Transcript of IIC/BEREC Telecommunications and Media Forum 2021

Day Two – Thursday 27th May 2021

Panel 2 – Paradigm shift for secure connectivity and critical infrastructure provision

DAN SJÖBLOM: So hello from one point in the programme to another, I hope everyone is feeling prepared for continuing straight away. We have a very packed programme for you here today. Welcome to this section of the programme. We will focus here on secure connectivity and critical infrastructure. I am Dan Sjöblom, I am the Director General of PTS Sweden, this year also Vice-Chair of BEREC with special responsibility for amongst other things, external relation issues and I will be the moderator in this session that we're opening here now.

In 20 minutes or so we will have a panel discussion with a great set of people, with various responsibilities in our ecosystem, and they will share their views on secure connectivity and infrastructure. But before we start with that, we will have a conversation with Mr Tareq Amin who is the group executive Vice-President and Chief Technology Officer from Rakuten which is, I am sure you all know, a Japanese company that has a wide range portfolio with products and services and the discussion will focus on the topical issue of open RAN. We're indeed very grateful that Tareq has been able to join us, I believe it's very late hour being live from Japan. How you are doing Tareq, is it still midnight?

TAREQ AMIN: No, no fantastic, it is still early for us in Japan, right about 6 o'clock here.

DAN SJÖBLOM: Ok, so it's not too bad.

TAREQ AMIN: Not at all, thank you very much.

DAN SJÖBLOM: Are you ready to go with questions we have lined up for you?

TAREQ AMIN: Absolutely.

DAN SJÖBLOM: So I would like make to start painting us a little bit of a picture what is open RAN evolution, what does it look like in the short to medium term, what will it enable for us and maybe can you even give us glimpse of you vision not only 5G but maybe even into 6G.

TAREQ AMIN: Absolutely. Let me start a little bit, maybe just give you a brief context about Rakuten's journey as we embrace a new platform architecture to connectivity. I joined in 2018, Rakuten, with an ambition and dream to try to build a disrupted platform architecture built on the merit of security, diverse supply chain, hardware disaggregation and embracing cloud in the essence of what we do, to drive agility, lower our infrastructure cost and drive better services and affordable for our consumers in Japan. One of the key tenets to enable this was of course open RAN, and open RAN as I am sure most of you have come to read about and understand, has become a very interesting debate item in the industry. While it's really gathered this attention, it is no doubt that telecom operators across the world today spend north of 70% of their capital expenditure on radio access. To understand the reasons and motivation to why we need to evolve, one much appreciates the past, how networks were deployed and networks were always deployed based in vertically integrated stack, integrated hardware with proprietary hardware with software. The essence of cloud really never existed in the DNA of traditional telecom infrastructure.

With open RAN the idea came about, where we wanted to disaggregate and have full control on the enter bases, full control on vendor intraoperability, and the goal and objective of course was to lower cost and economics and burden of deploying infrastructure. The second thing is really as an aspiration goal is to move from the network that always requires hardware upgrades, to a network that is always evolving through software upgrades. The analogy I would give you is equivalent to what you have seen in the IT industry with the adoption of cloud. It drove amazing agility, amazing innovation, we want to do the same thing with open RAN and the adoption of open RAN so the first

thing we have done is complete disaggregation of the radio, adoption of baseband deployed as software on our edge data centres, and a massive automation that enabled elasticity, productivity, and efficiency into our architecture that we have deployed in Japan.

Maybe lastly, I will tell of course you when we started this, this was really a dream. It wasn't really simple for us to go and enable this idea of this massive hardware disaggregation, cloud enablement in every function in the network but it required a substantial investment in our side to create a willing ecosystem of partners. Partners that believe on pushing the vision and strategy for the better good of the industry, and better good for consumer and I think better good for society and enablement of digitisation. So this was really our initial approach in Japan and of course I will tell you today, with over 20,000 [inaudible] both 4G and 5G fully compliant to all RAN standards fully deployed in Japan, we have validated and proven that this model is valid, this model is scalable, it delivers on cost and economics, and you know we believe that this is just, we're in the early days of scratching the surface of what is possible on infrastructure modernisation, and infrastructure cost reduction through automation and cloudification in every function in the network in Japan.

DAN SJÖBLOM: Fantastic, you didn't mention the term 6G but maybe we'll come to that later.

TAREQ AMIN: Let me, if you don't mind, let me take one minute here just to talk a little bit about the Gs in general, because a really important thing, I have been in this industry for such a long time, and you know if I recall maybe the first 30 years of my life as we went from 1G to 2G, to 3G to 4G, the process of network modernisation always had a the function of hardware replacement. We change one hardware to a new hardware, that's where we see the complexity and cost infrastructure and the affordability factor becomes always a concern for us. So for us, what we want to call it today a 5G network or tomorrow's 6G, the first thing that we needed to focus on I believe, before we get completely excited about a terabyte wireless infrastructure network, we thought we want to fix the foundation and foundation is a day in which network upgrades is done though software and not done through expensive hardware upgrades. Our view is we are more

than engaged and more than delighted about the potential of what a terabit network is going to offer to consumers. The first thing we owe everybody is a massive transformation on the foundation of how you build, engineer, architect the telecom networks of the future.

