

#96 (SHANE JOHNSON)

This transcription was provided by a transcription service that uses artificial intelligence. While their advertising claims accuracy for clear audio transcriptions, Reducing Crime LLC and Jerry Ratcliffe have not checked the transcription and make no warranties or representations of any sort, implied or expressed about the reliability, availability or accuracy of services, products, information or transcriptions contained on our website or in this document for any purpose. We make no claim that this transcription is verbatim. Any reliance that you place on the information contained within this document is strictly at your own risk.

Jerry Ratcliffe:

Reducing crime features conversations with influential thinkers in the police service and leading crime and policing researchers.

Professor Shane Johnson, MBE, is the director of the Dawes Center for Future Crime at University College London. We chat about his role as a leading researcher on the prediction and prevention of crimes facilitated by emerging technologies such as the internet of things, smart cars and wifi enabled toasters.

Jerry Ratcliffe:

I'm Jerry Ratcliffe and this is Reducing Crime.

One of the real delights of having this longstanding podcast is that it gives me the chance to properly chat with longstanding old friends. I first met Shane Johnson over a quarter of a century ago around the time we were both completing our PhDs. I was wrapping up mine at the University of Nottingham and here at the University of Liverpool. Well, since then, he has forged a stellar career at University College London as a professor in the prestigious Department of Security and Crime Science.

Over the years, his research has examined everything from residential burglary patterns to predictive crime mapping for smartphones. As the UCL professor of future crime, Shane directs the Doors Center for Future Crime and he co-chairs the Home Office Science Advisory Council. He's published over 170 research articles, attracted millions in grant funding, has a Chief Constable's commendation for his work on what works to reduce crime. And in 2025, Shane and his wife, Kate Bowers, were co-awarded the Ronald V. Clarke Award for fundamental contributions to environmental criminology and crime analysis. In 2024, in recognition of his outstanding contributions to criminology, security science and crime reduction, Shane was appointed a member of the Order of the British Empire. To us Lo Lifes, that's an MBE. Now back in January, I was in the UK for an intelligence conference. Well, I really went for the splendid weather at that time of the year, but took the opportunity to catch up with Shane in his office in Central London.

Jerry Ratcliffe:

Now you've got to position where you are one of the best people in the country to understand how technology can create crime opportunities and just how incredibly fast it's moving and how much it pervades everything. Every time

your two boys pick up their phones, do you kind of go, "Oh my God, what's on their devices and what's listening to us?" Is it painful to know what are the possibilities?

Shane Johnson:

Yeah. And recently the thing that I was telling them off about is obviously they don't update the software on their phones and they look at me and they go, "Dad, security, isn't it? That's why you're worried." I'm like, "Yeah, damn right security. That's what those updates are. " They're quite good actually, to be honest, because I've talked to them so much about it, but you do worry when you see the sort of things they can access and so on.

Jerry Ratcliffe:

Are we losing this race with certain generations? I got sent, I had an outstanding bill at my dentist, because of course, under the American system it's all for-profit and they couldn't guess exactly how much they needed for some dental work, but it didn't come exactly from the dentist's email address and it didn't come from a phone number. So I just had to ring them to check that this wasn't a scam. But I can imagine lots and lots of people at both ends of the spectrum, especially age, either young or really old, are incredibly vulnerable to this type of thing.

Shane Johnson:

It's really difficult, isn't it? Because it's so easy to do so many things like spoofing phone numbers, spoofing email addresses and things like that. So things that you take-

Jerry Ratcliffe:

And I just got to explain to folks, when you say spoofing email addresses and phone numbers, that's making a phone number, calling somebody, and making it look like it's a phone number they know or they recognize, but it's actually from somewhere else on the planet. Probably- The same thing with email.

Shane Johnson:

Yeah, absolutely. And really easy to do it should be easy to address it, I guess. And governments are making strides to do that, but it's certainly not in place in most countries. So it's easy to do. I guess you take it for granted that if it looks correct, it is correct. And the sort of advice always is to do some kind of multifactor authentication. And for a human that's, like you say, it's calling somebody and just checking, dialing the number that you verified and know is correct.

Jerry Ratcliffe:

But even that's challenging because I spoke to what I think as a human, but now with the growth of AI, I don't even know if I even spoke to a human being.

Shane Johnson:

You might not have done as well because the speed with which you can create deep fake audio, again, it's incredible and that can be automated as well. So it's not particularly challenging if you know what you're doing with these sorts of things.

Jerry Ratcliffe:

It's fascinating stuff. You got into this working in criminology, but like myself, your main interest is not in mainstream criminology kind of criminology. I always joke that if you weren't hugged enough as a three-year-old, there's a 0.9% statistically significant chance you'd be robbing a corner store when you're 30, but much more practical stuff, opportunity theory work. Yeah?

