Transcript TrustTalk Interview Paul Timmers

Listen to the interview on the podcast channel https://pod.co/trusttalk. The podcast can also be found on all major podcast platforms, e.g. Apple Podcasts, Google Podcasts, Spotify etc.

Interviewer: Paul, thank you for being our guest today. Before your current position, you were director at the European Commission's Director-General for Communication Networks, Content and Technology and you were responsible for developing a digital single market to generate smart, sustainable, and inclusive growth in Europe. How do trust and cybersecurity fit in this?

Paul Timmers: Well, thank you, Severin, for inviting me and also for this question. So, historically in the European Commission, topics like cybersecurity were more technical topics in the sense that European policy was about investing in research and innovation and then developing new technologies. But that kind of technical view has really shifted to a very, very political view. And the reason for that is I think that digital is now pervasive in society and economy and democracy everywhere. And that also what comes with it, some of the threats, like cybersecurity-related or data protection, they have become very political. They touch the foundations of our economy, society and democracy. And so you see that trust and cybersecurity have risen to the top of the agenda as the Germans would say it's a "Chefsache".

Interviewer: So why is trust in the cybersecurity world such an important issue?

Paul Timmers: What you see is that cybersecurity is pretty complicated, you know, it's not just a technical thing, and I just said it also in the policy terms, that is not just technical, it's really about it starts with people, then it's about organizations and how they work and the processes that you have procedures that you have in organizations to deal with information, for example. And then it's about technology, and then it also touches the bigger picture of our whole society. And with that, also the states themselves. And so you see that cybersecurity is so important because it's the foundation, it's part of the foundation on which we are building our economy and society ever more, the digital foundation, so it's complicated. It's also very important to safeguard that because if we don't trust it, we cannot really work in our environment, in the economy. And so you can make that much more concrete, of course, the point is that we need to find the right match between technology and the way we use it and the social constructions around it, like, for example, law, like legislation. And that's not so easy. Let's take an example.

Suppose you are using your smartphone app with WhatsApp say, then that is something that is in principle open to the world. You can get a link and through that link you can get anywhere and you can end up on a malicious website and download malware on your mobile phone. So the technology is very open but doesn't protect you, and the responsibility is with the user. You could also say, let's design the technology in such a way that these innocent users are at least a little bit more protected and don't easily fall into the trap of clicking on a malicious link. So here we have something about what are the rules around? What do we expect from technology and how is the technology being designed? And you could, even if you want to put it into policy or even into law and require, for example, technology to be more trustworthy and more protective of innocent users than it is today. And these are kind of things that we have a choice to make.

Interviewer: Talking about trust, the most successful methods of fighting increasingly complex and ever-changing cybercrime hinge on trust, right? Trust throughout the supply chain, trust between companies, even competitors, and trust between government and industry. So where do we stand in Europe in this regard?

Paul Timmers: What we have seen happening and I've been really in the middle of that, is that there is an increasing collaboration and the party start to get to know each other and getting to know each other is the basis for trust. So for example, in the beginning, when we came with legislation at the European level to collaborate and exchange information on cyber attacks, most of the countries said, no, no, no, we don't do that because that's national security. But then after a while they saw, you know, this is bigger than an individual country. We have to work together and exchange information, and let's find a way to do that. And with an attack like WannaCry, for example, that disabled one-third of the National Health Service, was an attack on hospitals. They actually worked together to combat this. And so states are starting to work together gradually. Private sector is the same kind of story. They might say, we keep all this information for ourselves because that's commercially confidential, but you actually become more vulnerable if you don't put a little bit of trust in it and build upon that little bit of trust to extend your circle of trust with your suppliers, for example. And that's so the developments have been in Europe very much towards more collaboration, but also to us, much more forceful legislation because we can't wait. You know, it's nice that we need to build up collaboration, but the attackers don't wait for us. So perhaps we have to be much more firm.

Interviewer: Talking about companies, the German company Siemens created in 2018 the Charter of Trust. What does that entail?