DAN SJÖBLOM: Great thanks Tareq. Let's turn a little bit to engagement with regulators. I understand you have been in contact with quite a number of regulators and we're hear a little bit later in the panel from Ofcom on maybe some of their aspects on this. But maybe if you tell us a little bit what from your perspective, what do regulators need to think of in terms of enablers and supervision of these new kinds of network, how does it change the game for a regulator? What has been the reaction up to date when you have met with regulators and explained and discussed open RAN issues?

TAREQ AMIN: Indeed, I really had the privilege and opportunity to meet regulators in the region we're in Asia and Asia-Pacific, and regulators in the United States as well as in UK and Europe, and the discussion point started by most of the regulators are intrigued and they wanted to understand more. They wanted to understand the use cases of open RAN to their geographies, to their existing mobile operators, and the benefit it could bring to the larger areas. I am going to give you, my discussion maybe with the regulators in Japan because obviously they have been extremely supportive and my early days of discussion really revolved around technology exchange and technology education, to ensure that we explain the merits of a cloud native open RAN platform networks. Our regulators were very concerned initially about stability and quality and rightfully so, because we needed to ensure that when we build mission critical platforms such as telecommunication network, they need to work 24/7. Service interruption is not acceptable and we needed to prove to the regulator the merits of such technology, we needed to prove the resiliency, the healing function we have led to deliver on what we call carrier-grade telecom network.

Those discussions in Japan were met enthusiastically by the regulators, and they wanted to really engage and embrace a discussion in which they encouraged, you know, a future blueprint where we believe that this is where the future blueprint of telecom networks need to be. Now, when you look at the regulators globally, I would tell you their objective

is also the same. Most regulators I believe, had a common objective is to drive competition, to drive efficiency and offering to end consumers and to make sure that digitisation across society is enriched by new technology like 5G, but digitisation cannot be just limited to only urban, dense urban area. We have to find a way to expand this to suburban and rural areas. This is where open RAN technology and open cloud native architecture enable a much lower cost point for telco operators to embrace adopt and obviously spread and widen the coverage footprint, increase digitisation.

So I think this has been met with, so far I really will tell you that we have received extremely positive reaction from all the regulators that we talk to, I think now the discussion point needs to revolve around the enablement and in a way I would say maybe a slight rewarding system to reward innovation and advancement in technology that would enable operators to deploy this, not only in the urban centres of their network, but to diversify this in their rural areas and suburban areas to accelerate 5G rollout or even in the future, 6G, across their markets.

DAN SJÖBLOM: Thanks Tareq. I will get back to the topic of innovation in a moment, I just wanted to raise one more point from a regulator perspective, see if you have any views on how the topic of open RAN would impact the traditional means of allocating or selling spectrum. Is there a relationship or an impact?

TAREQ AMIN: Yeah, this is, you know, I mean, I would tell you this is such an interesting point that is worth debate. Obviously, I personally have worked in United States, I worked in India and I worked in Japan and observed different characteristics to how spectrum is either auctioned or allocated. So most countries including the US, in which there are spectrum auctions that happen, that operators compete and spend a considerable amount of money to acquire spectrum and in Japan it's quite the opposite but the spectrum has been allocated.

You know if you asked me personally, I mean I think what I have observed in Japan is really a fantastic system. I mean it's a system that is built on ensuring massive digitisation and massive acceleration of enablement of modernisation of infrastructure, is all allocated in Japan and I think with open RAN, the regulators have now to look at interesting

viewpoints. The merit of spectrum sharing, and the merit of spectrum allocation versus spectrum auctions, I personally think there is really a valuable merit to what I have seen in Japan compared to other markets, and the evidence of this is a really amazing infrastructure that exists in this country and you know it's helping all of us, including Rakuten itself and the operators in Japan, to allocate and spend capital to accelerate the build out in 5G, to commit to building 5G not only in urban areas, but to reach rural areas. So I think with open RAN and most importantly open architecture with cloud native networks, now regulators have to think about the mixed-use spectrum use cases. One is the shared spectrum access philosophy, unlicensed spectrum and I think of them will have a role to play in the future technology architecture once open RAN gets materialised in a much larger scale than what it is today.

DAN SJÖBLOM: Great, so let's get back to innovation, there is I think a bit of an ongoing discussion about the open RAN on innovation, and some may say it will stifle innovation, less incentives to innovate into something that is proprietary and others will say it will enhance innovation because it will open up opportunities for newcomers and so on. What is your view on innovation and how can we, as a society, be convinced that this shift is positive?

TAREQ AMIN: I mean I am of the opinion, my opinion is quite the contrary. I think open RAN and cloud architecture is going to drive a massive transformation in telecom infrastructure. The analogy I advise everyone to think about, what would have happened if we had not had cloud platform serving IT industries? Think about the, all the platforms that we all enjoy today, including the streaming service that we are talking through today, the massive OTT applications that we cannot really function without today; that was all driven by adoption of cloud and adoption of distributed computer architecture.

Now open RAN requires a cloud native thinking in its DNA, let me give you a specific example of Rakuten's story in the early days because it might help you to understand what we have done to enable disruption and innovation but that was not at the cost of disrupting the business model of larger established equipment vendors. In the early days of Rakuten and mobile, I spent an enormous time with Nokia, with its Board, with its and leadership, convincing them that there is a business model in which Nokia that will sell

Rakuten, the remote radio head and they would enable the software through one of the subsidiary companies LTO Star. This relationship requires unbelievable engagement with Nokia, and to be honest with you our approach is we wanted to prove to Nokia that there is a viable business model, and I give Nokia lots of credit. They have taken a courageous step to move into this undiscovered territory, to discover a new business model.