Shane Johnson:

Yeah, absolutely. And actually that approach fits really well with thinking about the risk we're talking about, sort of event-based things rather than motivations of people and how they end up, how they end up and the things that they do.

Jerry Ratcliffe:

So explain a little bit the thinking behind the less traditional criminology approach, the more crime science approach.

Shane Johnson:

I mean, it draws on a number of theories that have been around for quite a while. So things like routine activity theory, where a crime occurs when you have a motivated offender, there's a suitable target that can be exploited, and we don't have capable guardianship in place. And the idea is that our routines, the things we engage in urban spaces, but now increasingly in online spaces create those sort of convergences. And so when those convergencies happen, crime is more likely to take place. And so that could be a fight in the urban space.

Jerry Ratcliffe:

Yeah. Kids congregate after school at bus stops and transit centers and that can cause problems. That's an example of it.

Shane Johnson:

Absolutely. Online, maybe more people buying things online. So that's more potential suitable targets if you don't verify the sorts of websites you're going to. You don't need more offenders for that to happen. You just need more people going to the wrong sorts of places that have been, again, spoofed. So you can spoof a website, make it look like a legitimate one. And if more people go to it, then you get more crime. What other theories? Yeah, of course, rational choice theory or rational choice perspective. So this idea of offenders weigh up the risk effort and reward when deciding whether to offend and if the reward outweighs risk and effort, crime's more likely. And we know that applies to crimes in urban environments, but again, it applies to crimes in online environments.

Jerry Ratcliffe:

Okay. In what way?

Shane Johnson:

When we think about online crime, it's becoming increasingly easier to commit offenses. So the sort of effort involved and probably the risk involved is lower and the rewards are higher. So you think about financial crime like fraud and

things like that. It's increasingly easy to commit those. We talked about a minute ago about generative AI and the sort of generation of content or it's sounding like somebody speaking to you when they're not. So the effort there is really quite low, but the rewards you might get can be incredibly high.

Jerry Ratcliffe:

Am I in the wrong job then? I mean, the mortgage has got to be paid somehow, right?

Shane Johnson:

Possibly. You probably heard of these virtual kidnappings. Have you heard of this idea?

Jerry Ratcliffe:

No.

Shane Johnson:

Okay. So this is a good example where the effort's got lower and lower. The idea is that you get a phone call from somebody. When these crimes started, it would be somebody typically in prison in a certain part of the world. I won't name it, but they'd call you up and say-

Jerry Ratcliffe:

Name it, name it. Where are we talking about? I mean-

Shane Johnson:

I don't want to give any ammunition to certain political leaders, so I'm not going to name the country, but you can probably imagine.

Jerry Ratcliffe:

You are a tease you know.

Shane Johnson:

You can look it up. They'll call you up and say, "We've got your daughter. We've Kidnapped your Daughter."

Jerry Ratcliffe:

It may be a country I've done some work in the last- It

Shane Johnson:

Might be. It may well be. It may well be. And you would say something like, "Are you okay?" And then an actor would sort of scream in the background, make it sound like they've got your daughter and then they would put a lot of pressure on you to pay a ransom, keeping you under pressure so that you're more likely to pay. So they don't give you time to think about it. The effort involved was calling up people to do it. The actors that were involved, don't mind, they were in prison, so they got a lot of time on their hands. But if you want to scale that up, you need lots of actors and obviously not everybody pays. Not everybody's got a daughter because these, as I understand it, these people were cold calling

people without any intelligence. But if you can now do this automatically with AI, you've lost all those constraints so the effort involved is incredibly low

Jerry Ratcliffe:

And the opportunities increase exponentially.

Shane Johnson:

Absolutely. Absolutely. And I guess as well the other thing is you could, I mean, we shouldn't probably be talking about tactics here, but you could use an AI to draw content online to find out things about the most likely targets that you might want to go after because they have got children, they have got resources and so on.

Jerry Ratcliffe:

So this suggests that if people are using social media, they should lean towards having things like restricted accounts that are only available to their friends and less public.

Shane Johnson:

Absolutely. There was an interesting report that came out, I think it was last year. What the researchers were doing was they were using smart glasses that take photos. Right,

Jerry Ratcliffe:

Like Meta glasses and some glasses that have cameras built into the side. That

Shane Johnson:

Type of thing. I can't remember it was it. I think it was those,

But it might not have been, but that sort of thing. And what they were trying to explore was if you walked past somebody and took a photo of them, what could you automate in terms of what you could capture online about that particular individual? And they were showing that given the amount of content that's online, some of it you have to pay for, but you could very quickly figure out where somebody lived, where they've been to college and so on, and you could automate that. So you can still see that's not a great place for us to be in.

Jerry Ratcliffe:

Could you almost do that in real time?