Paul Timmers: That's one of those collaborations that I was talking about and that was the Charter of Trust from 2018 was initiated by a number of companies amongst them Siemens. And in the meantime, they have expanded that to about 20 companies from Europe, the United States and Japan. And these are mostly IT companies, information technology companies and a number of companies that are close to that, like those that can offer cyber insurance, for example, or that can offer certification. And they have said we need to put down a number of principles of what we can expect from the suppliers. And they have written down 10 principles. For example, a supplier, you need to organize yourself so that there is a responsibility all throughout what they call the digital supply chain. So all these bits and pieces that you are getting that ultimately build a complex system like a government service, for example, they have to be provided on the basis of responsibility, but they have to be provided on the basis of security by default. They have to be provided on the basis of mandatory certification. And you have to add education to that. So these are four or five of these principles. And what they are doing now is principles is nice, but you know, you have to put it in a contract, you have to do a test, you have to do something a technical specification, very concrete. So they are doing also pilots to show how do you put these principles into practice? I must say that so this is one of the important collaborations that exist. There are several collaborations that exist. There are also collaborations with governments, for example, the Paris Call for Cyberpeace as well. You have collaborations in sectors like the financial sector that are doing a lot, also as industry and together with governments to write down what does it mean to have a trusted supply chain, which is one of the key themes? Very briefly, by the way, this trusted supply chain has really risen to the top of the agenda with some recent attacks. For example, the SolarWinds attack that happened in the United States, which was such an intrusion into the sensitive part of government that the government said: "this is national security". You need to do something so that you know, the software that you're getting is actually trustworthy, a trusted supply chain.

Interviewer: In our context, before we had this interview, I coined the term "foundational trust" and you asked me what I meant by that. I came to that after reading an article by PWC Netherlands, and I'm quoting them, "cybersecurity is invisible foundation of modern

organization. The realization by many CEOs that entities in trusted environments can lead to all sorts of trouble, and investment in cybersecurity is the foundation of working in a digital world."

Paul Timmers: There's this, I think, to look at trust foundational trust as being so essential in your daily business or in your activity as a government is, I think, really central to this. This is what you need to be aware of because as a matter of fact, you need to pose that as a question as a CEO, do we have trust sufficiently built into all of what we do and how would we then do that? That is, for example, such an initiative as the Charter of Trust can do that, but you might also do it by saying, well, actually, I want to work on the basis of what is called Zero Trust. So you just don't trust anything and you put everywhere the measures in place to verify that what is being promised is also delivered in terms of trust. So trust becomes the foundation of the business and trust grows over time, and that's a very, very important asset. It's actually a business asset, a key asset. If there is sufficient trust in the collaboration between, let's say, in the business ecosystem. Why is that an asset? Because this is not only technology again, it's also people and people can take much more efficient and faster decisions once they have that basis of trust. And then you can only then you will be able to beat attackers, hackers, malicious states, that have intentions that you cannot trust at all. So you do have to rely upon a foundation of trust.

Interviewer: You mentioned Zero Trust, a Zero Trust model, provide security against ransomware and cybersecurity threats. In an earlier interview I had with Jacoba Sieders, she talks about what it takes to get cybersecurity through identity access management and the security concept of what you also mentioned is Zero Trust, the belief that organizations should not automatically trust anything inside or outside their perimeter and instead must verify anything trying to connect with systems before granting access What is your take on that?

Paul Timmers: Zero Trust is I mean, we all have to be, of course, a little bit sober about these kind of slogans because it sounds very good. Zero Trust and it sounds very good to do security by design or security by default. Well Zero Trust is a way to do security by default and security by design, it's an excellent principle. Now you have to make it work, so you have to say, what are these tests that you are going to do on your components? And you have to be aware that you're starting to do this in an ever more complex environment. So we go to 5G. What they call

the attack surface is increasing massively because with 5G, you can connect everything and the network will be managed by partners that are less experienced in security. So you are expanding your vulnerability landscape and therefore Zero Trust is not a one-off type of thing. I also need to say ultimately in Zero Trust, there are still elements that you do need to trust. So let's take again the SolarWinds example. The NSA has recommended that after that, the only way to ultimately deal with the supply chain attacks is if you use hardware security modules and these are trusted pieces of hardware. And there it's kind of you have to trust your supplier. So the ones that are building the hardware security modules, you better know really very well which companies these are, because these are the ones that you need to trust, perhaps without you being able to inspect everything. So Zero Trust, great principle, very important because it's an approach for security by design. Be aware it also has its challenges and its cost.