We have innovated at every facet of this network. We have innovated on disaggregation of radio and hardware, we have innovated on massive edge computing platform deployment. We have innovated on massive automation to enable zero touch provisioning, enable lower cost of infrastructure to enable lower cost of services to the consumers and all of this happened by creating an ecosystem of willing partners including, I would say what we, including Nokia was involved in this process and still a critical partner to Rakuten today.

So I think open RAN and cloud native networks are exactly what telecom networks need to innovate. Innovation through proprietary hardware is a thing of the past. People that believe in cloud, people that believe in software, people that believe in AI and machine learning would believe that the future DNA of networks are networks that are built in the concepts of full autonomy, enablement of Level 4 autonomous network. That can only be enable by architecture transformation. And we are really a big believer of course in this new architecture, but we also believe that, you know, existing, large equipment manufacture have an amazing role and amazing contribution to do for the larger ecosystem and I am glad to show that everybody, the participation of large European vendors in Rakuten, how they helped and continue to help while making a considerable amount of revenue, of course, for their shareholders and for their corporation so we think it's an amazing opportunity to continue this innovation cycle.

DAN SJÖBLOM: Thank you and I will come to my last question here, it's about the topic of the day; so the security and resilience, and what are the practical results of open RAN seen from your perspective on those important topics?

TAREQ AMIN: I think security is critical by the way, and for us when you think about

security, you know the first thing that came to my mind, I don't think of security as only in software architectural security. This is a very broad topic that required us to rethink the entire apparatus of what our zero-trust network architecture that we wanted to do in place. The first thing that we wanted to push is security around supply chain. So maybe one question that I would ask a lot of people is, do most telecom operators know where the parts inside their platform comes from? Where they are engineered? Where they are manufactured? And what is the source of supply chain across the entire ecosystem?

So the approach that we have taken, by the way not just on radio, I am talking radio, core, transport, OSS and BSS, the first thing that we needed to ensure is one 100% visibility. Remove all the black boxes from this network architecture and start engaging about understanding supply chain engineering, component manufacturing, the source of the factories, where they come from, and then apply the, you know, the right software architecture whether it is around secure certificate architecture, identity management, all the premise architecture that we needed to put in place. So what I tell everybody is first thing about securing anything that you own is about visibility, and with open platform and open networking architecture the journey starts with visibility first and then we wanted to even drive this further and we wanted to own the entire supply chain discussion including understanding the components, what they are manufacturing and where they come from. I think this is really, you know, a never ending journey to ensure that security should be on top of mind and security, to me, is a massive responsibility of my job, and we obviously take this very seriously that we need to stay ahead of the game and ensure this product is secure, is hardened and all that the right visibility across the board end-to-end is provided to us to ensure that nothing is going to come to intrude with our operation and nothing is going to impact any sensitive data that we store on our platform and our network, and no malicious hardware will be deployed and commissioned in our infrastructure.

DAN SJÖBLOM: Thank you Tareq, this has been great. I think we could have continued this for quite a bit longer but our programme is filled with interesting things. I will say thank you very much for joining us at this late hour in Tokyo and until next time.

TAREQ AMIN: Thank you very much. Bye bye.

DAN SJÖBLOM: So we would, will now move into the panel part of the programme. You have seen that panellists have been asked to share their perspectives on topic with the links with resiliency and the vibrant and diverse market, what can regulation do? Supply chain risk mitigation is something many of us are thinking about and how to achieve the best out of flexibility of intraoperability of components and a high level of security. We will have, I hope, some diverse views. We have five panellists; they will all introduce themselves for roughly 5 minutes and I will just introduce all of them now and then we can pass the word quicker between the different interventions.

So first out will be Julie Ruff, who is the Head of Sector for Secure Value Chain of DG CONNECT at the European Commission. She will be followed by Yih-Choung Teh who is Group Director for Strategy and Research at Ofcom in the UK. Then we have Lorelien Hoet who is a Government Affairs Director for the EU at Microsoft Corporation. Florian Damas, he is Head of Policy and Regulatory Affairs at Nokia Bell, and finally Jimmy Ahlstrand who is the Chief Corporate Affairs Officer for Telenor here in Sweden.

So first up is Julie, you have the floor now for approximately 5 minutes.

JULIE RUFF: Thank you very much. I hope you can hear me very well. Good morning everybody. I have the pleasure to start the panel and maybe I say a couple of words about the big picture first, which is probably all well known to you but I think it's worth underlining first that 5G role out is a major property for the EU. You are familiar with the new targets we have and the announcing the Digital Decade so full coverage of the populated areas by 2030, so very ambitious and for that, there is a lot of effort invested in setting the right regulatory instruments around its policy tools with the implementation of the Codes, with the connectivity toolbox and also in terms of funding. There is 20% earmarked for digital under the recovery and resilience facility, so that is going to be a lot of funding available for digital projects and connectivity is one component also there.

