# The Tim Ferriss Show Transcripts
# Episode 48:  Marc Goodman
# Show notes and links at tim.blog/podcast

Tim Ferriss: Hello, ladies and germs. This is Tim Ferriss. Welcome to another episode of the Tim Ferriss Show. For those of you new to the program, this is where I try to deconstruct excellence. I talk to people who are the best in the world at what they do and try to distill or extract the tools and tips and resources that you can use.

This episode is a very unusual one, a very fun one, a very useful one, I hope. The episode guest is Marc Goodman. Marc Goodman has been a resident futurist with the FBI and worked as a senior advisor to Interpol. Specifically, he's considered one of the world's leading authorities on global security.

In this episode, we'll go very deep into the digital underground to expose the many ways that criminals, corporations, countries, organized crime, and the list goes on, are using emerging technologies against you and some of the simple steps that you can take to decrease your vulnerability.

Sure, 3D printers can produce AK-47s. Bio-terrorists can now download the recipe for Spanish Flu, and cartels are using fleets of drones to ferry drugs across borders, all of which we'll touch on. But what else is waiting for you? What else is potentially targeting you right now? We'll dig into it all.

This is not from a paranoid nut job. I think it's important to underscore this. This is from a very pragmatic, real-life oriented problem solver, who has been hired by people like the FBI and Interpol. This is an informed insider, and he will describe the Wild West that is the Internet.

In that Wild West, ignorance is no excuse for being defenseless. If you want to hear about current and future threats and simple, defensive steps you can take, then this interview is for you. So without further ado, please meet Marc Goodman.

Tim Ferriss: Hello, ladies and gentleman, boys and girls. This is Tim Ferriss. Welcome to another episode of the Tim Ferriss Show. I am so excited. I can barely annunciate properly because I have Marc Goodman on the show. I'll give a quick bio for Marc, and you'll very quickly realize why I'm excited to have him on.

This is pretty much directly from the bio, but he has spent a career in law enforcement, in many different capacities. That includes work as a futurist for the FBI. Who knew they had such a thing? Senior advisor to Interpol and also on the street as a police officer.

He's the founder of the Future Crimes Institute and the chair for policy law and ethics at Singularity University, where I've had some involvement often at NASA Aims. He's continued to investigate the often-terrifying intersection of science or technology and crime and uncovering all sorts of different nascent threats and combatting darker sides of technology, which I think don't get as much sort of radio time, perhaps, as all of the promise that we hear about and the benefits of Moore's Law.

He is also the author of the fourth-coming "Future Crimes," and the subtitle pretty much tells you a lot of what you need to know. Everything is connected. Everyone is vulnerable and what we can do about it. So Marc, thank you so much for being on the show.

Marc Goodman: Thank you, Tim. It's an honor to be here with you.

Tim Ferriss: I am thrilled to have you on because I wanted to grab you as quickly as I could, because I think that you are going to be getting interviewed a lot in the upcoming months, because many people are completely unaware of, I think, the threats that are not only, in some cases, ubiquitous now or at least upcoming, but soon will be right at our doorsteps.

Just as some background for people who are listening, because I've had a lot of public exposure since the unexpected success of the first book, I've really come to realize this in a very personal way. I've had people try to hack my sites, hack my phone, impersonate different people in my life to get information from other people. It's been a real fast education in cloak-and-dagger stuff.

I wanted to make sure I gave a very brief overview. But is there anything from your background or bio that I missed, that I should share with folks?

Marc Goodman: One thing you didn't mention is the fact that I'm a huge fan of Tim Ferriss. I really love, "The Four-Hour Work Week," and it's quite an honor for me to be speaking with you today. I actually got one of the earliest editions of the book. Some of the entrepreneurship suggestions that you covered were ideas that I tried to implement in law enforcement, with some difficulty, but I tried. It was pretty good fun.

I actually took your advice on some of the things you did. I went on an information diet, not a real diet, but an information diet. I also have a love of foreign languages, the way you do, and actually enrolled in the Hartnackschule in Berlin, in Germany, just the way you did. So thank you for your book. That's something else I wanted to mention right off the top.

Tim Ferriss: That, of course, completely makes my week. Bitte schön. I hope ...

Marc Goodman: Danke schön.

Tim Ferriss: I hope you had fun. I had a great time at Hartnackschule in Berlin. I think that language is a metaphor for so many different aspects of life. Becoming fluent in a language or becoming fluent in technology, I think, can sound very intimidating to people, but it doesn't have to be super, super complicated.

But before we dig in, I'm going to try something a little different, and that is to do ...

Marc Goodman: We're going to do the interview in German.

Tim Ferriss: We're going to do the interview in German, and I'll try to teach you Swahili. No. I thought that we might do just a little bit of calisthenics by doing some rapid-fire questions first, just to loosen up the joints.

Marc Goodman: Great.

Tim Ferriss: Then we can jump into all of the spy-versus-spy stuff, which I am absolutely obsessed with, which a lot of you might not realize. But before we do that, I have to get into the really important stuff, such as ...Sean Connery came to your house for dinner. What would you cook him?

Marc Goodman: What would I cook him? I don't know if he'd eat, but I'd make him some drinks. I'm sure he'd have a nice drink.

Tim Ferriss: What would you ...What's the cocktail or the drink of choice?

Marc Goodman: I think for him, a martini. He'd be a martini kind of guy.

Tim Ferriss: Martini kind of guy. Do you have any favorite documentaries or films that come to mind?

Marc Goodman: God, I love film, and I love stupid 80s comedies, so Ghostbusters was great and anything of that genre, anything with Bill Murray or Dan Aykroyd in it. I'm a fan. Of course, I like all those 80s hacking movies, like War Games and Sneakers and that type of stuff.

Tim Ferriss: Of the hacking genre or the crime/spy genre, what movies that you like are closest to reality and furthest from reality?

Marc Goodman: That's interesting. It's very funny when you see how Hollywood goes in and portrays hacking on the screen. Most hackers get a good laugh of what they type at the C-prompt. It's pretty funny. I think actually I have to give a hat to Walter Parks, who did the original War Games, because considering that it was in the early 80s before most people were thinking about computers ...Modems were super slow and incredibly rare. The fact that he was able to bring that hacker-type out there and show that the Department of Defense was connected to the Internet, and you could change your grades. He did that 30 or so years ago. So that was really awesome, and I think that's great.

Some of the other hacker movies ...Sandra Bullock, The Net ...It was a nice movie, not particularly realistic, but there were elements of truth in it. So there have just been a lot of silly hacker movies out there because, as I've been told, it's difficult to show cool hacker stuff on the screen in a way that people will understand.

Tim Ferriss: Yeah, I had a computer scientist friend of mine also say you can always ...It's always amusing to watch hackers typing in movies because they never use the spacebar. You can tell when people are BS-ing on a keyboard because you never hear the distinctive sort of thwack of the thumb hitting the spacebar.

Marc Goodman: Tim, as you well know, all the best hackers never use the spacebar.

Tim Ferriss: That's right.

Marc Goodman: Very common.

Tim Ferriss: All the Dvorak typers out there, like Matt Mullenweg.

Marc Goodman: Right.

Tim Ferriss: Let's see. What is the book that you're most likely to give as a gift or the book that you've given most as a gift to people?

Marc Goodman: This sounds like BS, but it's actually been your book. I have to say I've given it to a ton of people. I run into people all the time, both in law enforcement, friends of mine, folks that are struggling with their careers and trying to think about opportunities to see the world in a different way. No bullshit. I've actually given away about 10 copies of your book.

Tim Ferriss: Wow. Well, I appreciate that, and my publisher thanks you for that as well.

Marc Goodman: Yes, but that was before I had my own book. In the future, of course, I'll be giving them my book. But up until then, you were my favorite.

Tim Ferriss: Well, I'll take a runner-up when your book comes out. Are there any fiction books that you particularly like? It doesn't have to be science-fiction or any particular genre. But any fiction books that have been very influential in your life?

Marc Goodman: I love the old street-crime drama. So having grown up in New York City and kind of being very in tune with the New York City Police Department, there was a book called, "One Police Plaza," by a guy called William Caunitz, which I thought was awesome, and just really got what policing was and what policing was all about. I thought that was pretty amazing.

Tim Ferriss: Very cool. I'd love to check that out. I know less about the police than I do the other aspects of the military, oddly enough. It's the law enforcement that I have the most contact with, I have the least knowledge of.

Marc Goodman: I understand.

Tim Ferriss: I suppose it's ironic. Let's see here. I'm not going to ask too many more of these because I want to jump into, of course, the subject areas that are your expertise.

Do you have any particular morning routines? What does the first hour of your day look like?

Marc Goodman: I wake up. I take my dog out for a walk, and then I have breakfast, which I really enjoy. Catch up on some news, emails, and then go and take on the day.

Tim Ferriss: What time do you typically wake up?

Marc Goodman: It depends. I do a lot of traveling. So it depends on what time zone I'm in and how jet-lagged I am, but more on the early side these days, I'd say.

Tim Ferriss: Got it. Is that like a 7:00 a.m. kind of thing? Or 6:00 a.m.?

Marc Goodman: Yesterday, I was up at 5:00. The day before, I was up at 5:00. Then mostly, I would say 6:30, 7:00, somewhere in that time-frame.

Tim Ferriss: Got it. Do you change your ...How does your routine change on the weekends? How do you decompress, if you do?