Shane Johnson:

Yeah, they were pretty much doing it in real

Jerry Ratcliffe:

Time. So you could walk past somebody, take a photograph of them, and then about five minutes later, turn around and say, "Hey, excuse me, Brenda." And you know everything about this person?

Shane Johnson:

Yeah. And even if you couldn't do that today, you will be able to do that tomorrow because those sorts of things will speed up. I mean, the great thing about that research is what the researchers, they didn't publish, they didn't give the techniques away to anybody. And with this sort of research, people go through responsible research and innovation. So you would let the companies know this is what we found, you need to shut this down. But it's scary to think you can do that. It's that easy. The efforts reduce that much.

Jerry Ratcliffe:

Your original work was sort of like myself in physical security, urban security, reducing burglary, that kind of traditional crime. It seems like you need a mindset change, but fundamentally the principles about shutting down crime, it's mainly about reduction of opportunities, isn't it, moving into internet technology enabled spaces?

Shane Johnson:

Yeah, absolutely. The shift is not so much conceptually, it's more like who are the actors that might play a part in this as well, because relatively new to us in many ways. So we don't have police forces that police the internet in the same way that they police physical spaces, but there are also other sort of actors that can play a part that might not play an immediately obvious part in physical spaces and have the same sort of direct control.

Jerry Ratcliffe:

What do you mean?

Shane Johnson:

So a lot of stuff that we're using that's internet connected, it's obviously designed in a particular way and it should have security built into it to make it secure. But sadly, when lots of products and services are designed, those that make them don't think about security and so on. So there's a really important role for regulators in this sort of space that can impact upon the security that's built in, which can then obviously impact upon the crime that can take place. And I think it feels to me like there's a more immediate connection between what the regulators can do and those that enforce the regulation to reduce crime than in physical spaces.

Jerry Ratcliffe:

That makes sense. We used to often think that Apple devices, for example, were built with very little security because obviously the company didn't care. If it was stolen and taken away from you and somebody could repurpose it, that would just inspire you to buy another one. Now that may be Machiavellian thinking, but we're all good conspiracy theorists at heart, right? But that does suggest that certainly early on in the technological world, there really wasn't a lot of impetus to include security as a metric because you wanted it to grow as quickly as possible and that's changing now?

Shane Johnson:

I think so. Well, with some companies, I mean, Apple's a good example because they have a closed ecosystem. So when you're installing new apps on your phone and so on, it's going through the app store and they checked the content

Jerry Ratcliffe:

List.

Shane Johnson:

I hope so. Whereas you're using other systems, it's all fragmented. So there's a risk that the stuff you're putting on there potentially might have sort of issues malware and things like that associated with it.

Jerry Ratcliffe:

Are you saying you didn't let your two teenagers get Android phones in? Is that what you-

Shane Johnson:

That's pretty Much what I'm Saying.. I mean, it's good because it's locked down. I think there's a realization about the importance of security. I still think there's a long way to go. I don't think we're anywhere near there yet in ensuring that everything is secure by design, but I think there are efforts being made to do that. We've worked on quite a few sort of projects where we're looking at different technologies and you can see that security is often certainly not the first thought because security costs money as well is one thing. And it also costs size as well. To build it in, you need some compute power on a device and so on. And if you're building a little device, there's trade offs.

Jerry Ratcliffe:

And this stuff seems to be everywhere now. I think my car has probably more computing power than Apollo 11 that landed on the moon. I just had an upgrade of my water heater. My water heater is connected to wifi network. I can log into my water heater from the far side of the planet and turn it into vacation mode or turn it into ... It's a fucking water heater. I mean, it probably has an Instagram profile now. It probably is. It's more popular than me. My water heater is an influencer. He's complaining about his Tinder profile. I can beat that for ludicrous. I'm feeling really hot right now.

Shane Johnson:

Steamy. Yeah. So I can beat that one. So I was looking at, just before we spoke, like stupid internet products and internet connected products and a couple that I thought were great were internet connected kettles because it's like you've got to put water in it. You can't switch it on without water. So you've got to be next to it, right? The other one was the toaster, which by definition has the similar problem with it, but

Jerry Ratcliffe:

It's- Oh my God,

Shane Johnson:

Why? And the other one which is-

Jerry Ratcliffe:

Does it send you your annual profile at the end of the year? Here's how many muffins you've toasted over the last year. Let's go back and celebrate your highlights.

Shane Johnson:

Talks to the cattle probably, which is a fireus next.

Jerry Ratcliffe:

Oh my God, it's the talkie toaster from Red Wolf.

Shane Johnson:

Oh no. But the other one that I've always really liked was the hair curlers that are internet connected because again, you're generally users- When they're next to your head. So the need to connect them by WiFi seems a bit crazy.