I will move directly to security aspects and also of course touch upon open RAN in this context. As I said timely and fast deployment of 5G is number one priority for us and the objective is, of course, to make sure this is done in a secure way. I think everybody acknowledges that. We heard from previous speakers the importance that they also give

to security and we are reminded of that every day. Looking at the news for 5G networks it's really paramount and it's going to be a strong basis for mission critical services, and we also want to ensure uptake in consumer trust. So for all these reasons, there is a lot of work that has been invested already at EU level into strengthening the security of 5G networks. Concretely, what have we done and what is going to happen in this area?

First of all, you may know, of course, about the process of the past two years that led to an agreement among Member States about common approach through the 5G cyber security toolbox. This was based on the very thorough risk assessment something really unprecedented where Member States collectively worked together to collectively identify the right measures. Now we are in the phase where Member States are putting in place those measures in their countries and we also see that they remain very committed and we're continuing to work together with them at EU level, to exchange information, to encourage as much convergence as possible between the approaches.

We are also taking steps at EU level to support this such as, the launch of a request to prepare certification scheme in the area of 5G. That is something that help should address some technical risk and should come as a complement to other measures that need to be taken in this regard.

I will also mention that now looking forwards, 5G remains a very important element of our cyber security strategy, so the toolbox is not the end of this process. The new Cyber Security Strategy that was published at the end of last year announces some further steps that will be taken and identifies objectives for the future including some strategic objectives, I will come to that in a second. But I also want to mention the revised proposal on the NIS Directive which aims at including the telecom sector also under the same umbrella as other critical infrastructures which we think will be a valuable step.

In all this context supply chain security has taken greater prominence. So there is a lot of emphasis put on supply chain security and resilience in the work of 5G cyber security, but also in the NIS Directive there are new provisions about supply chain security requirements, about the possibility to conduct joint risk assessments to look at critical supply chains and this is because first of all it is a major vector of threats and it's also

very important from the perspective of EU strategic autonomy, has an important place in our industrial strategy also.

We have identified in the past months of this crisis, quite painfully, that vulnerabilities in supply chain autonomy can have very negative consequences.

Now just as a last point, to come to lead to the discussion before on open RAN, well, very clearly, we are looking with great interest into this evolutions and the Commission is really already investing in supporting software based networks and projects in this area, and I think nobody is disputing that it's going to bring a lot of interesting potential opportunities. So we're following this very closely. At the same time I think at this point, you know the pitch on the benefits the opportunities is starting to be well-known, and at the same time we feel that there's a need to analyse thoroughly a couple of aspects, so I will name them quickly. Of course the maturity of the technology, how does this link with our deployment targets. We would like to avoid a situation where operators would want to differ the rollout of 5G networks, to wait for certain technologies to be fully maturity. Then there's a cost benefit dimension that also maybe warrants a bit further assessment. Integration challenges in energy efficiency, EU capacities *et cetera* these are all aspects that we're now want to look seriously into.

Last but not least, of course, security. So we really want to be in a position to have a full picture of security implications, both from regarding the opportunities and the potential risks, that could you know arise from the new threat surface, from integration challenges, from complexity *et cetera*. So both the benefits and potential challenges, and Member States have come to the conclusion that the 5G toolbox offers an appropriate framework to conduct this analysis, building on the experience and expertise in this area. I stop here, sorry I might have been a bit full on.

DAN SJÖBLOM: That's perfect, thank you very much Julie, very dense and compact presentation of so many things that are going on, and we get back a little bit to that particular fact that so many things are going on. But right now I am handing the floor over to Yih-Choung Teh for his introductory presentation.

YIH-CHOUNG TEH: Good morning. I feel privileged to join this discussion with brilliant

experts from around the world, so my thanks to the IIC and BEREC. I wanted to start on reflecting on why innovation in network technology and services is so valuable to people in businesses. New and emerging technologies of just a few year ago are now widespread have transformed our lives. For example as we were hearing, cloud computing has not only brought cost savings and efficiencies, but it enables us to access our documents, photos and music wherever we are, on whatever device we choose. Over the top communications have revolutionised the way we communicate globally, with smartphones our most favoured device. Of course video conferencing platforms have been crucial throughout this pandemic without which we wouldn't be hear in this panel session today.

Ofcom has duties to further the interests of citizens and consumers and encouraging investment and innovation is vital to making that happen. As part of this we are committed to ensuring we have a healthy competitive supply chain that supports innovative new services, while ensuring high levels of security. Operators in the UK and globally are going through major architectural changes in their networks as Tareq was saying. This coincides with the development of 5G, but it affects all generations of their tech. Examples we have heard include virtualisation, where network function traditionally implemented in an identifiable box are now brought forward in a software module with no fixed location, as well as edge computing where functions are brought closer to users, in some case on cell sites in mobile networks. Reduced cost, greater flexibility and increased choice of vendors are all reasons for this technological shift. However, the implementation and management of these changes is very different from traditional operations, that challenges operators' skills and the relationships they have with their partners.

Alongside these architectural changes, concerns over the lack of diversity in the telecoms vendor market have come to the forefront, due to the phasing out of so-called high-risk vendors across many countries, including in the UK. As a result, there's a desire for operators to broaden out their vendor base and I suspect they have good commercial incentives to do so as well. No-one wants to be beholden to a single vendor, but the choice of alternatives is limited at the moment. At Ofcom we're focused on ensuring we understand emerging technologies and support the wide range of vendors and parties

working with the UK government and others internationally, to achieve and more diversified telecoms supply chain.