Marc Goodman: I like to go for hikes. I like to go outside. I like going to the movie theaters, seeing films, hanging out with friends, all the kind of standard stuff. For the past year when I was writing the book, it mostly was my butt in chair, typing.

Tim Ferriss: Right. When you think of the word "successful," who's the first person who comes to mind?

Marc Goodman: Wow. There's so many different ways to define success. Martin Luther King is one of the first guys that pops into my head. Clinton was a pretty successful politician. There are lots of folks out there. Of course, any of the entrepreneurs, like Steve Jobs and the like.

Tim Ferriss: Got it. So let's jump into the subject matter at hand. We can tackle this from many different perspectives, but perhaps you could give maybe a few facts or examples of things that might surprise people in the world, whether it's currently existing crime or things that you see right on the horizon, coming down the pike.

Marc Goodman: Sure. I'd be happy to do that. Basically my take on this is that folks are very focused on the cyber crime of today. Every day in the news, whether it be the New York Times or the Wall Street Journal, we're hearing that Target was hacked, and Home Depot was hacked, and JP Morgan was hacked.

What's interesting to me is that the media treats all of these as distinct incidents, like, "Oh, another company was hacked." A bunch of celebrities had their naked photos tipped off by a hacker. That stuff is all treated as if it were an individual act. What people don't see, from a 35,000-foot view, is that there's a systemic issue going on, which is something I try to mention in Future Crimes.

It's the fact that we have, thanks to Moore's Law, which you mentioned earlier, we're just moving at an exponential rate. So we're plugging more and more things into the Internet. The fact is, as you well know, software is eating the world. So everything is becoming software. Everything is becoming computer.

A car is not a car anymore. It's no longer a mechanical device. There's 250 computer chips in it, at a minimum. So a car is basically a unix box that we ride in. An elevator is a computer that takes us from floor to floor. As Cory Doctorow says, "An airplane is a flying Solaris box with a bunch of industrial controllers."

So people don't realize that. The big takeaway from that is that never has there been a computer system that could not be hacked. In other words, every computer system is hackable. There are no un-hackable machines, and that has some really profound consequences for us as a society and the world that we're building, because we're about to add between 50 and 200 billion new devices to the Internet of things, depending on who you ask. Cisco will say 50 billion by the year 2020. Intel says 200 billion by the year 2020.

The impact of that is that we're going to go from an Internet that is theoretically or metaphorically the size of a golf ball today, to one that is the size of the sun. Right? Massive.

Tim Ferriss: That's a substantial difference. Yeah.

Marc Goodman: Massive increase. We're just at the very, very earliest days of the Internet. So the, I guess you would say, mistake that a lot of people make is they think we're technologically advanced today, but they have no idea of the tsunami of technology that's coming our way tomorrow.

Tim Ferriss: I think also, to underscore that, that human beings intrinsically are very bad at thinking in exponential terms. They're very bad at predicting, for instance, the answers to a lot of these old riddles, such as, "You take one grain of rice, and you double it for each square on the chess board. How many pieces of rice do you have? How many grains of rice do you have by the end?" It's very hard for people to anticipate how quickly things can change.

For instance, I've listened to a number of your talks. You have a great TED talk. The fact that ...This may even be more accelerated now. I think your talk was in 2012. But the DNA sequencing is proceeding at five-times Moore's Law. The impact that that has on privacy and the weaponization of different types of codes ...

There's another term that you also use, or phrase rather, and that's the technological arms race, so the white hat versus the black hat. Then you have a bunch of folks in between. So I'd be curious to hear where things stand now, compared to a horrible 60-hour siege in Mumbai that you've talked about before, where terrorists built their own ops center in Pakistan to monitor the progress of these attacks in real-time, where they'd be executing people with a hand gun in one hand, while looking at their cell phone in another, which gave them huge situational and tactical advantage over the police.

But those are with relatively primitive devices, all things considered, because I think that was in 2006 or somewhere along those lines.

Marc Goodman: Right. The 2008 attack on Mumbai.

Tim Ferriss: 2008. I apologize. I remember doing research for the Four-Hour Body at one point. I was chatting with a scientist who shall remain unnamed, but he was talking about how negligent it was, in his mind, for a very well-known tech titan to have released all his genetic data or his DNA sequence, because people could create personalized biological weapons to attack him.

It sort of, I think, to the uninitiated, seems like complete science-fiction, like a fantasy. But where are we with that type of thing? Is that already being used on people?

Marc Goodman: Yeah. So you're spot on, actually, with everything that you just said. In fact, the cost of sequencing human genomes has dropped precipitously and is dropping five times faster than Moore's Law. So with Moore's Law, silicon-based technology, ones and zeros, that is doubling every 18 to 24 months, depending on who you ask.

Ray Kurzweil has shown, and the singularity is near, and many times since that there is this persistent exponential pace of technology. Synthetic biology and genetics are outpacing that by a factor of five. So biological advancements and computational biology were pretty much proceeding at Moore's Law's pace until 2008, when there were some massive breakthroughs in genetic sequencing, which made it go five times faster.

So what is the result of that? Well, there'll be tremendous opportunities for each one of us to know our genome. For example, today, most people would certainly never consider going in for a full genetic genome sequencing. Prohibitively expensive. When the US government launched the human genome project, back a decade or so ago, they allocated $3 billion to sequence the first person's genome.

They didn't get it done. They didn't complete it. Craig Venter, a world-famous biologist, came in and worked on the project built upon the work done by the human genome project. He was able to sequence, in full, the first human being, for a cost of $300 million, about 10 years ago.

Fast-forward to today. You can actually get a full genetic sequencing for $1000. There are companies, like 23 And Me, that will offer you partial genetic sequencing for just $99. Without a doubt, within a few years, it'll be the price of a cup of coffee. Everybody will have their full genetic sequence.

So that's great news for medicine. Right? Every cancer can be treated differently. You will know your proclivities for certain diseases. We'll be able to have really massive impacts on healthcare. But there's a flip side of that. When it costs $3 billion to sequence the human genome, and pieces of equipment to do that were in the tens of millions of dollars, only the government or the wealthiest universities could afford that.

Now, equipment that sold on eBay a year ago for $100,000 can be bought for $10,000 or $1000 today. That is putting the tools of genetics and synthetic biology in the hands of the common man. So there are actually high school clubs that are doing genetic sequencing today. Right? They have lots of groups. There's something called iGem, which is a high school and college competition that focuses on this.

So today's kids are very much at the cutting edge of science. Again, they'll do all different types of cool stuff. At Singularity University, we had a start-up that was creating a glow-in-the-dark plant because they thought it would be cool. Let's do that. You can do that, but the challenge with these things are not everybody playing with these tools, whether it be genetics, synthetic biology, robotics, artificial intelligence, is of a kind heart.

There are criminals and terrorists and bad guys that now, for the first time, have access to these tools. I know you're chomping at the bit. So I'll shut up for a second, and I'm happy to give some examples of what bad guys are doing with bio.

Tim Ferriss: Okay. We're going to come right back to that. I want to ask a very personal question, which is ...So 23 And Me ...I've always been nervous about having my own name associated with genetic data. So, I have thought to myself and talked with other people about, "Well, perhaps you should have a friend pay for your 23 And Me, who is of a different gender, so that if that data is ever compromised, it's tossed out or misattributed," or using a pseudonym, let's say with an authorized account under a separate credit card, et cetera, shipped to an address that isn't associated with your name, so that that data cannot be used against you in some fashion.

Is that paranoia? Or is that preparedness? Is that a practical thing, in your mind? Or something else? I'm just curious.

Marc Goodman: Well, if it's paranoia, you and I are both paranoid, because that's the exact advice I give to my friends that want to do the test. So I don't know whether or not this violates their terms and services, but the simple fact of the matter is we have no idea how they're going to use that genetic information. There are lots of sites out there, and some I mention in the book. One is called Patients Like Me.

Patients Like Me was a medical site where people were meant to be sharing confidential medical information with each other and get help for particularly rare diseases. They had something called the Mood Forum, where people were talking about psychotic breaks, suicidality, and the like. It turns out the folks that were running it were actually releasing all of that information to insurance companies. It was mentioned very clearly in their terms of service that they do so.

So you think you may be doing something that's safe and secure and private, but in fact, often you're not. So I would always look at the terms of services. Again, I don't know what the terms of services are for 23 And Me specifically, but I would say the following.

If I wanted to get genetic testing, I definitely share your concern and would not be doing it under my own name, because we simply don't know where this technology is going. We have a naivete about the future and what it might look like. I'm not sure if you ever saw the movie Gattaca.

Tim Ferriss: I've seen the previews. That's about as far as I've gone.

Marc Goodman: The short story is it's kind of a dystopian future, where everybody is judged based upon their DNA. So let's say you want to be a scientist, or you want to be an astronaut. Based upon your genetic profile, they'll say, "No, you know what? Tim, you're not quite what we're looking for." Everybody's social strata is determined by their DNA and what people presume that means.

So I won't say that exactly we'll be living in the Gattaca future. But for example, if there are genetic markers for a sexual orientation, for example, which some people suggest there are, there are definitely genetic markers for predispositions to violence, could be for schizophrenia and other diseases.

So the opportunities, from a public policy, law, and ethics perspective, to have your genetic material leak or the information about you and get out into the public sphere, I'm sure will happen. We know, today, that presidential candidates are forced one way or the other to release their medical records to show that they're fit and ready for office. I guarantee that will be happening with presidential genomes in the future.

