TECHNOCULTURE

Cybersecurity

Episode 26

Full transcript

Guest: Patrick Wheeler [Patrick]
Host: Federica Bressan [Federica]

[Federica]: Welcome to a new episode of Technoculture. I'm your host, Federica Bressan, and today my guest is Patrick Wheeler, co-founder of CyberWayFinder, a training programme in cybersecurity and an expert with over twenty years of experience in cybersecurity and technology. Welcome Patrick.

[Patrick]: Thank you very much, its a pleasure to meet you Federica.

[Federica]: I would like to start with the term cybersecurity. It has a very fancy ring to it, but it's also scary in that it seems something very complicated only for experts, for tech people, for nerds. So can you give a definition of cybersecurity and say if it is: a niche just for experts, or if it's a societal issue that concerns all of us, so in a way we should all be literate in cybersecurity, if anything to some extent.

[Patrick]: So, first I would like to say very clearly that it is a social issue that concerns everyone. When we look at cybersecurity today, this is everything from Facebook hacking, Twitter bots, social engineering of election processes; this is everything from that, through the traditional definition of cybersecurity or information security. So, if you will, a lot of the perception of information security grew out of the corporate or governmental networks, where we had these new things called computers, and then very early on we found out that people were breaking into these computers. Computers came out, and the internet came out, in a lot of the scientific and the academia, and these are very open societies that encourage collaboration, and encourage - literally - hacking. The origin of the word‘hacking’ was a very positive thing; it meant somebody who took something that had been constructed by somebody else, decomposed it into its component parts and rebuilt something new and exciting out of it. So in many ways, our initial computer systems are insecure by design, and so when we bring the technoculture - and that's why I love to talk with you and I love your podcast - is that... as we bring our society into the cyber-context, the things that we bring with us are the same things that have always been with us as humanity: Both the exciting and fabulous things that we can create, the new ideas that we can put together, but also the bad things. We bring with us pedophilia, terrorism, intrusion, spying, manipulation, thief... the thievery. So this is something that we've brought with us into the digital context. The big difference that we find in technology systems is that you can't visibly see the lock on the door. So what I argue is that cybersecurity, information security, is the same thing as other types of security within society; it is just with the concept of space, dis-intermediated - if you want to be fancy - or just space and geography are no longer relevant, meaning that you can be attacked by someone sitting in your living room here in Brussels and that someone can be completely across the planet, or in a place that we're not even able to be sure where they are. So, the challenges in cybersecurity are the same human challenges we've always suffered, but with the compounding issue that we've collected the whole world together.

[Federica]: When was it, that a hacker was not seen as a negative thing? And when did it change?

[Patrick]: So, first I actually do want to mention something. I grew up as part of the'California counterculture'. I grew up in back-to-the-land effort in the far remote mountains of Northern California, and I was 14 years old before my family installed a lock on our door. This wasn't because we were naive, we were very, very remote. And the assumption was that anyone coming to our door was either a friend of ours, because it's hard to find us, or it's someone that needed help. And, in the off chance that some member of our family or community was not present, indeed we wanted them to come in and get out of the snow, get out of the cold, have access to food and shelter, because that's a very important human need. So, unfortunately, indeed, human venality intrudes: this area was discovered by the marijuana growers and so we had a heavy-duty criminal contingent move in, and indeed we put a lock on the door. So, some people have asked me, "What is the minimum level of security we can expect?" And I would say, honestly, indeed - with full acknowledgement that we are probably never going to see that in our lifetimes - that I would love to imagine a world where we did not need to have locks on our physical doors. Now, indeed the use of the word'hacker', this is something that as we build a cyber-culture, and as we build terms and words of art around this, we often use and reuse the same terminology. So if you want to look at where the term hacker and where this term really kind of sprung onto the public consciousness, there's a book by a gentleman called Clifford Stoll and it's called "The Cuckoo's Egg". He was an astronomer working at UC Berkeley, and he wrote an amazing book about how he discovered some people going through all of his files in his UNIX server, and he didn't know who they were, he didn't know where they were from.