Jerry Ratcliffe:

I know one or two people who get a little bit anxious about whether they've been plugged in when they've gone to work. So I suspect that you may be laughing about this and there's a few people listening going, "Oh shit, that sounds like a great idea." I can just sit on the train on the way to work and just check with my hair products that they're all being ... You switched off. Of course it's not going to respond if it's switched off.

Shane Johnson:

I take it all back. They're brilliant ideas, all of them totally great. But of course the risk that comes with that is you connect these things and again, are you going to have security built into those and are there risks that are carried by ... So with the kettle and the toaster, obviously we were talking about routine activities before, like you might not see a risk in there being anything in the kettle that you want to steal, but it does tell somebody what you're doing when you're home, perhaps when you're not home.

Jerry Ratcliffe:

Your routines of your behavior.

Shane Johnson:

Yeah. Sometimes it's not immediately obvious why it would be useful to be monitoring the actions of a device like that. But of course, if that device has got a password associated with it, the other issue is a lot of people use the same passwords for everything. So we steal that and now we've got access to other stuff or you've got access to the network. So maybe the kettle's got a really weak security on it and that then allows you to piggyback into the rest

Jerry Ratcliffe:

Of the- Oh, right. The target really isn't the kettle.

Shane Johnson:

You're just bouncing off it.

Jerry Ratcliffe:

You're using the kettle as a weakness to get into somebody's domestic sort of wifi system and from there access much more important stuff.

Shane Johnson:

Exactly. Exactly.

Jerry Ratcliffe:

And then turn the fridge off and that's it. Disastrous. What about some of these devices that actually listen to you all the time, like Google home devices and Alexa and all that kind of stuff and hopefully people are listening at home on their speakers and if I say Alexa again, I'm just annoyed like 50 people

Shane Johnson:

Or hey Siri turn over

Jerry Ratcliffe:

The

Shane Johnson:

Chat at the TV. I mean, the funny thing with those as

Jerry Ratcliffe:

Well- Thanks. No, look, you've switched my phone on. Great.

Shane Johnson:

Of course the thing you notice that the thing which is funny about using those is how incredible they are in terms of they interpret what you're saying. So if you tell one of those devices to turn the light off, it's great, it understands you. But you also notice the frustration with how frequently they don't hear you correctly. Yes. We had one of those devices and its only job was turning the lights on and off and it would be like about three and 10 they would get it right. And you're like, "You've got one thing to do. You only need to learn one pattern of words or remember that all we ever ask you to do is turn the lights on and it doesn't work as well as it should."

Jerry Ratcliffe:

And it's often the simplest repeated instructions. You work the last three times, why are you now struggling with this? This isn't a developmental process.

Shane Johnson:

Yeah, exactly. So that then makes you think how well do these things work? Then that gets you to, given how embedded they are in everything, I think even 10 years ago there was more lines of code in a car than the large how drunk colliding. There's quite a lot of coding, I imagine, what you'd hope there was. So that will have increased massively since then. And as you have more AI built into systems like vehicles, you then start wondering, well, if the Alexa can't turn the light on and off, how comfortable are we with it driving you around and acting as a safety device as well as securing?

Jerry Ratcliffe:

Right. Yeah. I can speak to my car while it's listening to me, but I drive in suburban Maryland where people are abysmal drivers. So it's learning some very new and imaginative swear words. I'm not sure exactly how much that's helping the algorithm any, but yeah, you don't have a self-driving car, do you?

Shane Johnson:

I think most cars have some level of autonomous. It's not self-driving, but it will drive itself if you see what I mean.

Jerry Ratcliffe:

Yes,

Shane Johnson:

Still have to put your hands on the wheel.

Jerry Ratcliffe:

Yeah. My car will steer itself back into the lane if I start to deviate a little bit, but yeah.

Shane Johnson:

And depending on how much you're paying for that car, you have to grip the steering wheel really, really hard if the sensors are really cheap or you can just react.

Jerry Ratcliffe:

Yes. Mine has a sensor in the steering wheel and I think a little camera as well. And I've figured out how to cheat the system. I can just about get away with nodding off gently after a few beers. I'm only joking people, I'm only joking. Is there value in people trying to figure out how to crack a car?

Shane Johnson:

Absolutely. We did do a project on connected autonomous vehicles recently. So we were looking at what some of the security vulnerabilities are and what some of the actual crime threats are. In the information security world, they're really good at spotting security threats and doing the work on them, but they often don't follow through to say, "What's the real world consequence of that?"

Jerry Ratcliffe:

So they're good techie people, but they need a criminologist or a crime scientist to actually help them understand the implications. Might want

Shane Johnson:

That. Exactly. We did a systematic review and we found 217 cybersecurity threats associated with autonomous vehicles.

Jerry Ratcliffe:

Great.

Shane Johnson:

Quite a lot.

Jerry Ratcliffe:

Yeah, no, sure.