In fact, I talked about this. I wrote an article with two friends of mine, Stephen Kotler, who you may know, and Andrew Hessle, a synthetic biologist. It was in the Atlantic Monthly, and it was called "Hacking the President's DNA." It was all about what those risks would look like and a number of bio-threats that could be launched if you had access to somebody's genetic material.

So for most folks, I don't think they have to worry about bio-hacking today. But from a privacy perspective, I think I would definitely take precautions. The ones that you mentioned about using a prepaid credit card, for example, or having it shipped to a third party and all of that stuff, I think, are good, logical, common sense steps to take.

Tim Ferriss: So what are some other ...Just for what it's worth, I want to do like an urban myth check here because, of course, I get all excited about this stuff. When I was doing research for the Four-Hour Chef and became fascinated by marksmanship and hunting, of course, that very quickly leads to the prepper communities. There's the good, bad, and the ugly there. There were some very extreme edge cases.

But I was speaking with a very well-credentialed scientist. The example he gave was a personalized weapon doesn't have to be a synthetically engineered, super fancy, sci-fi-like dart or pill or anything like that. It could be that you know someone's predisposed to a disease and that you can accelerate the onset of, say, a neuro-degenerative disease by blowing blebdonum [SP] into their face at a public event, where they might not even register that's what happened.

But if you wanted to, say, take a long-term short position on their stock, and they're running a publicly traded company ...

Marc Goodman: Right. Right.

Tim Ferriss: It doesn't have to be ...That type of crime doesn't need to be ...The diagnostics and the determining of the target could be sophisticated, but the actual attack does not have to be something futuristic.

Marc Goodman: I agree with that. I'll give you a perfect example. There's a medicine called Warfarin, which is a blood thinner. There's a certain small percentage of people that have a genetic marker that makes them allergic to that, and it's deadly if taken. So that would be a perfect example. It's a common pharmaceutical that exists today, and it's not something that you can see by looking at somebody, whether or not they're allergic to Warfarin. But if ingested, now you have that additional piece of information. You know about it, and it could be fatal.

Tim Ferriss: Yeah. Yeah, that's crazy. Yeah. I think ...

Marc Goodman: So don't do that, kids.

Tim Ferriss: Yeah, don't do that.

Marc Goodman: Don't commit bio-homicide.

Tim Ferriss: It also brings up ...I want you to give some examples. A misconception I think that a lot of people have about criminals or particularly terrorists, specifically, and that is they're just uneducated. Maybe you can shed some light here. It seems that there actually seems to be a disproportionately high percentage of very, very, very well-educated people who then are recruited by militant groups as operatives or terrorists. I think people underestimate perhaps the intellectual horsepower of some people who could perpetrate these types of crimes. I would love to hear, certainly, examples. You mentioned you might have a couple of different examples ...

Marc Goodman: Sure.

Tim Ferriss: ...which I'd love to hear.

Marc Goodman: Yeah. On the terrorist front, you're exactly right. People tend to underestimate them. When we were first going into Iraq and Afghanistan, we talked about people with towels on their heads, living in caves. What could they possibly do to defeat us? As we saw, they were able to put up quite a hell of a fight. Ayman al-Zawahiri who was Osama Bin Laden's number-two, was an MD. He was a trained physician. Right?

So there are any number of doctors that are in these terrorist organizations. We've seen them recruiting specifically on terrorist chalkboards. They're looking for people with scientific backgrounds, with technological backgrounds. One terrorist by the name of Irhabi 007. He took the 007 from James Bond, and he was basically the CIO for Al Qaeda for a while, running their technology.

In the wake of the Snowden disclosures, there's been a ton of chatter on terrorist chat boards talking about the importance of encryption. So they follow the news very, very closely and are paying attention to it. They show tremendous sophistication. Let's go back to bio, for example.

The terrorist organization Aum Shinrikyo, the folks that carried out the 1995 terrorist attack ...

Tim Ferriss: Sure. Sarin gas.

Marc Goodman: Exactly. Sarin gas on the Tokyo subway. That occurred in 95. What most people didn't realize about Aum Shinrikyo is the fact that they had a bio-weapons project. They spent $100 million a year, for 10 years, from 1985 to 1995, trying to develop a powerful bio-weapon, and the science wasn't there yet for them to be able to do it. That's why they went with the chemical sarin gas attack.

Today, things like that would be much more trivial, given the wide availability of bio-toxins and other type of infectious threats that are available online. The code is there. You can download it. Basically build some of these things in your basement or garage and release them.

Another area where we see terrorists playing in really interesting ways are both robotics and social media and open source intelligence. I'll just give a few crazy examples. So during the terror attack at the West Gate Mall that occurred in Nairobi, about a year ago, we saw the terrorists from Al-Shabaab, the militants were incredibly sophisticated in how they were using social media and Twitter. They were live tweeting the entire event, and they were actually mocking the Kenyan police force and military guards throughout the incident, putting out information, adding to the confusion.

ISIS or the Islamic State has been doing the same exact thing. You mentioned earlier also the 2008 Mumbai terrorist attack. In my humble opinion, that was perhaps one of the most sophisticated terrorist attacks we've seen to date, from a technological perspective.

Ten terrorists were able to keep a city, a metropolitan area of 20 million people, completely shut down for 60 hours. So 10 guys, not just armed with standard weapons, AK-47s, RDX explosives, hand grenades, but these guys had night-vision goggles. They had satellite phones, satellite imagery, encrypted Blackberries. They used Skype type of communications during the incident.

Because they had all that technology, they had phenomenal situational awareness, situational awareness that beat the capacity of the Indian National Guard and the Mumbai police to respond. They used it to great effect, to actually kill more people.

There's an example I talk about in the book of a man called KR Ramaporti [SP], who was staying at the Taj Mahal Hotel in Mumbai. You may have been there. It's one of the most beautiful hotels in the world. When the terrorists took over the hotel, they started going room to room, trying to find more hostages.

They came across Mr. Ramaporti, who was on the top floor in his suite at the Taj. They broke into his room, and they said to him, "Who are you? And what are you doing here?" He said, "Oh, no. I'm nobody. Leave me alone. I'm just an innocent school teacher."

Well, the terrorists were dumb. But to your point about not being that dumb, they looked at this guy staying in a suite at the Taj Mahal, beautiful hotel, and they said, "There's no way any Indian school teacher could afford this suite." They picked up his ID at his bedside, and then they phoned it in via a satellite phone to the terrorist war room that was set up across the border in Pakistan.

There, in the war room, the terrorists were monitoring live. They had IBN, CNN, BBC, Al Jazera, and a bank of computers where they were doing real-time research. So you had the 10 operatives from Laksha-e-Taiba, an Al Qaeda affiliate based in Pakistan, that were carrying out the attack, broken down into five teams of two terrorists.

Then you had the terrorist war room. So when they phoned in the name of this guy to the terrorist war room, they simply Googled him. They came across his photograph. As it turns out, he was not a school teacher. He was the head of one of the second-largest banks in India, called ING.

They came across his photo, and then we know from the intercepted conversation, which we only discovered after the fact, that the terrorist war room said, "Hey. We found a picture of your guy. Is your hostage heavy-set? Yes. Does he have glasses? Yes. Is he kind of bald? Yes. Okay. We found him.

The terrorists then said to their op center, "What shall we do?" Then the order came down. Kill him.

So the fact of the matter is, back in 2008, terrorists were using search engines like Google to determine who shall live and who shall die. Though it's a black swan of Internet, you talk about those. The fact of the matter is when you're sharing in Facebook, it's not just the media and marketing companies that you need to be concerned about.

When you share openly, everybody has access to this. Even though it's a black swan, we're aware they could be terrorists or organized criminals as well.

Tim Ferriss: I think it's a terrifying example, particularly when you consider that 2008 was the Stone Ages compared to the implications of big data and ubiquitous availability of tools today and sophistication, certainly, of a lot of those tools, including reverse-image search and things like that through Google or 10-I or others.

The black swan events also ...Just because a black swan event is considered a black swan event to the victims doesn't mean it's black swan event, i.e. a low-probability, random event. It could be completely engineered, as it was in this particular case, through extensive preparations on the part of the terrorist.

So I'd love to talk a little bit about a phrase I've heard you mention before, and that is, "Public safety is too important to leave to the professionals." So, there are a number of ways I'd like to try to unpack that. The first is just to try to bring out my inner prepper.

So if you live in a city like New York City or San Francisco or Chicago, what are the things that should be keeping you up at night, that you should be thinking about mitigating as risks or black swan events?

Marc Goodman: Well, traffic, but it's not a black swan event.

Tim Ferriss: Right.

Marc Goodman: Keeps me up at night. When I talked about that, I was speaking more broadly about kind of the cyber threat, but it's also true in physical space as well. The fact of the matter is that the line between order and society and chaos is actually quite thin. In law enforcement, they talk about the thin blue line.

I was a patrol officer in Los Angeles during the LA riots. What I realized is the police are in charge, as long as the public wants them to be in charge. Once the public decides that they are not in charge, you are no longer in charge. I think LA had 1.7 police officers for every 100,000 citizens at that point.

