Chinese — if they can get a hold of something of ourselves — and the U.S. has accused them quite a bit of international property theft; and there are some facts behind that as well.

It's always like this. It's always going to be like this. But in our lifetime, we've never seen this new number one rising up. The last time this happened — yes, the Cold War could kind of count like two people or two countries or two groups of people jockeying for number one in the global stage. But, statistically, the USSR didn't compete very well with the U.S. economically.

China, by a lot of economic indicators, has already outstripped the U.S. There is some bible somewhere that says that the U.S. must be number one. China has rewritten that bible. They are taking the world stage by storm and saying, "Yes, you've done this this way and this has worked well for you but we'd like to try things a different way."

And they have the size and the weight and the growth and the influence in the world now where it's causing some concerns between old-school allies from World War II. The U.S. and the U.K., the Australians are right there in China's backyard and they're trying to figure out "Where did they fall? Do they want to buy Huawei equipment? Do they not?"

And then, when you look at 5G and AI and how influential that will be in the future, building these 5G networks and then being able to tap into them is highly savory to intelligence services, right?

What the U.S. does and what its allies do is the U.S. doesn't spy on its own citizens unless it has this very rigorous checklist of things that actually happens. What ends up happening is

the U.S. says, "Hey, U.K., can you spy on our people for us?" and U.K. says the same thing: "Can you spy on our people for us?"

This actually goes way back to the Five Eyes days of World War II. This established relationship has been around since, I think, the seventies as far as that. And the only reason that that law existed actually came about because, I think, of the some of the Watergate stuff.

It used to be totally carte blanche. You didn't know.

For the longest time, intelligence agencies — there are seventeen of them that are publicly known right now. I used to work for one of those agencies which wasn't publicly known in the public until the 1990s when Clinton accidentally said the three letters on national television during a presidential address.

So, all of a sudden, you have this whole industry of people saying, "Hey, no one knew about us." Now, they were publicly exposed in the nineties.

Oops, it happens.

This is has always been boiling around in the background and there's a lot unpacked. Feel free to just kind of dive into any one of those things.

LEDGE: Yes. Obviously, you could talk for days and it's just incredibly interesting — the dance back and forth and the stories about the imports, exports, and what have you.

I guess, AI is an interesting space there and the developments around advanced software technologies.

Being on the open-source front, what are the implications there?

You sort of have this ability for anyone to contribute and to sort of manipulate those products. What do you, guys, think about —

CHRIS: From the Red Hat perspective, I have no comment. Personally, I have thoughts about how AI will come about. Just like the Facetime bug that was discovered a few weeks ago. It was discovered by some high school kid in Arizona, I think, who just happened to stumble across it and was able to replicate it.

Honestly, I think that's how the next domino that needs to fall for AI to really kind of take off. That's kind of how it's going to be discovered. It's going to be somebody hacking away at something in their basements somewhere.

Now, whether that basement is in Shenzhen or in Durham, North Carolina, that kind of matters because if it's open to everyone on the planet which would probably be the case in the U.S. if this person was like an open-source developer, for example, that's good for everyone.

But if, all of a sudden, someone in the basement in Shenzhen discovers the next domino for AI, they're going to be well known very quickly because of the surveillance apparatus that exists in China. And then, the Chinese will, obviously, adapt that technology however they see fit and maybe not share it with the rest of the world.

And then, all of a sudden, we have this regime with a history that concerns some countries kind of in charge of everything because of their technological advantage. That concerns some policy makers in the U.S.

LEDGE: As we can understand, exactly! I mean, AI is going to become so ubiquitous. It's already built into consumer devices all over the place. These are narrow applications. We can debate all day long as to when the singularity in general AI is going to come around.

But there are, certainly, meaningful industrial and business applications that are getting quite robust and just the ability to process this endless amount of data to come out with some kind of decision making complex, this could be used for ill or for good, right?

I guess, that's the question.

CHRIS: It's not even that. It's never just one thing with the US-Chinese relationship. It's always a multitude of things and it's never just US-China. They're all interconnected now. There are all these other players that are in the mix as well.