Shane Johnson:

But in terms of the sort of crimes that you might do, some obvious sort of things are things like denial service. So one manufacturer at least a few years ago, all their cars just stopped working. People couldn't access them. The press on that was it was just a software fault.

Jerry Ratcliffe:

Well, if they were emergency service vehicles or for the military.

Shane Johnson:

Yeah. Then if it was just consumer vehicles as well, if you shut them all down, what would you pay to get access to your vehicle if you're using it to go to work?

Jerry Ratcliffe:

Yeah. I mean, Amazon and UPS rely on gazillions of these vehicles.

Shane Johnson:

Exactly. So denying a service like that is one risk. The other thing is of course, there'll be an increasing amount of payment services in autonomous vehicles, partly because the cars are electric. So you go to a charging station, you're paying for that charging through the vehicle. It's likely that manufacturers are going to start offering you more and more services through the car, just like they do through smart speakers and things like that, which means you've got payment information in your vehicle being transmitted to pay for things and so on, which then creates a financial risk.

Jerry Ratcliffe:

So I just shouldn't ever get in a Waymo next time I'm in San Francisco. Am I taking my life in my hands just watching this thing drive around that's going to ram me into a wall?

Shane Johnson:

Well, actually interesting to say Ramming to a wall. Don't know if you've seen any of these videos online where people have been showing how you can trick some of the vehicles. So a well known brand of, let's say, autonomous car

Jerry Ratcliffe:

Where- Does it rhyme with Bezler?

Shane Johnson:

It might.

Jerry Ratcliffe:

Okay.

Shane Johnson:

It really might be quite similar. Well, basically what they've shown is you put up a physical wall, but you put a painting of a road on it because this particular vehicle uses the cameras for object recognition and so on, it doesn't use LIDAR. They've made the wall out of polystyrene or whatever, so it's not

Jerry Ratcliffe:

Dangerous.

Shane Johnson:

But it just shows you can trick it.

Jerry Ratcliffe:

That's going to be freaky for the next Banksy.

Shane Johnson:

But there's a set of other attacks called adversarial attacks. There's a whole field in information security where you're looking at ways in which you can trick systems to make it think something is one thing when in fact it's another. Again, you might have seen these examples where people put little stickers on stop signs and it tricks the car into thinking it's like 60 miles an hour or 30 miles

Jerry Ratcliffe:

An hour. Oh wow.

Shane Johnson:

So come back to your question, should you trust, you kind of want to know what it's using. And these are real world things that they've demonstrate. They've taken the cars out, tested it, and it's got it wrong.

Jerry Ratcliffe:

So when my car is checking that I'm actually holding the steering wheel and it's using a camera to check that my eyes are open and I'm watching the road, that's actually a legitimate application of an important safety feature because the car simply can't be trusted yet to do its own thing.

Shane Johnson:

Yeah. Full autonomy means you can sit back and relax, you don't need to do anything, but the moment it's kind of hands on the steering wheel, looking at the road and the idea is that the human can take over if it does things incorrectly. If

you're not actually holding the steering wheel, you're not sort of actively driving the time it takes you to adjust to that is too long to actually adjust. If there's an emergency situation, you just can't react quickly enough. I've

Jerry Ratcliffe:

Got to be honest, it's sounding a little bit daunting like just the pace of changes for us mere mortals almost impossible to keep up with.

Shane Johnson:

Yeah, absolutely. And the pace of change is always increasing. I think it was Justin Trudeau that said this, things will never move as slowly as they do today because things are just moving so, so quickly over time. And most technologies have like an exponential trajectory in terms of their growth. With ChatGPT, I don't know if you've followed its trajectory in terms of its performance at task, but one of the things that they do is they'll get it to do human tasks and use that as a barometer of how good it is. So one of the tasks they get it to do is the uniform bar exam. And in between two releases of ChatGPT in just five months, it went from performing in the lowest 10th percentile to the top 10th percentile.

Jerry Ratcliffe:

So I don't need to hire a lawyer anymore.

Shane Johnson:

Probably not. Probably not.

Jerry Ratcliffe:

I just want to stress, not that I do anything that requires me to hire a lawyer. So I could put that caveat in there quickly Not anymore.

Shane Johnson:

But most technologies follow that exponential right trajectory. The problem with that, of course, is that we think in linear terms, so we think pretty much tomorrow's going to look a bit like today. Problem with that with prime and kind of technology and other things is that we tend to underestimate how quickly things will actually become available to criminal actors and so we don't have mitigations in place as quickly as we should do. And AI is an example of that. Five years ago, when I was talking to people about AI, you had to explain what it was, first of all. Now I think everybody, well, at least thinks they've got an understanding of what AI is.