In the last year, the UK have been leading important work in this area. The UK Government formed an independent task force to advise on interventions for diversification and published its 5G supply chain diversification strategy, backed by an initial £250 million budget. The strategy focuses on three main pillars, 1) supporting incumbent vendors, 2) attracting new suppliers for the UK market and 3) promoting the adoption of open intraoperable solutions. Open RAN fits within the third pillar which is Tareq said, enables the disaggregation of the radio access network, or open RAN functionality with open interfaces and that should help new vendors to enter the supply market.

Ofcom is at the centre of this innovative work. Next month, we will launch the Smart RAN Open Network Intraoperability Centre or SONIC Labs for short. This is a joint programme with Technology Body Digital Catapult, backed by the UK Government, to create a platform for new existing suppliers to test and demonstrate intraoperability and integration of open and software centric networks solutions, starting with open RAN. We will use the SONIC Labs test bed to evaluate directly the readiness of standards for intraoperability and integration. Now, the barriers of entry for a start-up in the mobile industry can be very high, so we want SONIC Labs to enable and encourage new vendors from UK and abroad to be part of the UK ecosystem.

Finally, we want to build a testing ground for longer-term technology and open RAN is a step along the way. For example, we highlighted some of these long-term technologies in our flagship Technology Futures Report published in January, covering not just mobile in wireless, fixed and optical and emerge in immersive communication services.

Tackling the lack of diversity in telecom supply chains is a global challenge but at Ofcom we are playing our part in supporting industry to overcome some of those barriers, and supporting innovation is key to this. We will use the expertise we gather from the SONIC Labs test bed to enable, stimulate and promote innovation. But we will only succeed in tackling this global challenge by sharing what we learn and partnering with you and others

internationally. Thank you very much.

DAN SJÖBLOM: We look forwards to hearing a bit more once that SONIC Lab is up and running, it's an interesting approach to some of the issues that we all are facing indeed in terms of getting a good market out there. So, without more ado, you will come back later on in the panel discussion I will pass the floor over to Lorelien for her introductory remarks.

LORELIEN HOET: Hello, thank you also to the organisers and thank you to all the panellists for the great contributions so far. I would like to spend a few minutes on thinking about the regulatory framework for resilience in cyber security of critical infrastructure and telecommunications in particular. and 5G of course. I would like to start with what Julie already mentioned is that draft Commission proposal for the NIS2, extends the scope of the existing Directive, includes the telecommunication services and proposes actually to exhaustively regulate the telecommunications security under NIS and to repeal the corresponding provisions from the EECC.

I have seen that BEREC questions this approach - sorry there is a lorry working just here. See that BEREC questions this approach, but I would like to answer this but before doing that I think it's important to look at the questions a bit more holistically, because the NIS2 proposal interrelates not only with EECC, it interrelates also with others sector specific regulations, like in the financial sector we have DORA. We also have the discussions on energy specific regulation, maybe health specific regulations, so we need to look at the full picture. Also, the NIS2 proposal interrelates with the proposal for CER Directive which is the Critical Entities Resilience directive. It's important when in order to have, when looking at all those pieces of the puzzle, that the resilience framework is put together in a logically and well-structured way we believe, in order to keep the consistency, and the legal certainty. Practically and concretely we think it's logically very logical as the NIS proposal has done to start with the horizontal approach, looking at the resilience requirements across sectors, and to set the foundational layer, and then to see sector specific whether additional requirements are needed. Therefore we think that NIS proposal makes very much sense.

Another reason why we think the NIS proposal makes sense, is that the EECC has been

expanded in scope recently and does not only encompass traditional, usually network based services, but also cloud-based services like OTT, and obviously with NIS covering cloud computing it makes perfect sense also to cover these, so to say, new telecoms services, together with the NIS, again in order to achieve consistency.

Another point I would like to pay attention to is the geographical scope of resilience regulation. We see that digital services are increasingly being offered cross-border. Cloud computing, that's clearly the case, but it's also the case for many IoT services or other innovative telecommunication services. We also see that cyber risk's, cyber-attacks, are cross-border. They don't stop at borders, clearly not. There is a general acknowledgement of that and also a general acknowledgement that it's important to work together, yet we also see that there is a national interest to control also cyber security questions at national level. That becomes very apparent if you look at the implementation of the EU cyber security toolbox where you see a myriad of different solutions of how this is being implemented nationally. Of course, national interests are key and it's logical that nation states want to take care of their cyber security at national level, but we plead also for a greater need for harmonisation and co-ordination and alignment in order again to keep the resilience framework consistent.

Maybe the last word that I would like to say, is on the topic of cyber security certification which has been mentioned by Julie already. Indeed, because we think that in this complex environment, of resilience regulation but also complex digital environment, cyber security certification could probably be a very useful tool to bring to, let's say, to determine the foundations of resilience requirements in a harmonised way. The cloud scheme is already ongoing, and Julie has mentioned that the 5G cyber security scheme is being prepared. It has been, I mean it's clear from the previous intervention, that 5G and 6G will become more complex. Open RAN more diverse, so to say, open RAN, cloud computing, but also at the retail side we will see more private networks we believe and specific tailor made B2B solutions. They if you start looking at 5G cyber security certification, we think it's important that the ‘new kids on the block’, open RAN but also CSPs, private networks are consulted and that these elements can be taken into account in the new cyber security certification scheme.