Interviewer: You cannot separate cybersecurity from technological sovereignty or digital sovereignty. This is especially important for Europe, I guess, which fears becoming too dependent on the U.S. or even China or Chinese suppliers and fears losing control. I bring into memory the discussion around 5G. You just mentioned 5G earlier. Can Europe trust other countries to use their technology to achieve global cybersecurity despite political differences?

Paul Timmers: Though in the past, we didn't really think about it, and I think actually the Dutch government had a good characterisation of that, they said we are a little bit naive and we shouldn't be naive anymore. So we cannot afford to be naive when we are talking about suppliers coming from China, but also not from the United States. They are always different interests there and these different interests are can be seriously different. You know, we can seriously feel to be threatened by some of the intentions, such as from China. So we are beyond naivete, but now we still need to. We are still working in a global world, so we still need to figure out how do we then work with parties that we can trust to a degree perhaps cannot really trust, but we are still dependent upon them. So you need to think about how do you deal with getting your bits and pieces from all across the world? And basically, I study this topic a lot, there are basically three approaches to that. You can kind of do your best. It's a risk management approach. You muddle through and you keep fingers crossed that it goes well. And this is actually probably 90 percent of the time what we do. Then you can say I only work with those parties that are really trust my like minded parties, and you could build coalitions in that, and that's increasingly popular. And then you could say, Well, but perhaps this problem of

these attacks is such a problem that we need to collectively at a global scale deal with it, take the stability of the core of the internet. The internet is of everybody. Perhaps we have to jointly manage the domain name system as we do internationally. We do that and Icann. So that is a core issue of trust, and we did find some way with all its pitfalls, but it works to manage the stability of the internet as a global system, as really in a global collaboration with the private and public sector. So we need to think about the approach that you follow, risk management, strategic partnerships or doing it as a global common good and you need to also think about it where would you then do that? So I would say I just mentioned hardware security modules. You know, that's hard encryption that is built into a piece of hardware. Probably you need to do that at most, which you like minded partners, parties, but not with everybody. That will not work. But if you talk about cybersecurity in the automotive sector, you know it's a global industry. Can't they figure out or health, perhaps an even better example in these times in COVID, can't we figure out global cybersecurity and health by working together internationally with the World Health Organization? I would say that's the way to go, global.

Interviewer: In your article called "Debunking Strategic Autonomy", you seem to allude to the issue we just discussed as well, noting that Europe's fear of losing control can be retaken by reversing outsourcing. What do you mean by that?

Paul Timmers: Yeah, that is one of the things that is proposed as a solution. When in COVID, it was said, you know, we don't produce enough of the masks, for example, that we need to protect ourselves for COVID. So let's because they are produced somewhere else in the world or basic components for medication, let's bring that back to Europe, and this has all been outsourced, you might say, over time. And then we are exposed and we see we are so dependent upon it that we don't have this buffer. We are not resilient. We are getting into a very risky situation. So the reversing outsourcing is bringing back part of the supply chain, the manufacturing, et cetera, back to what you have more closely under control. Now there are many downsides to that because this is not without reason that we have been outsourcing, there are upsides to that we will get more resilience. Perhaps we create new jobs in Europe, so that is also attractive. But perhaps we have to think about these things not only from a purely economic perspective, but also from the perspective of the somewhat longer-term future of what we want to be as a country or what we want to be as Europe. And data, data handling, is a good example. You know, perhaps we have to keep the data a bit closer to ourselves is being

argued nowadays, and so not bring them away to another continent because data are almost like a natural asset of your country and you are not going to sell that away or shift that out of your country, you want to keep it close to yourself as a natural asset, as a sovereign asset. So the reversing outsourcing is a trend, has been a bit of a slogan, has been put under pressure by COVID very much. I think we are now getting into the reality of it. If you do it, you have to be careful because it may be less efficient. It may be against WTO rules. It may be that it's not sustainable. But perhaps it's also a good thing because it may increase the value close to your own people, your own country.