Jerry Ratcliffe:

Its area of expertise seems to be writing mediocre student assignments

Shane Johnson:

And undressing people. It seems to be its only other use case so far. But the point I was trying to make about that is it's we've gone from five years ago it being something you had to explain to people to, this is completely ubiquitous and it's pretty much in anything that you're using, isn't it? Like we've said cars Already, Your phone has got-

Jerry Ratcliffe:

My down water heater will have it soon.

Shane Johnson:

Indeed.

Jerry Ratcliffe:

It becomes sentient.

Shane Johnson:

But it's happened really quickly. Adoption's been really quick and this responsibility in releasing it is perhaps not quite as responsible as it could have been.

Jerry Ratcliffe:

So do we need a separate AI that's designed to create security measures and keep up with security because human beings can't? You know I'm leading towards Skynet here at this point.

Shane Johnson:

The sort of issue with what you've just described, and I think that's the way people think about it is that most sort of generative AI sort of approaches have two elements to them. One will be something that generates things and the other thing which is a classifier. So it tries to understand what the generator's doing. So if you're generating pictures of faces, the original technology for that was generative adversarial networks and that's literally what they are. OI, basically one part of the AI would be generating the image of a face, handing it over to the classifier and saying to the classifier, "Can you tell whether that's real or fake?" Initially it produces a really rubbish looking face, but like if we were drawing a face, it would look like that.

Jerry Ratcliffe:

Pretty much.

Shane Johnson:

And classifier goes, "Yeah, that's definitely you've made that up." But then it goes through these iterations. As the generator learns what the classifier can differentiate, it gets better at the task. So ultimately it can generate a picture of a face it can't differentiate between.

Jerry Ratcliffe:

We can't use AI to catch AI because we're using AI to train AI how to defeat AI.

Shane Johnson:

I think that's pretty much, or at least I think- I'm

Jerry Ratcliffe:

Going to have to go back and listen to that seven times to see if I sounded like a moron.

Shane Johnson:

We probably can, but it's a bit more complicated than it sounds. And I think sometimes people just think we can just do that and it'll solve everything. You've got to remember that that's already happening in the background, that whatever the AI is producing, it's already gone through this arms race.

Jerry Ratcliffe:

It also strikes me then that the pace of change is such that we're always going to be lagging. I think you've talked to me before about crime harvests.

Shane Johnson:

Absolutely. I mean, you can trace this back hundreds of years where things are introduced without real attention given to crime and security. The first one is, you know the penny black stamp?

Jerry Ratcliffe:

Yes, very simple little stamps.

Shane Johnson:

Yeah. And so the idea was you could use it once and then there's void, you couldn't use it again. So they would do this. They frank the stamp once you used it and they used red ink. Do you know anything about red ink at the time?

Jerry Ratcliffe:

No, it's not my area of expertise. Well,

Shane Johnson:

You're going to be reading up after I tell you

Jerry Ratcliffe:

This. I've got some boring hobbies, but this was not one of them.

Shane Johnson:

So it turns out red ink was water soluble.

Jerry Ratcliffe:

Oh my goodness.

Shane Johnson:

So they used two colors and they hadn't thought things through enough to realize actually that there was a problem here. The ultimate solution was obviously to flip the colors, like you make the stamp red and the franking's black. So

then if you rub it with water, the stamp's worthless anyway. But it's a great example I think. Hadn't kind of thought about it because they wanted to make the stamp not worth anything once it'd been used, but they hadn't really thought about the ways in which people would get around

Jerry Ratcliffe:

It. I think we have to explain some of this. For people who are listening who are Gen Z, we have to explain what a stamp is, but it goes on a letter and used to write letters and then you'd post, then we have to explain to them what a post office is. This is going to be very complicated for Gen Z. It's like, where do you hit send?

Shane Johnson:

And what do you mean you write it? And just type in a prompt and it does it for you. But I mean, I like that example because it's really, really simple where you've only got two options and you pick the wrong one.

Jerry Ratcliffe:

Right. Yes.

Shane Johnson:

I mean, it's brilliant.

Jerry Ratcliffe:

It's amazing we still have a postal service.

Shane Johnson:

It's indeed. Probably why it's so expensive, isn't it?

Jerry Ratcliffe:

Exactly. You've said to me in the past that we solved some of the crime problems, but then that created more problems.

Shane Johnson:

Or it leads to new ones like emerge. So we went from physical keys where you put the key and you turn that and then we had these remote locks where you'd have a key.

Jerry Ratcliffe:

With the younger people listening, this started like too old farts just reminiscing about how the model two forward was fantastic. Well, it was. You had to crank that handle at the front and then the chat walked in front of you waving a red flag. Those were the days marvelous.