DAN SJÖBLOM: Thank you very much Lorelien, another reminder we're looking at a very diverse and complex environment, we need to be prepared to have allocate the resources necessary to be able to manage that jointly. That's an excellent introduction. I will pass the floor on to Florian for his introductory remarks.

FLORIAN DAMAS: Good morning Dan, good morning the panellists and the attendees, and thank you for the invitation from IIC and BEREC. First, as an introduction I just want to remind that the COVID-19 crisis has accelerated the digital transformation which has actually become a solution to many of the challenges created by lockdowns and physical distancing. The impact will resonate for years to come in the transformation of business, healthcare and education, creating a digitally literate society in which technology has the potential to support democracy, and restore public trust. The digital transformation of government and business plays a central role in Europe's post-COVID recovery and digitisation is key to empower, innovation and entrepreneurship, bolster the EU competitiveness and economic resilience, enable the green transition and strengthen European values and prospects for European citizens, and telecom technologies like 5G, fibre, artificial intelligence, cloud are especially critical as they are the essential enablers of the digital transformation. 5G is transforming our societies and economies and is boosting the fourth industrial revolution and 5G connective is one of the central building blocks in the interplay of sensors and data analytics to machine learning, artificial intelligence, high performance computing, autonomisation, and all will profoundly impact all sectors of the economy.

So what is the role of 5G and ORAN in network virtualisation in post-COVID recovery? First, as 5G deployments advance and we prepare to work towards 5G stand-alone deployments and the industrial Internet of Things, service providers and government have begun to take a closer look at the potential benefits of having an expanded ecosystem of mobile access players in the market.

So the future of open RAN has become a central subject of discussion and of strategic importance. While today the radio access network equipment of one vendor is typically intraoperable with the co-equipment of one another vendor, the different module or units within a given radio access network architecture has to be provide by a single vendor.

The concept of open RAN consists in opening the protocols and interfaces between the various building blocks for network components: radio, hardware and software and the Radio Access Network and by disaggregating the RAN component and leveraging open interfaces, open RAN will allow for a multitude of different vendor products to be used in one and the same Radio Access Network. This may stimulate new entrants and business models as the Rapporteur highlighted, and extend the current competitive set up to a multi-vendor marketplace.

Open RAN is independent from the common cellular innovation cycles which here impress visions from 6G but rather a potential evolution of the setup of the 5G network architecture. So what is Nokia's view on open RAN? We strongly believe that industry stakeholders must work together to create a path for adoption of open RAN. This must be done in collaboration with communication service providers and trusted vendors, each contributing to the standard definitions including open RAN interfaces and defining a technology driven plan for adoption.

Nokia has provided an initial set of open RAN functionalities in to 2020, whereas a more completely suite of open RAN defined interfaces built on top of Nokia's as scale software is expected to be available in 2021, this year.

We are ready to engage with partners and Governments to advise on how to set up conducive public funding programmes and to participate in concrete lighthouse products to develop, trial and deploy open RAN based connectivity solutions.

In this way we can expect initial deployment in Europe in the near future with open RAN enabled deployments predicted to gradually overtake traditionally RAN deployment over the coming years. And Nokia is committed to delivering on the 5G transformation and we believe as a well-coordinated effort around open solutions will contribute to this success of this journey. That will be my introduction.

DAN SJÖBLOM: Perfect. Thank you very much Florian and we will get back to you very shortly when we get the panel started. So last out among the speakers with introductory part here is Jimmy, you have the floor for your 5 minutes.

JIMMY AHLSTRAND: Thank you Dan, and thank you for having me on the panel. I am

here to represent Telenor. We are perhaps not known to everyone but we have a solid 160 years of experience in providing communication networks and we have 187 million subscribers across Northern Europe and Asia. My perspective in this panel will be the operator's perspective, and from that perspective I would like to raise three major points.

First, when it comes to security regulations, we see a need for predictable regulation and the long-term perspective. We operators are to invest billions in our networks and the 5G network that we build right now should work for a decade or more, and that network would be the digital grid that European competitiveness is built on. To be able to do those investments, we need stable regulation, secure regulations, for certain, but stable regulations otherwise we will see less investments, less broadband coverage, less innovation and less growth for Europe.

Currently, the new regulations are coming in with such a speed that authorities literally doesn't even have time to implement it before there is a new proposal. We should have strong regulations in this area, but when we have worked it through, as we did with the EECC, we should stick to it and allow it to exist for some time. Therefore, we believe that when it comes to these two, this might be a counter argument Lorelien, we believe that we should continue to have the telecom specific regulation in the code instead. So, predictable regulation will be my first point.

Secondly, I like to stress the importance of having equal security regulation for all competitors in the field, not to distort the market. This is important, not the least, from a security perspective. A competitive perspective, of course, but also a security perspective. To give one illustrative example, in Sweden we have stronger security regulations for mobile operators then for fixed operators and this means that fixed providers, all things being equal, can undercut mobile operators on price, driving consumers to less secure solutions.