So if you make the citizens really, really mad, as was the case during the Rodney King incident, then it's over. There's nothing you can do. So in physical space, all the basic stuff that you talked about, the prepper movement, but the Red Cross would give you the same type of advice or the California Office of Emergency Services, FEMA. There are any number of good checklists out there about having water and food and just be prepared. Have an emergency plan.

All of that is really good and useful. I also had, unfortunately, the opportunity to be in New York City, down at 7 World Trade on 9/11. So that was another experience that I happened to have lived through. [00:38:00] That brought out the best of people in that particular instance, where you saw total and complete strangers being as warm and helpful to one another as they could.

So it can really go both ways. When I talk about public safety being too important to leave to the professionals, what I would say is that people often advocate their concept of safety to the police or to the authorities and think that everything will be just fine. Mostly in our physical space, [00:38:30] in the developed world, where we have rule of law ...Think Australia, Western Europe, North America. That's a system that works quite well.

If you look at what's going on with [inaudible] and others in Africa, it's a different story. In cyber space, it's a complete "every man for himself" type scenario. What I find fascinating is that for the most part, law enforcement has advocated any responsibility for cyber crime.

Now, I know that some of my colleagues in law enforcement might take issue with that. Certainly they're trying hard, but the volume of the threat and the nature of the technology makes law enforcement nearly impossible as a solution for the cyber threat.

I talk about law enforcement as a nation-state type solution. Right? A policeman in New York cannot make an arrest in Moscow, and visa versa. So law enforcement is a local solution to a global problem. So no matter how good the cops get, even though there are organizations like Interpol also that are trying to make a difference, they're just fundamentally mismatched. That's what we need to deal with.

If somebody came into your house and broke into it and stole something, you dial 911. If some kid spray-painted your car or your house, you'd call the police. You'd file a report for vandalism. Yet, we have the equivalent of these things going on every single day in our homes, in our computers, on our cell phones, on our tablets. If you dialed 911 to report a computer virus, the cops would come for you as opposed to sending a car to investigate it.

So, I think from that angle, we need to get average and everyday citizens involved in this. On the one hand, law enforcement has very limited resources. It doesn't work internationally, and not all agencies are particularly well-schooled on the cyber threat.

Whereas, and you know this, living in San Francisco and Silicon Valley, there's tremendous talent in the private sector that fully is versed in technology.

There's a global community of people that could contribute significantly to this problem. I think that it'd be a great opportunity to get them engaged.

The last thing I would mention, particularly since we are living so much of our lives online, staring at screens on our smart phones or on our computers every single day, there's a part of our life that is taking place in cyber space. Yet, we don't have a common defense for us for cyber space.

So for 100 years, we've had reserve army. We've had reserve and auxiliary police officers. We don't have any equivalent for that in cyber space. So when the big cyber attack comes, we're going to have a [inaudible] of resources and talent to respond.

So one of the things I call for is the building of a national cyber reserve corps. Take average, ordinary citizens, men and women, young and old, it doesn't matter. Put them through a background. Get them cleared and part of the solution, because we definitely need their help.

Tim Ferriss: So I definitely want to come back to that type of distributed or crowd sourced workforce. On a related note, I want to talk a little bit about the physical world, so meet space and those types.

Marc Goodman: Yeah. By the way, on crowd sourcing, I'll give you some great examples when we come back ...

Tim Ferriss: Cool.

Marc Goodman: ... about criminals crowd sourcing.

Tim Ferriss: Okay. Great. We can talk about the counter-forces to that also. So I remember going through a northern emergency response team training course, which was organized by the San Francisco police and fire departments. So this was not a fringe group, teaching this class.

Marc Goodman: Right.

Tim Ferriss: I remember. I'm paraphrasing here, but roughly they said ...They polled the audience and said, "Okay. How many people live in San Francisco? How many fire engines do you think there are?" It was something like 38 fire engines for ...

Marc Goodman: Right.

Tim Ferriss: ...at a minimum several hundred thousand people. The point they made was if there is a ...In the event of a real event ...Let's just call it a 7. or higher Richter Scale earthquake, you could go and very realistically could expect to go seven to 10 days without food or water.

The fact that the Lord of the Flies type scenario, while unlikely, is not as unlikely as people might think. I recall when I was writing a section of the

Four-Hour Chef, called The Wild Section. It was all about sort of foraging and hunting and preparing food without the use of a kitchen.

I went down the prepper rat hole pretty quickly. I remember having some editorial feedback from the publisher, which was critical of how deep I went into this stuff. Just at that moment, when I was being told that it was too alarmist and too extreme, Hurricane Sandy hit New York City.

Marc Goodman: Right.

Tim Ferriss: It was just a perfect illustration of how ill-prepared most people were for what is going to be an increasingly common occurrence with climate change, at least according to a lot of scientists who've looked at the modeling of, say, 100-year storms and how those might occur every decade or even more frequently.

But let me ask you. Do you think having ...You're mentioning biochemical weapons or biological agents and how people ...It's become increasingly easy, in a way, to fabricate these or to engineer them. Do you think having iodine tablets and gas masks at home is overkill if you live in a metropolitan area?

Marc Goodman: I guess I would say it depends on your philosophy in life and how you choose to live your life. You were talking about 30 or 40 fire engines for the city of San Francisco. There were nights when I was working with the LAPD on morning watch, midnight to 8:00.

For a precinct that had 400,000 people living in it, we had three police cars on the road, in that precinct. Now we had other guys in other precincts that we could call, but that's three police cars, six guys and gals for 400,000 people. So yes, the thin blue line can be quite thin at times.

I'm always encouraging of people to be prepared, to have a plan, to be cognizant of the threats. Now, you can take that to an extreme. You can say, "I have to have a bunker. I need to live underground. We need to be prepared for nuclear Armageddon." That's not the way that I choose to live my life.

But I think common-sense tools, first-aid kit, having iodine perhaps, opportunity to have tablets too. Make sure that you have access to clean water that's decontaminated and things like that. I think that just is logical. I don't think there's anything over-the-top about that at all.

Tim Ferriss: With international travel ...We're not going to get into necessarily kidnapping and all that, but I want to use this as a ...

Marc Goodman: I have a great kidnapping example.

Tim Ferriss: Well, all right. If you're going to dangle that carrot in front of me, let's go there. No, I want to hear the kidnapping example. Let's do it.

Marc Goodman: Okay. So this is just something that occurred in Mexico City a couple years ago, when smart phones were first starting to come in. The cops in Mexico noticed a phenomenon that was really weird.

So I'm sure this has happened to you. You get off an airplane in another city, and somebody is holding a piece of cardboard with your name on it. You walk up to them. Have you done that?

Tim Ferriss: Right. Yes.

Marc Goodman: Yeah. So guess what? Cardboard can be hacked. Sometimes people lie, and sometimes the person holding the sign is not the person that you expect them to be. So about three years ago, four years ago, in Mexico City, when smart phones first came out, organized crime groups and narcos were hanging out at the Mexico City Airport. With all the signs up that said, "Mr. Smith from Dow Chemicals," and, "Mrs. Jones from ..." whatever the company may be.

The bad guys were sitting there, and they were using their smart phones to Google the people whose names were on the signs and looking for those that they estimated to be of the greatest net worth. Once they figured out who that was, the criminals were going up to the chauffeurs and saying, "Here's 100 pesos. Get out of here, and we'll kill you, or we'll kill you," and they were taking the cardboard sign.

The executive flying in from New York, San Francisco, London would then get off the plane, see the piece of cardboard with their name on it, walk up to the person who also took the ...was dressed like a limousine driver, got into a car, and was kidnapped as a result. There are actually a few people that were killed.

So my point is that most people are very trusting, and they should be. That's the way you want to live life. You want to be happy and think about that stuff. But when everybody thinks like that, those who think differently, for example, criminals, terrorists, and others, it's really easy to subvert the system. Cardboard can be hacked.

Tim Ferriss: Yeah. I hadn't heard that specific example, but that is yet another reason for me to use pseudonyms when using car services.

Marc Goodman: Right.

Tim Ferriss: Which I do, I have done for the last couple years, just because I've had some weird experiences with travel, even though ...This is where the Internet really fucks me because people think ...People can't run publishing numbers. They don't understand book economics. So they think I have like $100 billion, and I'm like, "No, no, no."

Marc Goodman: $100.

Tim Ferriss: Just like, "You got the wrong guy."

Marc Goodman: Right.

Tim Ferriss: God. Yeah, the kidnapping is terrifying. I have known people in Argentina and in other countries who have been kidnapped.

Marc Goodman: Columbia. Brazil. Very, very common.

Tim Ferriss: Yeah, it's extremely common. I know many people who have had family members or friends kidnapped in South and Central America and certainly not exclusive to those places at all. The question I was going to ask you is a segue to virtual attacks. One of the start-ups that I'm close to used to be called Reputation Defender. It's now Reputation.com.

One of the executives there told me that when he travels to China on business, he will use a brand-new, throwaway net book because he does not want any of his data compromised on his hardware. He brings a laptop with him. If someone is traveling ...Let's just say it's a business person. They're traveling to any number of countries, but let's just assume it's China. What are the precautions that they might take to try to prevent any infiltration of their data or sensitive information?

Tim Ferriss: Yeah, that is an awesome, awesome question, and it's one that people don't think about nearly often enough, whether it be an executive from Houston or New York City or those in Silicon Valley. Obviously business will take them to the most populous nation on Earth, the People's Republic of China.