Shane Johnson:

Not even go on to chokes. So the great thing about the remote key was at this convenience, right? You could open the car from afar. A thing I thought was nice about it was you had to press a button to send the remote signal. At some point the manufacturers decided pressing that button was all too much. Exhausting. I mean, who wanted to go to all

that effort? So they created the passive key systems that we have now. Now the key's always sending the authentication signal to the vehicle. That leads onto these sort of things we call replay attacks where what offender does is they capture the code which is being sent from the key fob. Once they've captured that, they can then play that to the vehicle and then open your car. And in some cars, you can then drive the car away because of the way the security works.

A nice example of where industry, because they've not really thought through the security fundamentally as they should have done, they've reintroduced a problem that they'd solved 20, 30 years ago and creating convenience to us that we didn't really need anyway.

Jerry Ratcliffe:

Could say that, but my car gets super excited every time my phone wanders near the garage and I'm just taking out some rubbish to throw it away or recycle it. And the car's like, "Are we going somewhere?" I shut the fuck up. The wing mirrors are opening, the lights are Going On. Every single fucking time. So Again, maybe I've got it wrong. Maybe we do need that. An offender would have to be there when you press the button, which made it relatively difficult to do it. Whereas if you're just always on transmit, it's Trivial.

Jerry Ratcliffe:

This whole thing seems incredibly daunting. Even phrases and things outside of sci-fi, I've never heard of. Quantum computer Computing and all that kind of stuff you've talked about. This seems to be stuff that's only for universities and super big businesses, but how is there crime around that kind of stuff?

Shane Johnson:

So first thing is I'm not even going to try and describe quantum computing. It's basically magic.

Jerry Ratcliffe:

Right. I mean, if you try and describe it, it becomes something else, isn't it?

Shane Johnson:

Exactly.

Jerry Ratcliffe:

Schrodinger as quantingum thingy Duberi, and we've lost so many people are tuning out now.

Shane Johnson:

I think the fundamental point to make about it is like-

Jerry Ratcliffe:

You're not even going to try either. I'm going to try- Can anybody explain what quantum computing is? No. All right. What

Shane Johnson:

I'm going to say is they're going to say, so with classical computing, we've got bits, ones and zeros, and you have to go in a kind of linear fashion. If you like, you have to try one thing after another. With quantum, you can effectively do- If you do a

Jerry Ratcliffe:

Basic program, it makes sense. You do one line of code and it goes to the next line.

Shane Johnson:

With quantum, the idea is they can be in any state all the time. So you can do things some things, some tasks incredibly quickly.

Jerry Ratcliffe:

So you can be between a zero and a one or a zero and a one at the same time. Or both.

Shane Johnson:

I mean, it messes with your head. The risk with it is, or one of the risks is most of the way that our data is encrypted uses public key encryption.

Jerry Ratcliffe:

Can I interrupt for a moment and ask you to explain to people what public key encryption is and why it's so appealing?

Shane Johnson:

You want a simple explanation of that? Okay.

Jerry Ratcliffe:

Well, I mean, it's got to be easier than explaining quantum mechanics. I'll give it a go and you can tell me how far I'm wrong. If I understand it correctly, what it means is you can publish a public key and I can use that public key to send you a message. And even though everybody can see your public key, only you can decipher the message.

Shane Johnson:

Pretty much. Yeah.

Jerry Ratcliffe:

I didn't completely foul that up. No,

Shane Johnson:

That's absolutely right. And a lot of data, everything that we use on the internet is using, as I understand it, is using public key encryption. The assumption is the approaches that we use for that encryption are safe enough because it would take a classical computer lifetimes to crack it. Let's not get into because neither of us are qualified. It involves the factorization of large primes do that.

Jerry Ratcliffe:

That sounds fantastic. You've never been so sexy to me saying that kind of stuff. It's like, don't ask me to rule out things I'm not qualified for. I wouldn't have a podcast for crying out loud. I'm not qualified for anything. Yeah.

Shane Johnson:

It'd be like listening to John Cages four and a half minutes of silence.

Jerry Ratcliffe:

Oh my God, yes. There's a deep reference. Three people got that, but

Shane Johnson:

They appreciated it. They did. They'll come back for more podcasts. So the issue with the quantum computing is when we have that capability, these sorts of approaches to encryption could be cracked and that data decrypted. But there's also this existing problem of, if you've heard of this phrase, "harvest now, decrypt later".

Jerry Ratcliffe:

No.

Shane Johnson:

It's the idea that nation states, maybe even organized crime groups are hoovering our content that they can't decrypt right now, but they know they're going to be able to decrypt it later And get That capability. Even if we use methods now to prevent onto machines from decrypting our data, we can't go back in time and encrypt data that's already been harvested.