So, therefore, regulation needs to be coherent across the - between the different market actors but also across the value chain and not all responsible for telco security issues should therefore be put on the operators. Providers of different key technologies and services, vendors in different fields are best placed to identify and solve the vulnerabilities

in their own products and services before they are spread across the whole supply chain. So we think that regulations should be broad in that respect and cover all parts of the value chain.

Third and last, I would like to stress the importance of working together, both within the countries, between authorities and market actors, but also between the countries. Security is something that we build together, not on our own, and that is not at least true for Europe with its many countries. What we see today is an increased fragmentisation of the regulatory landscape, based on partly the security arguments and we see this development as a risk. Not the least from a security perspective, we do not need perfect harmonisation, but some harmonisation and not at least operators need to be able to work cross-border to set up the strongest responses we can towards different cyber security threats. In that context, nationalistic regulation and strong demands for national autonomy, for example, can hamper those cross-border security solutions and therefore we want to see increased opportunities for building cyber security across borders.
I think I can stop there and hand back to you Dan, thank you.

DAN SJÖBLOM: Thank you, Jimmy. I like the part about co-operation and I think in the perfect setting here with a wide national coverage of the programme that we are having.

So with those five introductory statements there we are now about to move onto the question and the answer session, part of the session, and I should just mention that I believe you out there in the audience, if you have burning issues you want to raise with the panel, there is a means for you to submit the questions and there is a system for us to get those questions into the platform that we are using for the panel.

Sorry I wanted to say that and I think the first question to my five panellists would be perhaps if anyone, having listened to any of the other panellists have any immediate reactions or comments that you want to make at this stage? So, the question is for anyone who wants to grab the floor and say something about what you've heard from any of your co-panellists.

JIMMY AHLSTRAND: Jimmy, if I may start and I didn't commend on open RAN which is, of course, critical and many of my fellow panellists talked about open RAN and we heard

about Rakuten, and then the diversity is really critical for us as an operator and we at Telenor have a multi-vendor approach. For us, open RAN is a very welcome initiative and we support it fully. However, it also has to be noted, as was made by some of the speakers before, that it is a technology that is not fully developed yet and when we build regulation we must build it on facts and not assumption, which means that we think that is right by the governments and others to supporting the initiatives, but before we build regulation we must see that it really works.

DAN SJÖBLOM: Okay. So that's open RAN and we will be discussing open RAN a little bit later here. Anyone else that had any comments on co-panellists, I think the pictures are very small so just --

YIH-CHOUNG TEH: I am happy to come in. Thanks Dan. I am just going to comment on Jimmy's introduction actually, where I think the three points in principle that he sets out are very hard to disagree with, I very much agree with those point. As a regulator, we completely get that predictable regulation is really important. Indeed, in a different area on the fixed regulatory side we have just finished our market review of access networks, and essentially put in place a framework to try to encourage full-fibre deployment, thinking about a 10-year horizon to provide certainty for investors.

On equal regulation, across the value chain, again I agree and one of the challenges is as we move into a software dominated world, I think that is a real challenge for regulators to understand how the different parts of that value chain are going to move to show that there is a level playing field. Then, of course, on working together, I share those comments that as an independent regulatory in a global marketplace, particularly when it comes to mobile vendors and issues of open RAN, we need to work collectively together. In the UK we represent maybe about 2% of total vendor revenues. So we won't get very far by ourselves and so partnering with other regulators, governments, operators, vendors is absolutely critical for us to be able to move forward.

DAN SJÖBLOM: Thank you. I don't see anyone else in those tiny picture - oh Florian, yes, go ahead.

FLORIAN DAMAS: I would like to make two comments because we are talking about

ways when you entrance to run the software on commercial off-the-shelf cloud computing platforms. The reason why also established vendors have custom made system on the chip hardware solutions is to ensure that we meet the targets when it comes to energy efficiency. So we have to be careful between everything on the common platforms and also the objectives of the Green Deal to reduce energy consumption. So, that is my first comment.

The second comment, as some of the panellists have said, since open RAN is a natural technology evolution, respective deployment should be market driven and not mandated. Its introduction will take this gradually as the open RAN technology matures and it should be left to the telecom operators' choice of how to design their respective network architecture.

Now the regulatory environment should rather encourage and incentivise the development and voluntary adoption of open solutions, while taking Europe's strategic consideration of maintaining tech sovereignty in cellular connectivity into account.

DAN SJÖBLOM: Okay, perfect. Let's move a little bit deeper perhaps into open RAN opportunities and challenges. We have heard many things starting with the presentation from Rakuten and the discussion there, many of you mentioned in your opening remarks to have the opportunity presented by open RAN for increasing vendor diversity in the Radio Access Networks. Reducing cost was mentioned I believe, increasing the speed of rollout. We also heard some comments about security, intraoperability, views largely were on the positive side but if you listen to the discussion there are cautionary statements being made as well. So I think the first question for the entire panel is in your view, what are the main remaining challenges to solve, if we want to fully unleash the potential of open RAN here in Europe for example or elsewhere, but let's focus on Europe for this discussion. How can we work to overcome those challenges? Who wants to start? Yih-Choung The, yeah go ahead.