There, the rules are very different in terms of what the so-called police can do and how they will treat you and your technology. So all I would say is if you're going over there for business, pay close attention. The fact of the matter is their screening of you begins when you fill out your visa application. Right? Nothing there is random.

So why do you have to do a visa application? Because they want to know who you are and if you're interesting. If you're Andy Grove from Intel, traveling into China, they're going to pay attention to you.

I'll give you one simple example, and this was reported several years ago. Andy Grove, the former chairman of Intel, actually took a flight into Beijing. He gave a lecture before 1000 people and presented from his laptop. After his presentation was over, two very young, pretty Chinese women approached him, and they were ever-so subtly just moving their own bodies to get him to turn away from his own laptop.

He had a lovely conversation. When he turned around, his laptop was gone. Now, the big mistake in that particular case is not that he brought a laptop, per se, but as the chairman of Intel, he actually had the designs for one of the latest

Pentium chips, some extremely valuable intellectual property on the computer that disappeared along with the laptop.

So my general rule of thumb is laptops, net books, whatever they are, they're just a couple hundred bucks today. If you can afford a trip to China, you should be able to afford a laptop. You can bring a dummy phone with you.

Just to give you an idea of some of the information that leaks, the minute you connect to a hotel in potentially-hostile territory, whether it be Iran, China, whatever country you're traveling to, they have the ability to insert Malware onto both your phone and your computer, the minute your device connects to their network.

So you know when you have to log into the hotel webpage to pay? That's when the handshake takes place, and that's when your device gets infected. So that's step one. If you go ahead and leave your laptop in any hotel safe, routinely the hotel security gives access to the local police. So they all know the combinations, and anybody can open up one of those saves incredibly easily.

So what I would recommend is, if you bring technology, carry it on you if you want to hold onto it. I would limit the amount of information you put on it. I would certainly consider what we call a throwaway laptop or mobile phone. I would make sure that those devices were encrypted. If you know you're going to call 10 people when you're over there, have those 10 phone numbers and don't walk out there with all of your contacts, with your business plans, with your sales figures.

The thing that mostly the Chinese are interested in, besides intellectual property, is they're very aggressive about being helpful to their state-backed industry. So if you're over there as an American businessman or woman or regardless of what country you're from, and you're negotiating a deal with the Chinese, they'll be very careful about monitoring your email, what you're doing, and any negotiations that you may be having with your counterparts from your own company in the United States, whether it be your general council, the head of sales.

They're going to take that information and feed it to their Chinese equivalent in order to do that. In fact, there was a case that I mentioned in the book, where an executive from Coca-Cola got fished with a spear-fishing email. They were in a multibillion-dollar deal with a Chinese beverage, state-sponsored Chinese beverage company.

They were under bid and lost out. So one fishing email to the right executive, crafted in the right way, infected the computer, and then the deal was done. Billions of dollars were lost.

Tim Ferriss: Wow. So the fishing email was something like ...Whatever it might be. Your account is overdrawn from the Bank of America.

Marc Goodman: Yeah, here's an important tip. Yeah.

Tim Ferriss: Click here to confirm your blah, blah, blah.

Marc Goodman: Exactly. If I could just give one general tip, something to keep in mind ...I don't know everybody that's going to listen to your podcast, but I'm going to postulate that most of your listeners actually do not know a prince in Nigeria. If you get an email from a prince in Nigeria, do not click on it. He's not your friend. He doesn't know you.

Tim Ferriss: Yeah, very good advice, very, very good advice. Yeah, the opportunity cost of missing the real email from the prince in Nigeria, pretty low when you look at the probabilities.

Marc Goodman: Yeah, but you hit on something major right there, which is actually that is one of the major causes of infections to people's computers, is that they're clicking on the wrong link. In the old days, you used to be able to tell a fishing email because they used bad English, bad grammar. Now, they're perfectly well-crafted. A spear-fishing email, targeting a specific individual or executive, is even more so.

So you have to be really careful. Basically my general rule of thumb is don't click on links. If people send me a link, I'll call them and say, "Hey. Did you send this to me?" They think I'm crazy, but I don't click on links.

Tim Ferriss: Yeah. Well, ditto for attachments, which can be ...

Marc Goodman: Right. Exactly.

Tim Ferriss: ...executable files. All right. Okay. So I'm going to ask about an edge case because I love asking these absurd or extreme questions. But if someone has a nearly unlimited or unlimited budget ...Let's just say it's a hedge fund manager who's worth a billion dollars-plus. You were their personal security consultant. You can interpret that any way you'd like. Security/Armageddon-proofing consultant. What are some of the things you would have them do?

Marc Goodman: I would have them hire a guy who didn't discuss their security plan on a podcast with Tim Ferriss, my first piece of advice.

Tim Ferriss: Right. Good advice.

Marc Goodman: Don't do that. Generally speaking, every person you work with is unique and different. So I work with a lot of folks of high net worth in a lot of the general public corporations. The advice is very specific on what people's threats are. So for some people, the biggest threat to a hedge fund manager may be that their son or daughter is addicted to meth, and that's bringing all types of other people into their home that causes them difficulty.

In others, it may be some of their personal proclivities, things that they're looking for online that could be personally embarrassing, mistresses, extramarital affairs, all of that type of stuff. So those are the general things that you look at. Then you work up a threat profile. That's something that I find that most individuals don't do, and certainly most corporations don't do.

The fact of the matter is, in the same way that hackers are using the Internet to gather lots of information about their targets, you yourself can go out there and use tools. You talked about Reputation.com and others, but there are lots of tools out there that will allow people to get really good open source information on themselves and the threats against them.

That's one of the key steps that I always mention to my corporate clients, is that they need to go ahead and implement an open source intelligence program because if you are working on a secret project ...Let's say it's the latest iPhone, or you're working on the latest version of Android, something that you don't want people to know about.

If you got your search engines up and running, and you start seeing people talking about it, or sales lists are leaking out there, or employees resumes are out there, showing that they're about to jump to the competition, there's just a lot of stuff that you can detect.

The other point that I tell them is, and most people don't realize this, is make sure that you're looking in the digital underground. So most people think when they search Google, they're searching the Internet. When you're searching Google, in reality, you're only searching about .03% of all the available electronic information stored on the planet.

Tim Ferriss: So how do you go about searching the digital underground?

Marc Goodman: You have to go underground. The quickest way to do it, one of the ways people do it, is by using Tor, The Onion Router.

Tim Ferriss: Right.

Marc Goodman: So that's a specialized piece of software, actually produced by the US Navy. It was meant originally to help democracy and human rights activists overseas bypass their national firewalls, whether in China or Iran, so that they could get around to communicating. It was very useful for their personal safety.

There's a million great reasons why you would use Tor. Again, in the wake of Snowden, if you wanted to go ahead and have good encryption of the information you're looking for, then Tore is a great useful tool for that, with some noted limitations.

But the other side of that is that there's something called Tore Hidden Services. If you're running this particular piece of software, you can now get access to a whole world that you don't know exists. So this is where hackers, and terrorists, and hacktivists, and spy agencies, and law enforcement hang out. So I'm sure you will be familiar with the Silk Road and what went on in that case.

Tim Ferriss: Sure.

Marc Goodman: It broke very close to you in San Francisco. The fact of the matter is Drug Pirate Roberts, the alleged person who was running that, had the largest drug website in the world. Whether or not you like drugs or not and whatever your position may be, a National Institute of Health drug abuse agency studies that at some point, 20% of all narcotics purchased in the United States transited the Silk Road.

Tim Ferriss: Wow. I had no idea the number was so big.

Marc Goodman: The money that Drug Pirate Roberts brought in in those 30 months was $1.2 billion. So $1.2 billion on 30 months of methamphetamine, AK-47s, uzi's, child pornography, fake passports, whatever you're looking for. You could buy it there. Because Silk Road operated kind of like eBay, where the house took a cut of everything they sold, Drug Pirate Roberts is alleged to have amassed a personal fortune of $110 million.

So let's say you're a 28-year-old entrepreneur, and kids don't do this out there, but if you're a 28-year-old entrepreneur, going from zero to $1.2 billion in 30 months ...He had a relatively successful exit, except for the life imprisonment he's facing. But other than that, he had a pretty good gig.

Tim Ferriss: Right. The rather punishing asterisk on the income statement.

Marc Goodman: Yes. Exactly.

Tim Ferriss: Yeah. Comes with free imprisonment for life.

Marc Goodman: Exactly. Free prison companions.

Tim Ferriss: Yeah. Oh, God. So you mentioned drugs. I want to chat about that for a second, because I've heard you mention, and maybe you can elaborate on drug production. So this is something that I'm very fascinated by. I think drugs is a bit of a ...In the Nancy Reagan, "Say no to drugs," sense, it's a bit broad. I think a lot gets mixed into this so-called war on drugs that shouldn't be part of it at all, and a lot of good therapeutic agents get disregarded and blah, blah, blah.

The point being, when you look at just some of the real cash cows, if you look at the opiates. You look at heroin. You look at cocaine. Marijuana is a very interesting case. We won't get too far into that, but just the sort of decriminalization of marijuana is really fascinating.

Marc Goodman: Isn't its use mandatory in San Francisco? I believe.

Tim Ferriss: It's pretty close.

Marc Goodman: If you go to Delores Park, you, by law, yes, are required to be using Marijuana.