Jerry Ratcliffe:

I can see that having some major national security implications. I'm here in the UK because I was just at the National Police Chief's Council's National Intelligence Conference. I gave a plenary on bizarrely pushing back against all the tech and the digital stuff and saying, "We actually need more face-to-face informant gathering." Because I think the criminal fraternity are becoming wise to a lot of their digital protection. It's getting harder to break into their stuff and they've moved to more face-to-face communications in the middle of a field as a way to avoid surveillance. But I can't deny that 90% of the talks had a digital component to them. This whole conversation is leading me to fee that the solutions to this, they're not really local, are they? Though I think there's a role for policing in, they'll be the first ones to see the crime problem because it gets reported to them.

But how quickly can we get it up to the level where ... I mean, what is the level where organizations can do something about crime problems like this?

Shane Johnson:

One of the problems we have right now is actually counting this stuff because a lot of the crimes that involve an internet connected device or let's say somebody's used a deep fake, committed crime against you, which might be like non-

consensual sexual abuse imagery, that sort of stuff, really difficult to report that. Who do you report that to and are they counting it?

Jerry Ratcliffe:

Even simple stuff, I've been the victim of basic credit card fraud. I think most people have. And I reported at the credit card company, they refunded my money, but I never reported it to the police and I doubt they'd appreciate it anyway.

Shane Johnson:

Well, exactly, because there's more crime to deal with, right? But if you can't count it, you don't know what the problem is. We do need some transparency around that so we can really understand the scale of these issues and how much they're growing. But like I say, with fraud, you don't have to report to the police to report to the bank. So there's almost no incentive for you to report to the police.

Jerry Ratcliffe:

And I guess the banks aren't that keen on advertising how much fraud they're the victim of because that might drive people to not bank with them.

Shane Johnson:

Exactly. Or use them as much as they might otherwise do. And you don't want to advertise your shortcomings. It's okay to do it for other people's, but You Don't want to do it for your own. The banks have an important role to play not just in recording the issue, but actually addressing it. And that sort of leads us on to what brings us back to where we talked about routine activity theory before and there's John X extension to that where he talks about place managers and the banks in this case might be-

Jerry Ratcliffe:

Yeah. In a physical sense, we would think of place managers maybe being shopkeepers who keep an eye on the public space outside their shop. They're not responsible for it, but they take on a de facto responsibility to look out for that space and they might call the police or shoot some young kids away or causing some trouble there. Yeah.

Shane Johnson:

Yeah. Or a bar manager might hire security staff to manage things in a certain way on certain night.

Jerry Ratcliffe:

But they also keep an eye on the street outside as well.

Shane Johnson:

Yeah, Exactly. And so they're playing this crime prevention role and in some cases they've got a legal duty to do it. In others, it's something that they do, which is additional. And the banks clearly have that role in this case, but going beyond that, John Eck talks about super controllers as well. So what happens-

Jerry Ratcliffe:

They're the really awesome controllers, right? They're the best place managers. Yeah.

Shane Johnson:

It's a great awesome controller. Yeah, maybe it needs relaying. But I really like the idea because it's like when the place manager doesn't do what they're doing, who is it that encourages them to do things? And so John talks about there's a range of super controllers. So we can be super controllers because we think like a vehicle's not secure or whatever, and we decide not to buy it for that reason, then we influence the market.

Jerry Ratcliffe:

So if word gets around on social media, that particular type of vehicle could be easily broken into like the Kias did for a short while, I'm sure that their sales probably plummeted because you suddenly saw Kia make a real concerted effort to fix the problem quickly. Yeah,

Shane Johnson:

Exactly. So it exerts pressure on them. And in this case, it's not a legal thing, it's a market force. So that's a great thing to use because it speaks directly to the language of what they're trying to do. There are other kind of super controllers and regulators are another who can kind of set standards or legal requirements for things, but there is a caveat to that, which is we talked about super controllers nudge the place managers. What happens when the super controllers aren't nudging the place managers? So like who regulates the regulator? And I think that might be, again, the public saying, regulate, find the-

Jerry Ratcliffe:

And that's what the voting booth is for to solve this Russian doll of regulators. So you've got super regulators, not so super regulators, less awesome ones, right? It doesn't sound like any point soon you're going to be unemployed.

Shane Johnson:

Probably not or maybe not. I won't stop thinking about these sort of issues at least.

Jerry Ratcliffe:

Well, it's been a fascinating tour of a field that is, as I say, both fascinating and slightly terrifying. And I don't know how much work it probably takes you and your team just to keep up to date with all of this stuff. So you've given us a little glimpse into the window and I really appreciate it. Thanks, Shane.

Shane Johnson:

It's a pleasure. Thanks, Jerry.

Jerry Ratcliffe:

That was episode 96 of Reducing Crime recorded in January 2026 in London. If you teach, DM me for multiple choice questions for every episode and you can find a transcript of this episode at reducingcrime.com. If you do not subscribe at Spotify, SoundCloud, Apple, or wherever, your kettle will tweet bad things about you.

Be safe and best of luck.