Interviewer: The journalist Daniel Bogler wrote in an article in Forbes in January of this year, and I'm quoting him, "Sharing information on cyberthreats is the test that will determine if all the principles established by organizations such as the CoT will actually make a difference in the real world. If companies are willing to share data, then threats and new attacks will become quickly visible. They are spread from industry to industry, can be prevented or slowed, and best practices in combating them can be easily shared". Would you agree with him?

Paul Timmers: Would I agree? I would say yes and no. Yes, because we saw, for example, with this WannaCry attack or earlier there wasn't was a vulnerability which was called Heartbleed in a basic component of the internet that sharing the information was actually tremendously helpful because everybody could quickly start to repair their systems and avoid that it spreads around and destabilise, for example, whole logistics chain or a hospital system at large. But you need to be very, very fast to do that. You know this information sharing, because also the attacks are going very fast, and you need to be reasonably sure because you don't want to create panic from nothing. Recently, we had an interesting case. There is a volunteers organization in the Netherlands called the DIVD, and they found a weakness in software from a company called Kaseya. And while they were finding this and sorting out what the vulnerability was, there was in the meantime, there were hackers that started to attack. So they were actually very careful, these people of DIVD not to start shouting, crying wolf too soon. But in the meantime, the hacker started to attack. So your information sharing is absolutely essential. But the real world goes very fast, and to make it a bit sharper, some of the attacks we can only follow with the help of artificial intelligence because they go so fast that we need artificial intelligence to follow the pattern of attacks and how they are shifting. And so we will have artificial intelligence talking to artificial intelligence somewhere else, telling, you know, it looks

like there is an attack going on here. So we are starting to put our autonomy in the hands of artificial intelligence. And you've got a fantastic what you're discussing about trust in your podcast and TrustTalk, trust in artificial intelligence is starting to become a real important theme. Do we want to give that out of our hands because we have to do it as the world is going so fast and only artificial intelligence will be able to do that? But is artificial intelligence then allowed to take a decision to say, switch off half of an electricity network to stop spreading the attack? Question mark? We don't know. That's a thing, well, I'm trying to set it up, but it's certainly a thing we need to think profoundly about, and this has huge political consequences.

Interviewer: Another important field where trust plays a role in e-commerce, for flourishing e-commerce, important preconditions must be safeguarded. Security, trust and reliability of the digital infrastructure. Given what you just said, has Europe a role to play here?

Paul Timmers: Now, I find it a very interesting topic, because in the very early days that e-commerce was coming up, I had actually the privilege in the European Commission to work on the first -commerce policy. And at that time, we were thinking about, of course, all the opportunities that internet commerce would be bringing. And we started also to think about some of the security and trust issues. For example, you need to be able to have reliable payment systems, you need to be able to identify yourself reliably. And a lot of that has been done by the private sector, but also part of it has been done by governments. And so let me just give one example. Governments are issuing electronic identification means, which may be a smart card or maybe through an app. And these electronic IDs are now usable all throughout Europe. So as a matter of fact, I can get access to public services in Austria with my Belgium electronic ID. I can sign my tax form in Belgium if I want to, which my Estonian electronic ID, which are all recognised under the law and technically they are interconnected

Interviewer: same with the corona checks?