So, he figured out that he would stalk back and figure out who these people were. He found out - I believe, if my memory serves, I read this many years ago - that they were a group from China; in the Chinese military or somewhere in the Chinese government, who were looking for secrets, scientific secrets, that they could use for their own purposes. He attempted to alert the authorities, he attempted to go to the FBI, he attempted to go to the police and they looked at him like he was a crazy man. So, there was a lovely part of this book... it's a lovely book, it's one of the things that is in the cybersecurity canon, as far as everybody who is in cybersecurity must read this book. And indeed, I trace my own history in this to Clifford Stoll's book: my wife, one day, after having read a book, handed me this one and said "you have to read this". And this was a trigger of a lot of my interest in cybersecurity. And so indeed, the idea of hacking, you find it in a lot of places now, very positively: life hacking, growth hacking, all of these types of buzzwords that come out of Silicon Valley. We still use the term hacking in both contexts and so you have to be careful when you hear someone say about hacker, what do they mean? When we look at the malevolent parties, the opponent - as we like to call them - they come in different grades and different intents and different levels of malevolency. So, we have what we call the'script kiddies'. These are children who just like to do defacement. Think of them as the ones who spray a spray paint on the walls. Some of them are lovely, artistic, they can do actually interesting and cute things, but they're intrinsically motivated and you can kind of look at it and say, "Okay, that's bad, we're sorry, we'll clean it up." We try to keep a civil society around these. Unfortunately, there are other actors and indeed, I mentioned the nation-state actors. So, China is still very prevalent as a nation-state actor, the United States is very prevalent as a nation-state actor, conducting espionage in the cyber-realm. North Korea is credited with the single largest cyber-breach and cyber-theft in the 1 billion dollar attack against the Bank of Bangladesh. So when you look at the top line, you end up literally with armies, and these are quite professionals. One step down from the armies, if you will, if you wish to put them in a hierarchy - part of what we love to do is place hierarchies and categories and labels on things - would be the criminal groups. There are some very organised criminal groups that specialise in hacking banks, hacking financial institutions. Right now the state of the art is that it's easy for them to launder somewhere below 20 million euros or 20 million dollars. So most of the current thefts are somewhere between 13 and 19 million dollars. And this is the point that they find their sweet spot and so they make their living doing this. We can trace these people, we know where some of them are, some of them live in countries that provide protection to them. And so, here is where the space issue, the geography issue, and the fact that our international country based jurisprudence, legal system, isn't adequate to deal with this threat... so when you talk to criminologists about criminology and why people steal things, they actually have what they call the fraud triangle, or the fraud diamond. And, one of the elements that you can try to work against in a criminal enterprise is to reduce their return on investment. And the problem is, when we dis-intermediate space, meaning that I can attack you from across the world, there's no local police officer, I don't have to travel, I don't have to get onto an airplane, I can stay in my own legal jurisdiction, and if that legal jurisdiction provides protection to me, and I'm able via the global financial network to launder those proceeds, then indeed that becomes a very interesting business model for me. And so, indeed there are a great many people that tell their mother that I'm an internet entrepreneur, when in fact they're a thief on the Internet. I work predominantly in the larger financial sector, but you see this happening everywhere. One of the favourite places right now is in the online gaming networks. This is a place where young people spend a lot of time, there's a lot of money involved in this. And so there's a lot of hi-jinks, the script kiddies, the people who think they're playing games, because they literally are playing games as well. But, there have literally also been people who died over this. So we don't have too many deaths, fortunately, but we have had a lot of theft, and there's a lot of problems going on right now for the corporations that are trying to provide these services in a secure way. So, to get back to your original question of what is cybersecurity: I like to try to define it as an effort to ensure that the understood rules of engagement are observed. We have social norms, social conventions of things that we expect to happen: if I walk into this door that should be okay, this should be a safe place for me to play my game, I shouldn't have to worry about walking out the door to my house and being flocked by criminal elements trying to bash me over the head, steal my wallet, and run away with my car keys. And yet, in the paranoid version of cybersecurity this is exactly what we have online at the moment.

[Federica]: Most of us have a sense of what it means to be safe or to be at danger in the real world; for example, not going in the bad part of town is recommendable, because it's dangerous. So, if you really need to go there, you know you're vulnerable, therefore you try to put in place strategies to defend yourself or at least be ready to respond to danger. And we've mentioned this in a previous conversation, that being online is like being in the bad part of town, up in that dark alley. And you don't have a choice: if you are online, that's where you are. It's just a dangerous place, so you should put in place some measures and strategies to defend yourself. But the problem is: how to do that? It's hard to know how to go about the virtual world.

[Patrick]: Let me pick it up from from you right here. And indeed, I think this is a really big point. And this is one that goes to some very fundamental challenges that we face in society. If something bad happens to you, we tend to ask: Did you do due diligence? Did you do your part to make sure nothing bad happened to you? Now, nobody wants to get into victim blaming, because whenever someone gets hurt or someone gets damaged or gets stolen from, our first response should be sympathy and an offer of assistance. And, in some form or another, if it's just emotional, "I'm sorry this happened to you", because you can imagine it happens to all of us. And indeed, one of the challenges that we have is that right now we think if you're in a bad part of town and you get your wallet stolen, that's almost something embarrassing. But let me use an analogy for you: if you're sitting at a traffic light, and somebody comes up to your passenger seat, and bashes the window in, and steals your purse, are you at fault? No. That's completely beyond the pale of what's expected in the norms of today. We can take this to an extreme. I actually have a friend who was taken to task by his partner, because the burglars overnight broke into his car to steal the papers from his car. And she said to him, "Well, that's stupid; of course it's your fault, you should have left the glovebox open, because when you leave the glovebox open and empty, this way the criminal comes by looks inside of your car and knows that you don't have any papers for him to steal, that you've taken them in the house with you. And so, "You dummy, it's your own fault that your car window got bashed in!" That's a step too far. And I think we can all agree in here there's a step too far, and all of us have a slightly different line on that. I draw my line at the point where I would like to encourage us to foresee a civilisation, an online culture, that is safe enough so that you don't have to worry too much about how this system works. Right now you don't have to be a locksmith to understand how your door key works. You don't have to understand the key fob that unlocks your car, starts your ignition and allows you to drive it down the road. You do need to know you have to press the button or turn the key to lock it when you walk away, and if you forget you go running back to your car. A big problem in the digital realm is we don't have the equivalent of this right now. We're very immature in cybersecurity. The systems themselves were built around an open, trusted, scientific, explorative community. So, we're having to adjust some of our fundamental principles to this. And so, indeed the argument is - sadly - in the current state of the art; yes, we need everybody who is involved in a digital life, a digital culture, especially those who are acting in ways that influence others, or place themselves in a role of responsibility, they need to have a certain level of competency, a certain level of knowledge of what's happening in cybersecurity. I wish that wasn't true.