Tim Ferriss: Yeah, if you stub your toe, and therefore have chronic pain, you can get ...

Marc Goodman: You're permanently disabled. Yes. Now you need marijuana.

Tim Ferriss: But I've heard, and I haven't verified this, but there are poppy fields, even within some national parks in the US, that are policed by Mexican narcos, and you have to be careful even as a hiker in some cases, if you go too far off the beaten path. Is that going to change? In so much as, will drugs ...The example that you used was involving yeast to synthetically produce cocaine, or not synthetically perhaps, but I guess it would be synthetically, produce cocaine or other drugs like that. Are these fields? Is that entire production chain and all the shipment ...Is that just going to go away?

Marc Goodman: Yeah, so you've hit on a really, really interesting point, which is in the same way that Apple can go ahead and disrupt Microsoft, and Google can disrupt somebody else, the fact of the matter is that the old-school original gangsters and narco dealers are going to be faced with some challenges to their business model from a new generation of joke dealers. It's going to be really fascinating.

So to your point, when you think about what is required for the production of cocaine today or heroin, you need these massive fields of coca leaves and marijuana plants or poppy plants, et cetera. That is really tough for the dope dealers. A, they're expensive to main. They have a very huge footprint, in terms of hectares and hectares of fields that need to be maintained. They're easy for law enforcement to detect.

So now, thanks to synthetic biology, one of the amazing things that you can do is, because all of those marijuana, poppy, or coca plants are all naturally-occurring substances that contain DNA, you can actually go in and sequence cocaine plants or poppy seed or any of those things. From that, deduce the genetic code for coco.

You can go further in and say, "Well, what's the active ingredient here?" You can isolate that, and you can snip that part of the plant or the active ingredient, and you can insert it into yeast. Then you can grow those yeasts, and you could bake bread with it, and you could make beer with it.

So we're not quite there yet, but all of these things are very close on the horizon. It completely breaks our current global security model around narcotics because, again, we have these big fields. We look for these big fields, and we have dope-sniffing dogs when you arrive at the airport or going through customs and immigration, but they're not going to smell a loaf of bread that is just as powerful as cocaine.

So there's some really interesting opportunities there moving forward. It's going to make for some really interesting beer and bread in the future.

Tim Ferriss: Is it conceivable ...Now I'm going to really go off the deep end, into my sort of detective novel mode. Is it conceivable that the US government could decide that it would be pragmatic to, in some way, seed people domestically with technology to, in a very decentralized way, produce, meaning synthesize, cocaine, heroin, et cetera, to disrupt the incentives and finances of, say, cartels, who are shuttling drugs from ...I know the Mexican cartels are now, as far south as Columbia where I've spent some time, it's very, very prevalent.

Marc Goodman: Right. Right.

Tim Ferriss: Basically in a way to reduce violence and disrupt that chain, do you think there's any conceivable scenario in which the government or some facet of law enforcement would decide that that type of ...Even the introduction of that type of production would either be done deliberately or have a blind eye cast to it, for the tradeoff, which is disrupting the immensely violent and problematic influence of the cartels in Mexico.

Marc Goodman: Yeah, you're asking for a particularly interesting public policy and political question. There are plenty of folks who are advocating for this. There's a great talk by a gentleman called Ethan Nadlemann, who I just saw speak down at TED Global, who really gives a very powerful and compelling talk for why drugs should be legalized. You can Google that and find his talk.

We're kind of seeing the beginnings of that now with marijuana. There are other countries, like the Netherlands, that have allowed people to be on heroin for years and put them on methadone. So there have been lots of different experiments around this. I would say I don't know that the public policy, and more importantly the politics around this, is there yet but you can certainly look at the costs of what it is doing to our society, particularly here in the United States.

We have the largest incarcerated population in the world. I think there are something like 3 million people that are somehow in the criminal justice system, at state pen or at the local level, in federal penitentiaries. So the costs of maintaining that ...Most of those folks are there for drugs, one way or the other. So there's certainly an economic cause to be put forth.

Again, I'd refer you to Ethan Nadlemann, who makes that way better than I can. I don't know that the government, any time soon, is going to see this more as a public health issue and focus on demand reduction. Right now, public policy in the United States has been heavily geared towards supply reduction. So let's go ahead and drop napalm on cocaine fields in Columbia, and that'll solve it.

Of course, as the people in Latin America, the Mexican president and others, have mentioned, "Well, don't blame us. You guys are the ones that want to buy it." So it's really complex. Right? How this works ...I will mention that the narcos are all over the drug trade, all over the technology space in really amazing ways.

So narcos are using robots. They're flying drones. They've got drug subs. There are now quadcopter drones and octacopter drones that can carry like 1000-kilo loads of cocaine and marijuana across the Mexican-American border. We're starting to see 2000 tons carried by remote-controlled narco subs.

Some of the Columbian cartels literally have an R&D budget. So the cocaine cartels in Columbia have like $5 million allocated to R&D for robotics, because the day that they can launch autonomous subs against North America, they've hit pay dirt. So we're seeing that.

The money and the subs are involved. We were talking earlier about how clever terrorists may or may not be. You should look at the sophistication among the narcos. The money that they have allows them to bring in tremendous talent. El Chapo Joaquín Guzmán who ran the Sinaloa Cartel was recently arrested in Mexico.

At the time of his arrest, he had a room in his mansion, a cash room, with $200 million in cash, just sitting in his house. We call that the Tim Ferriss room, obviously, for obvious reasons. He was actually listed at number one on the Forbes Wealthiest List, ahead of Oprah and French president Sarkozy. Right? So the amount of money ...

By the way, to put $200 million in perspective, Interpol's annual budget is $90 million.

Tim Ferriss: Wow. So if you were a sports team, you would bet on that sports team against Interpol in a heart beat.

Marc Goodman: It would seem to be the wiser bet. Yes.

Tim Ferriss: In terms of talent recruitment, he should have a number of incentives to use. I will kill you, or you work for me.

Marc Goodman: Yes. Exactly.

Tim Ferriss: Or I will give you twice as much as anyone else, any other law enforcement agency, or at least Interpol, can pay you.

Marc Goodman: By the way, that's exactly happening right now. We're kind of joking about what's going on with the narco wars in Mexico, but there have been 50,000 innocent Mexican citizens, nationals, that have been slayed in the past six years. So just south of our border, 50,000 people ...Right? More than live in Palo Alto or the suburb of New York, have been murdered.

So there's a massive war going on between the people. We talked about crowd sourcing before. There's a ton of incredibly brave Mexican citizens who are actually crowd sourcing the location and activities of the narcos. They're using open source tools, like Google Maps, to report dope dealers and bring that information forward. The dope dealers have gotten hip to that and have now actually gone ahead and killed off a bunch of these citizen reporters.

So to protect themselves now, those guys are using encryption. The narcos have gone out there and actually kidnapped hackers. They've kidnapped top hackers off the street and brought them back to their headquarters and say, "Hey. You decrypt this, or I'm going to kill you."

The payback, once somebody is identified as being a potential snitch for the narcos, have been draconian. It's kind of gross, and you can edit this out if need be, but to make their point, some of the narcos have gone ahead and kidnapped some of these folks who are using tools like Google Maps to crowd source what was going on with the drug dealers and their activities, kidnap them, and killed them, and decapitated them and taken their heads and brought them to the central square of the town, like right in front of the church when everybody shows up on Sunday morning.

They took two computer keyboards, put them in the town square in front of the church that everybody shows up at, with the head, the human head of the snitch, right there with a note in big letters that said, "This is what happens to rats."

Tim Ferriss: Horrifying, of course. The number that I have so much trouble grasping is 50,000. It's so many people. How does that break down? If you're looking at the pie chart of reasons for these deaths, how many of them are snitches? What percentage versus stray bullets and just collateral damage versus shock-and-awe campaigns to instill fear and terror into entire cities into compliance? Because I've read these stories of, say, 20 or 50 students being killed and decapitated.

Marc Goodman: Right. We had that right now in the past couple of weeks.

Tim Ferriss: Right.

Marc Goodman: We've had all these innocent high school students who were just murdered, allegedly by the mayor and the police in the town. So I can make up a story, but I don't know the exact breakdown of what it is. My gut tells me, based upon whatever I read in research, that brought me ...There's some percentage of this that is drug dealer-on-drug dealer violence, so one cartel fighting with another.

The others are people that won't go along with the narcos and what they are up against and what they want to do. So they get taken out. Law enforcement officers get taken out. Then there's just a tremendous number of casualties when the trucks come through the little town, and everybody is shooting AKs and M-16s. Five-year-olds get gunned down as kind of collateral damage.

Tim Ferriss: Man, good to count our blessings when you don't have to contend with that on a regular basis or an any-time basis. It's really horrifying. To just maybe project forward a bit ...I'm not sure if it's projecting forward that far, in fact, but artificial intelligence.

There are a lot of differing opinions on this. But what are the threats, if any, of artificial intelligence? And where are things now versus where you think they might be?

Marc Goodman: That is a great question. It's actually very much in the news today. Elon Musk, and I quote him in my book, talks about the threat from AI being greater than nucs. Stephen Hawking actually put an op-ed in the Independent in London about a month or two ago, where he was very cautious about widespread adoption of AI.

Just for folks who aren't particularly familiar with AI, there are generally two types. There's the narrow AI. That's the artificial intelligence that goes ahead and puts a recommendation for you out there on Netflix or Amazon about what book you might like. If you enjoyed this movie, you might like this movie.