So when the U.S. is mad at Huawei and they accuse Huawei of stealing intellectual property, the real crux of the argument is while all these U.S. companies had to spend this time, effort, and energy to patent this intellectual property that they've built their business around, China, possibly, went in and just stole it overnight, one day; and now they're

building the same product at a much lower cost because they had zero R&D budget and they didn't need it, to begin with, anyway.

Their R&D budget was a thousand dollars and the next. And that's all it took for them to get to intellectual property that they can bake into anything now for any of their businesses. And they have a competitive advantage already just from that right there.

So that's kind of the U.S. story on that side.

Now, what's going to be interesting is, as China falls will we start doing the same thing as China?

Obviously, our defensive policy within the U.S. regarding Internet infrastructure has changed under the current administration. "Defend forward" is the current kind of strategy whereas "Don't let the attackers come to your door. Maybe go find the attacker's door and close it before they can use it" kind of thing —

So "defend forward" is kind of what they're saying as the technology strategy or defense strategy now for "cyberspace," as government calls it.

Cyber security is changing everyday.

And that's just like AI like quantum computing and all these things —

LEDGE: All that converge in a short period of time — certainly, less than ten years, if not, less than five where you have a convergence of all these very powerful technologies.

Quantum encryption — people are experimenting with quantum communication now and the networking technology is leaps and bounds —

CHRIS: I read something the other day that some Chinese military industrial company figured out a way to create quantum radar in a very small size. But, basically, that's how they create radar like one bounces and the other doesn't but they disconnect. That's how it knows. Only one came back; the other didn't kind of thing.

The Chinese figured out that this bond the exist between these two molecular objects, the radio wave, can be stretched like long distances. So you could literally figure out of

something stealth is out there because this bond now is broken because something broke this molecular connection between radio waves. It's super crazy to think.

LEDGE: There are so many applications — that's amazing!

CHRIS: Oh my God, it's terrifying, right?

LEDGE: And you get down to "Do I want the bad guys to have that? Wait a second, am I the bad guy?"

CHRIS: The U.S. government thinks it's the good guy.

LEDGE: Absolutely! And it comes down to "How will two number ones get along in a technologically advanced society?"

We can go on forever. Let's break it down to one or two takeaways.

You're consuming so much information from the entire industry and you're just out there thinking, talking, and writing about so much. Maybe a couple of trends that engineering audience must pay attention to in the next twelve months.

CHRIS: For twelve months, pay attention to the system back inside Kubernetes but how to make Kubernetes easier 0:18:05.2.

Kubernetes is not the end goal. Kubernetes should just fade in the background like the CPU although, thank you, Spectre and side-channel text is now back in the forefront.

You don't really think about where our CPU came from unless we're really talking about some particular application or a specific thing. We only care about megahertz or what class.

Kubernetes used to get to the level where people just assume it's there or the APIs are just there and they function well and they're stable and easily deployed and managed.

After that, you really kind of need to look at if you're not writing stuff and go and rust as an engineer, you kind of have to ask yourself "Why?"

I think we've seen enough stable Go code running at scale out on the Internet at this point but there's really kind of —

Yes, Java is the predominant language out there right now but there's kind of no reason why Go can't fill a lot of those voids that Java is filling right now and, usually, in a much more efficient manner.

For a third thing, I've come to the conclusion that there's no way to separate tech from everything else in the world.

In my newsletter, I dive into topics of politics and diversity and inclusion and all these things because the world is so interconnected now. You can't have your politics over here and your tech over here. The two touch now. And you need to learn to operate in that space.

LEDGE: Big thinking stuff, man. I love that.

CHRIS: It's not to say that it's the right thing. This is the reality of the world.

LEDGE: I take away the lesson to consume as much as you can and try to draw lines because you just need to put them all together and you can't be a single discipline professional anymore. You won't get anywhere.

CHRIS: If you're the best widget maker in town, prepare to have somebody come to out-widget you.

LEDGE: Chris, it's fun spending time with you, man.

CHRIS: I appreciate it. This is pretty fun.