[Federica]: An average user, a private citizen, will normally have several accounts online. Even if you're not on Facebook - and many people are - you will probably use online banking, sometimes you book a flight online, I mean it's really hard not to be online nowadays. So, even if you're not on Facebook by choice and you don't use certain services by choice, you are out there in some form or another. And that makes you vulnerable. But there are some things that we know we can do, like not using the same password for several accounts; but if my facebook account got broken into, I would definitely consider Facebook accountable for that. So, where do you draw the line between what you know you can do, and where the service provider, the platform, the other party, is responsible? And also some threats we know like, "Hmm, somebody could break into my Facebook account", but what about the threats we are not aware of? God knows what those are. So, how can a private individual, a regular citizen, actually navigate through this very complex landscape?

[Patrick]: Um, so, indeed there's a lot of things in what you just said, and I'll try to deconstruct some of it. Let's go indeed to the part where, if your Facebook account is hacked that's Facebook's problem and there's a lot of things inside of that, but let's go to what we call'Single Factor Authentication'. Right now, most likely you have a username and a password that allows you to get into Facebook. Human nature being what it is, you also have a lot of other online accounts and your username might be exactly the same and quite often it's your email address. The password you use on Facebook might be exactly the same password you use on some other website; that other website gets hacked through their insecure workings, through no fault of Facebook at all, you use the same username and password somewhere else and someone knows that almost everyone has a Facebook account. So we have computer scripts that will automatically try a bunch of hacked passwords and we try that username and password on your Facebook account. If we get in, we own your account. As far as Facebook is concerned, you just logged in from a different device and, indeed, if you've gone through the experience of logging in with a new computer replacing your old, Facebook might set you through some additional step of authentication because they're saying, "Hey this is a different device, it's a different place". But, indeed, we also expect to be able to log into a social media account from any terminal, in anywhere, that we happen to go into from our mother's PC, from a PC in a hotel. So, the first thing that we argue in the industry right now, is that everybody should adopt what's called a'Two-Factor Authentication'; something you have and something you know. And most responsible websites offer some form of Two-Factor Authentication and what this means is that if somebody is able to steal your username and password - and there's many ways to steal your username and password besides hacking some third party site - but if we're able to do that, without this the other token and without the other element and to show you. . . if I pull up my telephone device, I have various Authenticator apps that we can have. And so for example, if you wish to login to my Google account, you need to know my username and password and also this code that's going to change in just a few moments. And so, if you don't have that, you're not going to break into my Google account so that being said, there's some other ways to do it but we won't talk about that today. So, the the biggest thing that we argue for everyone right now in "due diligence", is that we need to step up our knowledge and our use of this'Second Factor Authentication'. Such that, that physical key that we currently have to unlock our door is always in our presence: because right now, the username and password is a virtual key that can be passed around far, far too easily. Now you also asked, a little bit what you know what are the risks out there, and who's after me and why? And indeed, you mentioned the obvious risk - which is your bank account, of course - if I can load malware onto your laptop and I can be inside of your browser session with you and I can send money from your account to my account without you noticing it, then indeed that's a type of banking malware that's very, very prevalent today and people make tens of millions of euros from it. And so, that's a very common threat but there are also a lot of other threats that people don't think about. I'm sure you've heard of cryptocurrency, there are people who load malware that has no other purpose than to mine cryptocurrency using your laptops, or your computer's resources. So your smartphone or your computer runs hot, the battery goes down all the time, it doesn't behave the way you expect it to be. But indeed, what it is doing is it's using your electricity, using your device for someone else's profit - without your permission - and so that again goes back to the idea of; it's okay for you to mine cryptocurrency with your laptop, if you agree to have that happen with you. And, one of the biggest points that we run into is‘informed consent’, and indeed one of the challenges people have when they first become aware of cybersecurity topics is; how do I go into Facebook, Google, Twitter, all of these social medias and how do I understand the settings that they’re giving to me? How do I understand what is my‘due diligence’ in here? And fortunately, we have amazing tutorials on YouTube, we have a lot of information that’s available out there…unfortunately it does take some time. And so, what we ask people is, we spend a lot of time on the Internet, it’s an amazing place and we really need to try to do better and making sure that it stays a safe place. And it’s important for us, not just for ourselves, but also for our counter-parties. You may say, “There’s nothing interesting in my email, I’m just a normal person”. But, maybe someone else sends you an email that has a heartfelt concern in it, or they’re telling you an intimate secret of theirs: all of a sudden inside of your email box it’s not just you, it’s actually your friends and so you have a responsibility to your friends and your community to be responsible over protecting their information as well as your own.

[Federica]: When I start thinking of all the ways in which we are vulnerable online and all the ways in which we could do something to protect ourselves better - but we don’t - because it takes time, or it is too complicated, we don’t know how to. Then, I feel a mounting anxiety inside and some paranoia, because you know that danger is out there but you don’t even know how to see it sometimes. So then for me, the next step is just to be fatalistic and just say, “Okay. let’s hope they don’t pick me!” Or, when a news website just wants me to agree on something to let me read a piece of news, I’ll just say, “Okay, okay, okay!”, I do that, I’m guilty of that and I’m not talking about any exotic type of web site it’s really the news and stuff like that. So, when you talk to different types of non-expert audiences, how do you address this issue to avoid just spreading the panic and actually encouraging people to want to do more and be responsible?