So that kind of narrow AI is widespread and ubiquitous. It's AI that allows you to talk to American Airlines while you're on hold. We're seeing that every place. Then there's the broader, more widespread AI, which is kind of artificial general intelligence. That's this kind of AI that people fear will run the planet.

There are some concerns about both. Broadly speaking, we all saw ...Most of us may have seen the television episode for a Jeopardy, when IBM's Watson was playing. Did you happen to catch that?

Tim Ferriss: I didn't personally see it.

Marc Goodman: So IBM built this computer called Watson, and it's doing a narrow AI. It played against the top, top Jeopardy champs and just kicked their butts. Right? So this big computer with a funny voice, called Watson, was able to beat the best champions in the world at Jeopardy. Before that, we had our greatest chess champions being beaten by computer.

But the question that people don't realize or don't often ask themselves is, "What would happen if Watson turned to a life of crime?" Right? How much healthcare fraud could Watson commit? How much identity theft could Watson commit? The fact of the matter is that day in and day out, we are turning over more and more of our lives to algorithms.

People worry about individual bits of data being stolen, but that's kind of a low-level threat. Of course, that's happening. The bigger threat is having our algorithm hacked. Algorithms are very complex mathematical formulae that go out there and carry out everything from the anti-brake system in your car to the GPS navigation used by aircraft around the world, to all the trading on the stock floors. Those are all algorithms.

We've seen a couple of really crazy, wacky things going on in the world of algorithms that look like market manipulation. The challenge is that Moore's Law applies to criminals as well. The big paradigm shift in crime has been as a result of algorithmic programming.

So in the book, I talk about the fact that the old paradigm of crime is you get a bad guy. He goes out and buys a knife or gun, hides in a dark alley, and says, "Stick them up." Right? That was a good business. You could be your own boss, set your own hours, start-up costs were low.

But Tim, you know this better than anybody else. What was his problem?

Tim Ferriss: Didn't scale.

Marc Goodman: How do you scale your business? Right? That was tough for a criminal.

Tim Ferriss: Two arms. Two guns.

Marc Goodman: Exactly. Everybody you robbed might shoot back and kill you.

Tim Ferriss: Right.

Marc Goodman: So technology came along that actually improved upon that business model, and the technology was the locomotive. Now, rather than robbing one person at a time, we could rob 200 people at a time. When they created trains, nobody thought about that, but of course that was a consequence.

Fast-forward to today to the days of the Internet, and we've had hacks like at Target and the Sony Playstation hack before that, where 100 million people were simultaneously victims of a crime. In the Target hack, one-third of all Americans were affected by that.

So if you talk about exponentials, we've gone from criminals robbing one person to one single, lone individual being able to rob 100 million people. That is a complete paradigm shift in crime. Because it's exponential, it's only going to grow.

So, my big fear and concern that I write about in "Future Crimes," the book, is the fact that our systems of justice and law and order and public safety are all deeply, deeply linear. Yet, the threat is entirely exponential. We're seeing criminals use algorithms.

You know why you can rob 100 million people? Because computer crime has been reduced to an algorithm. The old days ...I talked about the movie "War Games" earlier. The old day was you'd have the high school kid with the bag of Doritos and Monster or Red Bull, sitting at his computer, hacking away at all hours.

You don't need to do that anymore. You can write scripts that carry out crime. You have heard of software as a service. Guess what? There's crime as a service. You can actually go out there and buy programs like Black Shades and others that will go out there and commit crime for you.

So when a computer program can do the identity theft, can do the denial of service attacks, can do that for you, it can run in the background 24/7, 365 days a year to carry out that crime. That's why it scales, and that's why the profits are so high.

A lot of the principles in the Four-Hour Work Week have been implemented by organized crime. I'm not saying they read your book, but I'm saying that the logic that you developed and a lot of this ...People are seeing that. So now we have fully automated crime. That's algorithms that are carrying it out and AI.

Tim Ferriss: Yeah. These principles ...Whenever you look at principles for effectiveness and efficiency or scaling or building an organization, they can of course cut both ways. They can be used as a surgical tool to do good things. It can be used to decapitate people, metaphorically or physically even.

Marc Goodman: That's an important point I'd love to make. I'm not saying, "By the way, technology is bad." I, like you, live in Silicon Valley. I'm a huge proponent of technology. It has the opportunity to bring tremendous abundance and positive good to the world.

But as you mentioned, whether it be ...A knife can be used by a surgeon to heal or by a criminal to kill. It's just about how we use it.

Tim Ferriss: Absolutely. I'd love to chat. I know we're probably going to be wrapping up pretty soon, but I wanted to ask you just about what can be done. So let's assume that the people listening are, for the most part, not going to feel compelled to dig a spider hole in their backyard because they're afraid the black helicopters are going to come for them, and they're going to fight off the US government with their stash of hand guns.

Marc Goodman: Right.

Tim Ferriss: Let's just assume that that's not who we're talking to, primarily. But for people who are like, "All right. I'm busy. I've got a little bit of money. I'm well-educated. I'm very worried about doing stupid things that compromise me." What are a handful of simple steps that they should take or might consider taking to decrease the odds of bad things happening?

Marc Goodman: Sure. I can throw out some tips for individuals, and then some for start-ups and companies. So on the individual front, common sense is actually not so common. The number of people that will click on links and open attachments is really high.

As a really strong piece of advice, just don't do that. It's really bad cyber hygiene. I talk about the concept of cyber hygiene and the idea of keeping yourself clean. If you think about sexually transmitted diseases, if you're not clean, you transmit it to other people.

The same is true with our computers. So don't do that. Another thing that you can do is make sure that your computer or your mobile phone is constantly up to date. Have you ever been sitting in front of your computer when you get a little notification like, "Hey. There's a new update to Windows, or there's a new update to IOS or something like that." Have you come across those?

Tim Ferriss: Sure. Yeah, I get notifications all the time.

Marc Goodman: Right. So what that isn't saying ...It sounds really nice when they say, "Oh, there's an update." What it really means is our software has been riddled with security holes for the past six months, since the previous update, and we're now finally fixing them. So there's the flip side of that.

I would say always make sure that your software is up do date, across all of your devices. Keep that updated. Another thing you can do ...I am not a fan of single sign-on and using the same password to log onto all your services. The challenge with that is if your account at Target gets hacked, and you use your same Target email and login across multiple sites, now the bad guys, and they do routinely do this ...Once they get 100 million accounts from Target, they're taking your Target name and password, and they're trying it at Bank of America and Citibank, and they're trying to get on Facebook and Google.

So if you have ...You should definitely have a different name and password for all of your sites. Now, I know people will say to me, "Oh, great, Marc. How am I going to remember 300 passwords?" This one wants a capital letter, and this one wants the name of my favorite child actress. It's all too complex.

There are a number of pieces of software out there called password managers or password wallets that I recommend. You have to use some caution because ...Guess what. Organized crime have created their own versions of those. So they'll upload something, and it's like, "Super number one best password program," and get it into the Android Play Star. Tens of thousands of people download it, and of course, your passwords are just being fed to organized crime in the background.

So I recommend One Password. There's another one called Last Pass, which is quite good. Then there's Kee Pass, K-E-E-, P-A-S-S, which is an open source version. So definitely do not use the same password.

If you're in a public space, always make sure that you use a VPN, a virtual private network. This way, any of the information that is transiting from your computer to the Internet is encrypted from that point to point. If you're not, and you're sitting at a local Starbucks, I can go ahead and just, because we're on the same network, see everything you're doing on your computer.

There was a hack a few years ago, called Fire Sheep, where I could steal your Facebook session cookie and log in as you and post things to your Facebook account, just because we were on the same network. You didn't need to be sophisticated. Actually it was just a browse-in for a Firefox browser that allowed me to hack. So the tools of hacking are becoming particularly easy to use.

So if you do those things, if you maintain your site, if you go ahead and constantly update them and use password managers, you can actually avoid 85% of the threats out there. So you can make a massive, massive difference.

The last one that I tell people, that most folks don't consider, is do not use the admin account from your own computer as your primary account. So if you have on your computer a Tim Ferriss account, that account should not have administrative privileges.

You should have a primary account which is administrative privileges, and the one that you use day in and day out should be a user account with degraded, non-administrative privileges. Why would you do that? Because if you clicked on the email from the Nigerian prince by accident and get your computer infected, if you're already logged in under an admin account, then that code needs no further permissions to go ahead and infect you and to get onto your machine.

But if you're on a user account, and you get that infection, in order to change the system files, it will ask you to enter in your password, which would be a good clue that you've been hacked.

Tim Ferriss: Got it. Okay. So you're talking about for the computer access, the local computer access.

Marc Goodman: Correct. Yeah.

Tim Ferriss: Got it.

Marc Goodman: If you're logged onto your personal MacBook Air or a Windows machine or a Samsung machine, whatever it is, your laptop, your home computer, it's really wise to never run it as an administrator.

Tim Ferriss: Got it. No, that makes sense. Just to add to your password recommendation, which I think is a smart one, whether it's one password, less, or otherwise, is enabling two-step authentication.

Marc Goodman: Excellent.