Paul Timmers: Exactly. That's a similar actually a similar kind of technology underneath to interconnect these various systems and to do that importantly, with minimal information disclosure. So the next stage that Europe is going to do is come up with a wallet in which you have things about yourself like, you know, I'm a professional, I have a professional education. My age is more than 18, and a wallet can be used linked to your electronic ID, so it gets a legal

status, it can be used to tell something to a service provider. Yes, I'm older than 18, but I don't need to tell exactly my age, it's minimal information and how do I know it's true? Well, because it's backed up by government this type of declaration. So it's like your passport is backed up by your government. Now, so Europe plays an active role there. Countries are, of course, at different stages. Just one other example. Private sector has also been very active in this territory, and Europe is worried about the role of the big platforms that they are perhaps too powerful, that they are controlling too much and are to a degree, anti-competitive. And so Europe is also proposing laws like the Digital Markets Act that essentially says if you are a big platform provider, you cannot keep everything in your hands. You have to unbundle somewhere and including, for example, on the ID system, which will give people more choice. And let's be honest, you know, if you identify yourself with your electronic ID everywhere that you get from your government, it's very convenient and it's trustworthy. I live in Belgium and actually it does work there, so I use it almost on a daily basis, and I don't need to have a Facebook ID for that.

Interviewer: To conclude our interview, my last question. What would be the best division of roles between government, private sector, civil society to enhance trust in our digital life, whether in economy, society or even democracy?

Paul Timmers: Yeah, it's, of course, easy to say that everybody has to play a role. I's true, but I think in many instances you actually see there is an unbalance, so civil society is not always as much at the table as others. Private sector sometimes has the lead, where actually governments should also be on the table. You mentioned 5G. 5G security is actually an example where private sector was moving ahead and ultimately did deliver something of which government said, well, this is not quite the security that I need for my national security. What has happened here? So getting these parties around the table in a balanced way is something we have to do. It's a challenge to achieve it. But that will actually also enhance trust because then these parties see each other when they talk about AI, they say this is the type of, AI we call, trusted AI. We have an understanding about that. When they talk about encryption, same type of story. I know it's very difficult to get to deals in such a setting, but then it's what we need to do because otherwise we put an imbalance in trust. You just have to say, well, just trust your provider. But we know cyber attackers love that type of statement because the provider cannot always be trusted or the user is then becoming the weak spot. So in the interest of trust,

soft trust and hard trust, these parties need to be all around the table. From topic to topic it will be different, but it's starting, the principle is essentially we need what they call with this horrible word "multi-stakeholder" approach. We need to have that and take that seriously, and we can do that also supported by law. You know, that's also where innovators can be at the table. I don't believe at all that this will stop innovation. I don't think it's the case. There is a lot of creativity that comes, for example, from the civil sector, even if the civil sector may be a bit more careful about the protection of your personal data, then you want to be as a company. So, yes, I think that's a thing that has to happen. Just one additional word about that. We tend to think that we can ultimately have everything in our hands, but we should not be naive about how much technology is actually conditioning the way we work. So we also need to carefully think about the kind of technologies that we want to have and whether they make it possible for us to work together as citizens, private sector and governments. And some technologies are designed in a way that they gave, for example, all the control to the state. Well, that's not the kind of deal we are talking about.

Interviewer: I was referring to democracy in my question. And of course, that is a big issue. You can have all the technology advancements, but if it is in the wrong hands of governments that you don't want to have the technology, then we all know what can happen.

Paul Timmers: Exactly. I mean, if you have a fully distributed solution where there is no central point of control, it's very hard for a government to start controlling all the citizens. Perhaps that's what we want. But if you as a state, well, actually, as we see in some states, don't like all of this democratic debate that happens and you want to keep that under control, you will not be happy with all kinds of distributed solutions. You will want to have a centralized solution. So you see the technology architecture kind of mirrors the social system that we and democratic system that we have. And that's why this debate that we have about trust and technology is going really to the foundations of the kind of society that we want to have.

Interviewer: Well, thank you very much for being our guest today, and I wish you good luck with your further research on this subject.

Paul Timmers: My pleasure. Thank you very much, Severin.