[Patrick]: This is a huge challenge and this is one of the core elements that’s in our Cyber-WayFinder program is: “I’m having to learn to be better at doing this”. I had the opportunity to give a presentation at a major conference in Helsinki last year. And afterwards, a CFO of a major corporation came up to me and said, “Patrick, thank you very much for this conversation. All of the other trainings and awareness we’ve done on cybersecurity have left me feeling so inadequate and yet your discussion made me feel that I could actually do something about this.” And, this crystallised for me a problem that I had been working with. The vast majority of the communications we give out,‘we’ being the cyber community, the cyber professionals, are‘shoulds’…you should do this, you owe an obligation. You heard it from me just now; oh it’s, it’s not just about you, it’s about your friends. I was really putting a social pressure on you and giving you a sense of inadequacy because, my god, I’m not doing this. I’m sorry, this is instinctive for us because this is a big part of our narratives that we do. And, this was a big part of what I’m working on is to try to make it easier, so that we understand better what it is and to change some of the ways that we talk about it. And, to change some of the tools that we have and some of the expectations that we have. And, this is kind of part of how CyberWayFinder came to be, because a lot of the discussion around resourcing and the challenges we face, we've been talking about these for the last 10 or 15 or 20 years in the industry and we're not changing them at all. And so what I want is I want to bring you, people like you, into the cybersecurity discussion and have us - society and culture - demand that we as an industry, that we as corporations do better. You can measure your degree of openness in cybersecurity and privacy and intrusiveness, and just as we might with other social measures, we measure countries and cultures by how collective versus individualistic they are. How long-term thinking versus short-term thinking they are, as individuals we can ask ourselves, "What kind of lives do we want to live: open or closed?" And so indeed, we need to engage with people, we need to have this discussion; so that you are understanding of the risks that you take, such that you understand when you post something on Facebook that that is not just, "Oh Zuck has everything on me, so why not?" And you understand the role of a third party game app, or psychometric trick that people use which is now quite famous for the stuff that led to the Cambridge Analytica, that led to the Trump fiasco and all of the stuff that's going on in the political system. And, if you follow what's happening with the Brexit and the Trump election and the accusations of the Facebook data that was used to manipulate people, it's a very interesting discussion and in many ways this goes to the heart of cybersecurity and culture.

[Federica]: I like what you just said, because it shows that cybersecurity is not only about hacking systems and breaking into your Facebook account, not about things that we already consider as crimes, but it's also about knowing who owns your data. And, isn't it a lost battle? Because you can say, "I will not be on Facebook and to buy my flight I will go to the travel agency, I refuse to give my credit card number online!" but it's not sustainable to opt out of all of the services online. Even your passport has your biometric data, so your data are somewhere no matter what you choose. You cannot choose not to be any place data wise and in this sense being vulnerable is not a choice you can opt out of.

[Patrick]: Decision fatigue, a sense of inadequacy, a sense of impending doom and so, people shut off and walk away from the discussion…

[Federica]: Are there common weak spots in cybersecurity, for example, private users have passwords but also very large corporations have some passwords. So, are there some shared weak spots across all types of entities online: individuals or organisations and so on?

[Patrick]: One of the things that we like to say and is very common in the the phrasing of today in cybersecurity is that the'human is the weakest link'. And, we like to follow that up now - a little bit more frequently now than we did in the past - which is also the human is our first layer of defence. And, this is why most corporations have a very strong cybersecurity awareness campaign. The problem I have with this is that this only reaches our corporate employees in the context of their corporate behaviour. And, we're able to govern certain types of their behaviour in our corporate setting, that are not applicable when they go home and they hand their iPad to their child. And this is where we tend to find the work-life interface of Technology, where this type of awareness tends to break down. Now, what the single largest influencing operation is and the single most likely successful influencing operation is, has to do with what we call social engineering. And indeed we have built firewalls and we have built access controls and in my corporation we may have complete'Two-Factor Authentication' everywhere. We monitor what people do, not because I think you're a bad employee, but because I'm desperately afraid that someone stole your credentials and that's not you logging into the payment system to authorise a billion euro transaction. So we've done all of that in the corporate environment, but we haven't done adequate, in my mind, in how we deal with this as a social issue. And when you look at people who are social activists in this topic, you find that there's a lot of good things happening. And this is also why, I think I've made it clear to you, I'm European today. I love the ethic that Europe is trying to bring to this discussion. Now we're failing on many different levels, there's a huge number of problems with our GDPR, our data privacy rules, however this is the best thing going anywhere in the world and so literally, Viviane Reding, the lady who helped put this together, she's a heroine of mine!

[Federica]: At this point in time, would you agree that it's a lost battle? Again, it's a frustrating experience to go online and want to access some popular services, like Facebook, and to not be able to discuss, object, opt-out of the terms and conditions that invariably you're asked to agree with and just click OK. Or, no thank you, and then you don't get access to that service. Sometimes, you can do that, but we just said that it's not really a sustainable option, that of refusing to be on all of these platforms. And oftentimes, you have to agree terms and conditions. So, even if legislators are currently at work to tackle some of the issues and find a solution right now, so at this point in time, do you agree that there is an element of powerlessness in that you have to bow and agree to those terms and conditions?

[Patrick]: I don't accept that it's okay that I walk out of the street and I'm assaulted by five people, every time I walk out my living room door. First off, I would like to mention that, it's not so hard to leave Facebook. When you look at some of the damages and some of the statistics that people are looking at - which has to do with the human happiness - there's a huge and I believe correct argument; that getting off a lot of these social media that ferment FOMO, fear of missing out and inadequacy, that there's actually a really good argument that we should - if not get off of Facebook - extremely curtail our activity on these'types of platforms'. And I say these types of platforms, Facebook is not the only one! I will also say that I'm not on Facebook, my dead cat is on Facebook. When he died I asked Facebook to memorialise my dead cat because he had a lovely account and Facebook said, "It looks like you're using your dead cat as a pet and we don't allow that, that's against Facebook's regulations". And so, I said okay, the next notice is that I'll get from Facebook is that they've terminated and killed my cat's online identity. In fact, Facebook has never done that. My dead cat is still alive on Facebook, because Facebook sells the images of my dead cat, or the the looks, or the views to their advertisers as part of their millions of users.