Tim Ferriss: It's really a good idea for Gmail, for Facebook, for any account that you can, to enable two-step authentication. For those people listening that don't know what that is, it's usually within settings somewhere. All that means is if you or someone else tries to log in to your Gmail account from an unrecognized computer, it's going to shoot you typically, very often, a text to your cell phone with a pass key that you need to enter in order to then enter your password. So it's just another barrier, so to speak.

Marc Goodman: Yeah, that's a great piece of advice.

Tim Ferriss: What about ...So with the start-ups, are there any other pieces of advice you would have, low-hanging fruit for those folks?

Marc Goodman: Well, for the folks that are working in the start-up world, and I advise a lot of different start-ups, as I know you do. They're running around crazy, trying to get their beta out there. They want to ship their code, whatever their product is. So probably the very last thing on their list is security. They don't think about it.

So for a company, you need to think about these issues. Right? Because all you have is your intellectual property. There are actually companies out there that specialize. The minute Facebook is launched, they create the German version of Facebook. They create the Chinese version of eBay.

So ripping off your IP is very much what they do. So both for start-ups and particularly for larger corporations, one thing I often suggest is you need to be keenly aware of what's going on with your competition and with your own company. So that goes back to implementing an open source intelligence program.

You also need to have somebody who's in charge of your security and kind of thinks with a more of a conspirial mindset that you and I seem to have in talking about this stuff and figuring out what can go wrong, because most people are good people. They don't think like bad guys. Right?

I've put handcuffs on bad guys for 20 years all over the world. I know how they think. So if you're not trained in that, it's not at all obvious. It's also important to realize that not everything needs to go into a computer. Both Coca-Cola and Kentucky Fried Chicken, KFC, the secret recipes for their food is not in any electronic system and be retrieved. It's air-gapped, written down on a piece of paper.

So if it's really important, think about that. We talked about some of the travel tips earlier. The last thing that I would mention is to red team and test your assumptions. Red team is a term from the military. You kind of have the blue team and the red team. The blue team is the United States. The red team is always the bad guys.

The military trains this way, where they use sets of bad guys to try to break their stuff. I can guarantee you that if you're doing anything interesting on the Internet or in your personal life, there's somebody who's trying to get access to it. It may not be an individual hacker, sitting at a keyboard, targeting you. Because as I mentioned earlier, a lot of these attacks can be scripted.

The thing I hear all the time is, "I've got nothing to hide. I've got nothing to lose." Then you don't lead a very interesting life if that's the case. I would think we all have something at risk here. So you should be testing those assumptions. Because if you're not trying to hack yourself, the bad guys are. So better that you uncover those threats first.

Tim Ferriss: No, definitely. Just to your point, there are some real hot beds, I think. I want to say Estonia, for some reason, but it might be Bratislava, somewhere out in that neck of the woods. There are entire cottage industries that have popped up.

Marc Goodman: In Romania, they have that for sure. Yeah.

Tim Ferriss: Romania. That's what it was. That's what it was. Romania.

Marc Goodman: Yep. Yep. It's actually called the cyber crime headquarters of the world. It's very funny. They have something like 500 people in this village, but that one Western Union office in Romania does more than most of western Europe, because of all the illegal cyber crime payments coming in there.

In Nigeria, they have what are called the Yahoo Boys. These are the ones that send out all of those emails, trying to trick you. So yeah, there's definitely a very vibrant cyber crime economy out there. A study by McAfee and CSIS, a think tank in DC, estimated the global cyber economy at $400 billion a year. It's tremendous.

Tim Ferriss: That is so wild. Yeah, and growing, no doubt about it. Well, I think this is a good round one for us. I'm already looking for round two. So I think this is a good introduction for folks, gives them plenty to think about. Okay. Here's one for you. Do you have any habits that might be non-obvious to people or habits you think improve your security or give you peace of mind that other people find odd?

Marc Goodman: One that I get commented on all the time is ...If you look at any of my devices, whether it be my cell phone, my laptop, or my computers at home, they all have yellow stickies over the camera. The fact of the matter is that not only can people hack your camera, but they can hack it in a way such that the little green or red light isn't on.

There's malware out there that does this really easily. I mentioned Black Shades earlier. That will do that. There was a girl called Cassidy Wolf, who was Miss Teen America. She went ahead and had her camera taken over, ultimately we found out by one of her classmates. She clicked on an infected email, and Miss Teen America, 17-year-old girl, was coming out of her own bathroom after taking a shower. Her laptop was open. This creep was going ahead and surreptitiously filming her and taking the video and then blackmailed her and said, "Hey. If you don't do specific sex acts for me in front of the video, I'm going to release all this stuff live."

So unlike Teen America, people are not lining up to see me naked, but I still go ahead and cover up the video camera. It's super cheap to do, and it's just something to keep in mind.

Tim Ferriss: So funny you mention that. I have masking tape over my camera on my laptop right now because I was hanging out with a buddy of mine who, in a previous life, got in a lot of trouble with the FBI for hacking. He is a world-class hacker.

If you want to talk about a very competent red team, he now gets paid by companies to do that, to try and beat their systems, which he usually does successfully.

He said, "You know, you might want to put some tape on that." I was like, "What are you talking about?" He's like, "Well, if I wanted to hijack your computer and videotape you, I could do it pretty easily." I was like, "Okay. Say no more."

Marc Goodman: Right.

Tim Ferriss: I've actually heard of business travelers who have been blackmailed very similarly, usually female travelers who have had people attach cameras to their hotel peep holes, from the opposite side.

Marc Goodman: Absolutely.

Tim Ferriss: So business travelers ...There's some business travelers I know who will similarly cover up that keyhole so that people cannot surveil them.

Marc Goodman: Absolutely. Talking about cameras, I mentioned earlier that everything is becoming software or hardware, and cameras are a perfect example of that. We all go ahead and have cameras around us, not just on our cell phones or on our laptops, but everywhere we go. Right? There are now cameras at the dry cleaners, cameras at the bakery, cameras at the ATMs.

All of those cameras are connected to the Internet, and they're all hackable. Some crazy number, like 30% to 40% of all camera systems have absolutely no password. Another 30% or 40% have the admin password that's written in the manual that's available on PDF on the Internet, if you Google the name of the camera system.

So that means they're widely available to be hacked. Yet, people use things like baby monitors, nanny cams, things like that to protect themselves and were finding that they're just easy marks. Within the past week actually, here in late October, we had an incident where it was reported that 76,000 camera systems had been compromised and were being live-streamed to the web.

So you could log in, because all of these cameras had been hacked and easily taken over, and you could see women sitting on the couch. You could see people in their bedroom, having sex. You could see mothers breast-feeding their kids, people sitting in dry cleaners, cooking stuff at bakeries.

So we think these systems are there to protect us. But in fact, they can be compromised and used in really interesting ways. If you have time, I'll tell you another funny story about that.

Tim Ferriss: I have time.

Marc Goodman: Awesome. There was a case called the Crown Casino in Melbourne, Australia. This happened about a year ago. A man comes in and starts playing poker, and he's doing really, really well. He ends up playing for two days, almost straight. He walks away from the Crown Casino in Melbourne, Australia with $33 million, playing poker.

Gets back on a plane and flies back to his home country in Asia. What the hell happened? Because the casino got cleaned out. They had no idea. They ended up looking at it, and it turns out that he was part of a hacker team that went ahead and hacked the security cameras in casinos.

All casinos have a ton of cameras. The hackers that were working with this guy had given him an earpiece. So by having commandeered the casino's own security system, they could see perfectly clearly what the dealer's cards were and the players of all the different players at the table. They were basically, via electronic messaging to his ear, telling him, "Stay pat. Hold. Double down," all of that stuff.

In just 48 hours, $33 million. So the cameras that are meant to protect us, if they're not locked down and encrypted, can definitely be used against us.

Tim Ferriss: Wow. Yeah, good luck extraditing that guy.

Marc Goodman: Exactly.

Tim Ferriss: Oh, man.

Marc Goodman: He can now afford a good defense.

Tim Ferriss: Yeah, I bet. Wow. Well, there's so much more to talk about, but I will certainly look forward to some following conversations. Maybe we'll inject some wine into the mix to make things more rambunctious. Since I know we're practically neighbors ...

Marc Goodman: Yeah.

Tim Ferriss: Even though we're doing this virtually ...

Marc Goodman: I would love to meet you in person some day and hang out again.

Tim Ferriss: Likewise. The recommendation I make to folks is go to Futurecrimes.com. Check this out. Marc did me a very big favor by coming on the show early for you guys. Do me the favor. The book is very inexpensive. It's going to be spectacular. Pre-order the book. So it'll take two seconds. Grab it on Amazon or wherever. Futurecrimes.com. Check it out.

Definitely take a look at his TED talk. Where else should or can they find you, Marc?

Marc Goodman: I'm at Singularity University. So I teach there. We have a bunch of great executive programs. Other than that, on a plane somewhere, traveling the world.

Tim Ferriss: So Singularity University is fascinating, guys. If you really want to train yourself to think about exponentially growing technologies in a new way, to expand your mind, I can guarantee that Singularity U will help. That's what it is on the web, Singularityu.org. You can take a look at everything there.

I will also include links to various resources and books and whatnot that we mentioned in this episode, as well as Future Crimes in the show notes for those of you listening who want to simply find the one-stop shopping for everything we talked about. Go to Fourhourworkweek.com/podcast, all spelled out. Marc, until next time, thanks so much for taking the time. This was a blast.

Marc Goodman: This was awesome, Tim. Thank you so much.