[Federica]: Before we move on to a broader question, which is where I'm headed, I would like to try to ask you a specific question on a specific app, for example Whatsapp. It's a very popular messaging app. Is it even known to the users, how it works? So can we know if they keep all the pictures, even after we delete them? For example, do they browse the chat, are there maybe things that are safer to do and things that we should avoid doing. So we still use the app, we don't give that up, but we are careful with certain things. So, can you say something about WhatsApp in particular? It's so common that I think it will be of interest to more than some listeners.

[Patrick]: The answer I would give you today, would have to be qualified based on information I don't know. However, I do place a great degree of credibility on the people who founded the platform and who know the platform. And the gentleman who walked away from Facebook literally walked away from over a hundred million dollars worth of stock options, so I'm pretty comfortable saying it's an ugly situation on the surface of it. What Facebook is selling about you and your WhatsApp is your contact details and certain amounts of information about what's going on in there now. They're clear that it's encrypted end-to-end but they're in the middle of this and they are taking knowledge out of this. And there's a reason they spend billions of dollars to buy this platform, they didn't do that just because Zuck wanted to have a W on his Android phone.

[Federica]: This is the paranoid me speaking, but also the curious me speaking, I'm sure that many people - not just I - would like to know some of the behind the scenes of the apps we use daily. For example, is it true that our chats are parsed? You see the morbid curiosity? Is it true that, you know, I know some people, who a couple of years ago would refuse to, for example, use the word'Bin Laden' in their chats; because that would be recognised and then they would be followed as potential terrorists. Now, I never knew if I had to buy into that narrative, but they believed it was true, so they didn't do it. I didn't know and I kept doing it, so nobody really knows. And yet, we have to make decisions about these things. Back to the morbid question: do they parse our chats?

[Patrick]: So, there's a step beyond this even; where people feel that Facebook and other social media entities have turned on the microphone of their phone and is listening to that. Because quite literally, they were having a conversation over dinner with a friend of theirs about a new Jaguar car, or a new coat that was being offered by a fashion house and then the next day on Facebook or on Google they see an advertisement for that car or that coat. And the sad fact is that, we humans are so predictable and - at least the argument is - that they're getting so much information on us, that they don't have to listen to our chat. They actually know when and where we become interested in these types of things, by the other bits of metadata we leave streaming around. And so, they have a certain amount of hit-and-miss for these. But what we notice and what our mind remembers is the hits, the times when you get this creepy feeling that,'oh my goodness', someone's spying on me because that ad, how could they have known I was talking about that last night to my girlfriend? Uh so, there's a real challenge in here, in this kind of. . . 'where we're going with it'? And so, we need to try very much to separate out the paranoia from what is really going on. There are some really good researchers, from really good people looking at these - I don't put myself on the frontlines of those - I'm actually not a researcher, I'm someone who sits a little bit in the back. I work a lot in infrastructure, I work a lot in building the next generation of people who are going to be doing this and who'll take this discussion further than I will. So I'm not the one doing all of this research upfront, but I read people that I respect and people who do what I believe is quite good science or engineering and looking at these types of topics and these are topics that desperately need to be looked at.

[Federica]: Do you see where the paranoia comes from? There's so much we don't know and I'm a curious person, so I wish I knew; Do they do this? Is it true that they can read this? Is it true that they do that?

[Patrick]: And who'they' are is obviously a big question mark as well, it's the nameless, faceless, unnamed'they' indeed!

[Federica]: The'illuminati'. . .

[Patrick]: Exactly.

[Federica]: There are some things that are understood, for example, we should all pick a different password for each account that we have. This does not change really, it's just a rule of thumb that works. But, there are other things that just get updated every week, every month, there are new ways in which'they' try to lure us into let'them' know about us. So, how is a user supposed to keep up with all these things without becoming paranoid?

[Patrick]: This is one of the challenges that we have in a civil society. I don't know. . . have you ever been called by Microsoft's tech support service? Okay, there is a very active scam that is someone calls you up and says, "Hi, I'm from Microsoft's tech support service, there is a virus on your computer and you need to talk to me and I will help you to remove the virus from your computer". And I'm er, I know this is a scam since long and many years ago I received this phone call and it was a Saturday, I was downstairs doing the laundry. And I had a choice: I could talk to a scammer or I could do my laundry. So of course, I sat down and took the phone call and it was really fascinating to me because instead of playing a game with him, there's a lot of people who'd run into this person and they post a script of, you know, how they the games they played to try to reverse trick to this person. But I actually told him right up front, "I understand this is a scam and that you're not from Microsoft", "Oh no, Sir I absolutely am, we're contracted by Microsoft to do this". And I told him, "Well no, I don't think so, but tell me what you have to tell me", and I walked him through his script. So, call centres, contact centres have scripts and he walked through his entire script with me and quite literally, halfway through this conversation I stopped myself and I went up to the Internet and pulled up in a web browser and typed in Microsoft Tech Support scam; because I just had to revalidate, because this person was gonna do anything they could to try to convince me that they were from Microsoft. And, it was something that truly gave me a sense of sympathy for the people who fall victim to these types of crimes because: they're very good, they're very persistent and they keep trying. So quite literally recently, I don't know why, we've been getting up to three or four calls a day and six to seven calls per week the last several months, here in Belgium. I don't know what has triggered that and, indeed, my wife has taken to telling the people on the end, "Your mother is ashamed of you!" and it's really interesting to see which ones care and which ones hang up immediately. And I feel sad in some ways, but indeed, the only way to truly stop this is to try to ask police to shut this types of thing down - which they've proven incapable of doing as yet - or indeed, to ask the people who are doing this, "You should really be ashamed of yourself, you should try to find an honest way to make a living."

[Federica]: Speaking of vulnerable population groups, in the real world, in the streets you would think that it's easier to steal the purse of an elderly person, unfortunately, because they are physically weaker and also they will not run after you online. Is the population also divided by age or - it's rather like you said - people in specific situations: so across age groups, but maybe alone, lonely hearts and situations like that?

[Patrick]: It depends on the criminal scam and it depends upon the criminal group and it can be either targeted or less targeted. There are some very specific scams that target young people particularly, the I watch, "I hacked your webcam and I watched you masturbate, tell your parents to give me a thousand dollars or a thousand euros or else I'm going to release this to all of your Facebook friends and your social life will be ruined forever ever", and literally there's a kid who jumped off a bridge and killed himself. And they went back and found that this is this was what had happened, so literally people have died over this type of hack. The other thing that I think is, as we say often,'there's a special place in hell' for, there's a lot of people who like to do the Lonely Hearts scams. And this is a nice lady, maybe she's widowed and this fellow - who works on an oil drill rig or maybe he's in the military stationed in Iraq or someplace far away - and they start up an online romance and slowly this falls into a situation where there needs to be some money sent - because a daughter's going to surgery, or I'm going to come visit you, but my credit card isn't working right now, can you buy me a plane ticket. . . which can be refunded for cash - So these types of things. And literally there have been people who've been taken for millions of dollars from this. This is what I tend to call the retail crime, there's ABC's: the addicts, bikers and carders. So this is really the the mass-market crime, if you will, where a lot of the scams that have been going on forever in society, since well before digital came along: have been elaborated, have been professionalized by this. Many people used to talk about the'Nigerian 409-scammers' and the'Nigerian Lonely Hearts' and the'Yahoo Boys' which is a region in Africa where this was really institutionalised and made very profitable.

[Federica]: Is it true that Nigeria is a hot centre for this type of scam?

[Patrick]: It was and it still is, but it's not only Nigeria anymore. The other thing is, that the Nigerians have diversified. So the people who spent 10 years performing this type of scam have actually become quite good hackers in the mean time. So people love to differentiate the different hackers and they love to pen talk about Russia and Korea and Iran. But, I argue that nobody should ever discount the Africans either, as far as hacking capacity and ingenuity in committing a fraud. And for that being said they shouldn't discount the British or the Americans either.

[Federica]: I think it's interesting what you've just said, then, when an ill intentioned person targets someone, the decision of who to target is not dependent on the technology - like what device they are using - but always on something human. So are they lonely, or are they naive, so the human factor is so important.

[Patrick]: It can be. But it can also just be a scattershot approach. One of the things that people talk about is: how could anyone be so foolish to fall for a scam that is poorly worded, that has bad English? But the thing is it's very, very cheap to send out an email to a lot, a lot of people and so that type of scam is very easy to send out. And indeed, the argument is that it's poorly worded exactly to catch the person who's not paying attention, or the person who is in a financial constraints who just might - for a moment - believe that that might be true. And quite literally, I get people in my social circle who say, "Yeah Patrick, I got this email do you think it might be real?" and you just look at it and say, "How? My god, how in the world could you think for a moment that it was real?" And so, normally I called them up and say, "Hey, what's what's going on in your life?" Then, I often find that there's a lot of. . . you know. . . difficulties, troubles, health issues, they're in a weak point in their in their life, their defences are down because of other things that are happening in life. And indeed, I break the news gently that this is a scam, absolutely never go ahead respond to any of these types of things. But, I don't hang up the phone there. I actually spend some time with my friends to talk about it. And say, "Hey let's talk about it". . . let's have a little bit of human contact. . . let's see what's going on with you.

[Federica]: Do you think that cybersecurity should be taught in schools? Again, to defend this vulnerable age group. Or do you think that it should be in the culture so that it's not necessary to have one hour per week of cybersecurity training in the schools?

[Patrick]: I think it should be in the culture. If you look at what we teach children today; we teach children today to be careful - you know depending on your level of paranoia and depending on if you live in a high trust culture or a low trust culture - you teach your child never talk to strangers, never get into a car with a stranger. And yet, we let them loose on the internet without a concern. Now, we don't want to make our children paranoid, we don't want people to grow up with a'fortress mentality', but until we get some of this sorted out online, there is a certain amount of parenting or adulting that needs to be done. Are children particularly vulnerable? Of course! Cybernetically? Absolutely! But, as well as physically. So when we look at the damages that are being done, particularly to people in puberty when they're in a vulnerable stage. When we look at a lot of the stuff that is going on right now, there's something that is unique to cyber, cyber topics. Which is the space issue, the geography and the sense of'pseudo anonymity' and you see it when people drive cars. You can work with people in the office and they're absolutely amazing and then they get into traffic and they turn into a raving lunatic; and screaming and yelling and swerving in and out. . . you're smiling, you've seen this before! You know it, this is the same thing that we can argue leads perfectly decent people to behave like butt heads on the Internet. And so, we get people who create a pseudo ID to as an adult, to pick on a'former friend of their daughter' and drive this other girl to suicide. There's a case of this where a lady is in jail right now because she did this, quite horrific. And so indeed, these platforms lend themselves to this type of abuse and this was one of the big arguments in the social media platforms. And, if you have an app or something online that is targeted to child users, you have an obligation to make sure that that is a place that's a safe place for kids. And we, as society and regulators and people who look at this also, need to look closely at what we're doing in these types of places and make sure that we protect people. One of the definitions of ethics - that I love the most is -'How do we protect the least among us?' And the'least among us' are often people who are not as mentally astute, or not as developed, or have or in a weak state for themselves. And so, we need to foresee a way forward where we are protecting'the least among us' in our physical space as well as in our digital space.

[Federica]: Let's push the anxiety levels to the max for a moment and let's look at the future: with biometric data becoming more common and with the possibility to monitor citizens with such accuracy and also threats over cyber attacks from one nation to the other, it seems like it doesn't look very pretty does it?

[Patrick]: Okay, so one of the challenges that we have today is people talk about my company is going'digital' or we're going to have a'digital company'. Well, right now, our society is already digital and so all of our companies to say,‘I’m a digital company’ is like saying: I’m an air-breathing mammal. It’s part of the definition that’s in the taxonomy. And so, indeed there are people who worry about the‘zombie apocalypse’ and there are people who worry about the‘cyber apocalypse’. And there are very responsible people spending a lot of money addressing this topic. And so, we have what we call‘critical nation-state infrastructure’ and that might be a power plant, it might be a banking network, it might be anything that society depends upon. And if you think about it, indeed, there was an incident recently in the UK where the NHS, their medical system, was hit by a cyber attack and there were people who had their surgeries delayed and they may have died from it. And so indeed, those of us who are responsible for cybersecurity in a‘critical nation-state infrastructure’ entity, are held to a special level of governance and we’re told to spend a certain amount of money making sure that we’re able to deliver our services against a reasonable level of cyber attack. The biggest problem we have is that that level of cyber attack, the proficiency of it, the skills of it, the likelihood of it is ever increasing. And this is where the sense of impending doom starts to come in. Because, we have to turn around and ask our ratepayers, our citizens, to pay more in banking fees, in electricity fees, or whatever they are in medical insurance fees. And of course, none of us want to do that as well. And especially when cybersecurity - being as immature as it is - it’s very hard to prove success, it’s very hard to prove good enough. So, those of us who practice at a deep level, we have standards, we have audits, we have multiple layers of audits and inspections of what we do and we have entire systems. I work with 200 colleagues that are dedicated just to cybersecurity. I work with 15 people that are like me who are - shall we say - well past 40, who’ve been in this industry for a long time and we consider ourselves the brain trust of our organisation. And we are working desperately hard, because we truly understand how important this is for our clients, as well as for the service that we provide to society. I’m very proud of my ability to work in this domain and do this, because this is something that does go back to my childhood where I was a volunteer firefighter. When something went wrong when I was a kid, people came to‘The Wheelers’ because they knew that we would be there to help them. And so, that is a big part, this continues to be my motivation to do this kind of work. And a big part of what I’m trying to do in our CyberWayFinder program is to reach out to more people who want to try to help fix this problem, address this problem. Stop the bad things and continue the good things that we’re getting from our digital economy and our technological society.

[Federica]: Very well, this brings us back to the training program: the‘CyberWayFinder’. With this program you’re trying to promote a culture of cybersecurity and that’s interesting because it debunks another myth of cybersecurity. . . that it’s all about the technicalities and it’s all about the algorithms and the hacking. But you’re trying to promote a culture of cybersecurity, what is that. . . can you talk about that please?

[Patrick]: So, one of the big discussions in cybersecurity right now is: why is it so male-dominated? One of the last statistics that came out - we’re waiting for some updated ones please - is that in Europe, we were at a staff level approximately 97% male. And, when I look around on my plateau and my teams, we're 97 percent white male. So, a big part of this - you can hardly argue we represent the culture that we're attempting to defend - if we don't have people on the floor, people in our defence that are looking like the culture that we're trying to work with. Now, a lot of people address this as a social issue. It's just unjust that we don't have greater gender, or colour, or immigrant representation in our cyber teams. And, I agree with that, there's nothing wrong with that statement. But that in and of itself hasn't been sufficient to drive the change in the last 10 years. As a matter of fact, the representation in diversity and cyber teams has been reducing in the last couple of times. You know admittedly. . . our statistics are not good, so we're trying to get better statistics on this. But in our realm, if you consider cyber a subset of Tech - which a lot of people do - and Tech is heavily male-dominated and if you have to come through Tech in order to get into cyber, with a leaky pipeline, it's inevitable that we're going to remain very male and very pale. And yet, when I look around and I see some of my favourite cybersecurity practitioners: people like Becky Pinkert, who has a degree in psychology, people like Michael who has a degree in international business. These are people who work at the top, top levels of cybersecurity and did not come through Tech or did not come through a degree in science technology, engineering or maths as we tell everyone today. So our program is really designed to take people, mid-career professionals preferably, people who have had some very interesting careers, who understand how society works, who are good influencers in their office space, in their professional life. And ask them are you willing to take a career pivot? If you're under challenged right now, if you're frustrated because you you feel a lack of meaning and intent behind what you're doing. . . and you say, "I still have something to give and I want to really turn my career pivot" and, I'm sorry,'kick-ass', then this is what our program is about. The core of it is that you learn cybersecurity by doing, not by doing it in a university so our effort is we'boot camp' people. We give them 40 hours of training on nights and weekends, while they're working already in their day job. And then, we try to position them and transition them into a cybersecurity team well before they're ready - with only a month of training, 40 hours of training - you're not competent yet. But that doesn't matter, you are actually more competent than you realise; you've been doing passwords for a long time, you've been doing governance for a long time, you've been managing projects for a long time. There is a huge amount of potential in our mid-career workforce, that can be used in cybersecurity. If you wish a military analogy, you can use the Bletchley Park out of the UK. When the World War I happened and the World War II happened, there were all of the men off fighting in the wars and the women back home were actually'freed up'- quote-unquote - to do some amazing things in a technological realm. If you wish to use the analogy that we're in the midst of a'cyber war' right now and, I'd either agree nor disagree with that, I very firmly placed myself in a civilian capacity. But the argument is, we need all resources that we can and the most interesting and engaged resources that we can get. And so indeed, CyberWayFinder is designed to find these people and these resources that we can put to work now. Not er, the people who are 12 or 14 years old right now, that we can convince to go through a technology university program, graduate, get a masters, work for 10 years in technology and then maybe enter cybersecurity. We don't have that much time to waste so, what we're really about is building this type of community and cohort right now. We follow this program, it's a three year program. So, we get the people working in their cyber teams, each year they sit for an internationally recognised, standardised, cybersecurity certification. So indeed, there's no standard university degree right now, but there are some technical certifications that you can get that are recognised. And so, we ask them each year to take a new certification. And so the goal is, you take an individual - a man, a woman, white, any colour - and they have three years of technical experience. And what I mean by technical, I just mean with a job that says'cybersecurity', they're working with teams around cybersecurity, even if they're in the legal department of my cybersecurity team. . . that's still technically legal, so it's legal technicalities that they're working with. You have three years of experience in cybersecurity, you have three certifications that are recognised internationally and you have ten years or five years of work experience in something else. You know a lot of people, because the teachers and the evening lectures are led by industry leaders and thought leaders in our ecosystem. The practitioners and the doers. So you make a massive network of'who is who' in the local cybersecurity community. You're somebody, you're not just an entry-level person anymore you're actually a mid-career cybersecurity professional. Now that is a heavy, heavy lift. There are people who say our program is too long in three years, there are also people who say it's too short; you can't attain that in three years. And, one of the things that we love is the women in our program who have accepted this challenge. Some of these women when you talk to them they'blow your mind'. . .

[Federica]: Okay, so your program is based in Brussels, Belgium. Where can people find some information about it online and if you will, also some sources on cybersecurity in general?

[Patrick]: The first question is very easy to answer,'CyberWayFinder' is the name: all one word dub, dub, dub and a dot com at the end, or you can just google that word because, as far as I know, we're the only one who seems to be using that word at the moment. So that's an easy way to find out about us. We're not just in Brussels, so we are expanding right now into Luxembourg and some very nice people made a request to have us in Den Haag, in The Hague, in the Netherlands. Soon we have discussions ongoing in Paris, as well as in London and there's an amazing girl in Finland who wants to spin up a version of us. So, we are absolutely moving forward with a geographical expansion. As far as online sources, this is one of the problems with the Internet. There is so much information out there, the thing I would recommend is that almost all responsible media outlets have some good information on this. And so, go to your favourite regular news source and look inside of their technology section and see if they have some good cybersecurity advice. If you are someone who is taking care of an elderly person and they're clicking on every link and every email that they get, make sure that you sit down and have these conversations with them. One of the challenges that we have is that, there, there is a lot of information, there's a lot of what we call'fudds up';'fear-uncertainty-doubt-disruption' and the zombie apocalypse! And so, some of the blogs are quite scary, some of them are quite funny. If you're interested in criminality and protecting your financial well-being, there's a gentleman called Brian Krebs, and he has a blog site called 'Krebs on Security' and he's one of the people that I think writes really well at the intersection of people and what's happening in the financial world and who's trying to steal from you. And I think, he's one of the places where I like to send people. Also, just, he's a cool guy when you when you read how he got into it and what he's doing; good, good for him. There's some other people who do some really interesting things. One of the websites I really recommend to people is'Have I been pawned" and that's'P-W-N-D' and this is a gentleman called Troy Hunt who is a security researcher. And he collects from all of the known sources, the username and passwords that have been breached. And he runs a very responsible website where you can put in your email address and it will tell you what is known of the known breaches. So did you use it. . . was that email address compromised in the LinkedIn breach, in the Yahoo breach, in any of these known major breaches out there. And a lot of the other ones, where he doesn't even know where they came from, we just find these batches of passwords on the internet and you can figure out if your username and password have been compromised, or are known to be compromised. And it's a really good thing to do with your own account but the thing that often frightens people is that I asked them then; if they have children that have emails, put your child's email address in there, or put your mother or your grandmother's email address in there and then go have a conversation with grandma, mom, or your kids.

[Federica]: Thank you so much for your time, and kudos for what you do. Thank you for being on Technoculture.

[Patrick]: Thank you. It's a real pleasure.

Thank you for listening to Technoculture! Check out more episodes at technoculture-podcast.com or visit our Facebook page at technoculturepodcast, and our Twitter account, hashtag technoculturepodcast.