YIH-CHOUNG TEH: Thanks Dan, happy to make a start and for others to come in. I think what Tareq and Rakuten have done is absolutely brilliant and really inspiring, very encouraging in terms of how we can get a lot of the benefits he described through open

RAN. I think one of the things that strikes me in Europe certainly in the UK, is that the challenge is that we have existing mobile networks with existing deployments and incumbent vendors and I don't really see an opportunity any time soon for someone to build a completely brand-new network in the UK. That leads then to the question of integration with legacy networks how quickly that can happen. That's into the straightforward question it's partly where we're coming from in terms of our SONIC Labs' test bed, an opportunity for vendors big and small to come and test how that might work and prove intraoperability, but I think that is a challenging process which will take time and there will be other test beds to try to help that migration point, that's the biggest challenge for us, that it's not a green field site we need to worry a little bit about backwards compatibility with existing legacy kit.

DAN SJÖBLOM: On that point, are you working with mobile operators in UK for that test bed activity?

YIH-CHOUNG TEH: Yes, absolutely. We have been all going to UK operators as well as of course incumbent vendors and prospectively interested new vendors, and the SONIC Lab's test bed is very much an early stage of technical readiness to try and provide a little bit of support to those who don't have R&D skill to come in. The UK Government have bigger ambition in terms of a UK telecoms lab which would take that to a much bigger level and provide capacity and capability to try and help that process of integration and intraoperability.

DAN SJÖBLOM: Very interesting, we'll keep track of that development. So, yeah, Lorelien.

LORELIEN HOET: I think, so, outside of this panel I have heard sometimes views about open RAN which are a little bit more pronounced like you have this, there's seems to be a distinction between believers of open RAN and the non-believers. I think we should try to stay away from such dogmatic discussions, because that's not worth it honestly. It's all about innovation, and embracing innovation, and indeed working towards supplier diversity, which is, which can be good for resilience, but which obviously also brings challenges which have to be looked at, so I think it's important yes, like with any change,

there are clearly upsides but there are things that have to be looked at and that shouldn't be neglected of course, and, but, I would like two stay away as much as possible from these black and white discussions that we sometimes hear.

DAN SJÖBLOM: I like that comment, I think as regulators we often try to pride ourselves as being technology neutral, so the discussion and the while we're talking about open RAN here it's not because we're particularly want to support that technology, it's because we want as you say to have the ambition should not be implementing open RAN, it should be having secure, reliable networks with sufficient diversity in supply chains. It's indeed a very good comment. Julie? I think you're on mute. The most common comment in these kind of conferences ever.

JULIE RUFF: Sorry, and it still happens. So thanks a lot, I just would like to support and echo what was said about the need to have a more sophisticated approach to this issue, and it's not about being for or against innovation, absolutely not. So on our side we really want to find the way to support innovation, in the best possible way, and at the same time, to articulate this with the other very important policy objectives. The timing targets, really important. The security objectives, and also the sustainability objectives. So what we feel is that we only starting to scratch a bit the surface of these topics, and we're working with experts to look more in depth into this and maybe three things.

First, we are trying to identify a bit better the various scenarios for deployment, so what is it short-term, mid-term, long-term, what kind of use cases will be the ones that open RAN will be more suitable to support, *et cetera.* So we're looking at this because it has an impact, and then on the other policy decisions, to try to understand what may or may not happen. Then from a security perspective, as I said earlier, we don't think we have fully analysed everything yet so that's also important to in order to have the confidence, to move forward and with trusted approaches. Then, of course, how can we foster an innovation friendly and good environment for new players, including existing and new players, so that is also something that is central to our reflection. To finish, of course, diversity as you just said also Dan, is important. It's important for resilience, it's however not an objective in itself for us, the objective is resilience, and security and then we want to see what's the best path to achieve that, to maintain that, and well at this stage we're

also looking at the impact of this new technologies and solutions. In terms of diversity, short-term but also long-term, so might be a lot of things that may happen, as a result of these very exciting developments, and we would like to have some questions about that to see also what are the conditions to realise this resilience objectives in the best way, in the sort of futureproof manner. Thank you.

DAN SJÖBLOM: Thanks Julie. Florian?

FLORIAN DAMAS: Thank you. So I mean, two reactions. First, it's not a black and white world. Aside from this open RAN ecosystem we're working on, we are already working on 6G as well and there's EU's objective called 6GX project with key EU players which also funded to see which innovation we can bring in our future mobile networks. The other thing is on open RAN you know does it solve network security and the resilience challenges? Well, open RAN is not more secure per se, rather on the contrary it creates new security challenges which can, and must, be solved. The potential variety of network elements originating from different vendors will need a considerable system integration effort which is scaling in an expensive manner. Products and solution from different origins are being included in the network so a requirement which instead of being a one-off action, needs to be understood as a continuous ongoing process. Even regular software updates. This will present a challenge in particular to security, as security needs to be built into the overall system, in early on in the design phase, rather than being added on late in the process, with solutions defined in the integration phase.

Furthermore, the open RAN is meant to diversify networks it still requires the same security checks and certificates for all. In the future, more segmented network element as RAN and core components requires today and existing ones relating to system integration. Therefore, the concept of security and trust outlined for instance in EU 5G toolbox, apply equally to open RAN.

DAN SJÖBLOM: Yep, very sensible comments. I think I saw Jimmy raising a hand, I hand the floor over to you Jimmy, if you could whilst commenting also give us your take on what kind of development will we see in the short to medium term. How much open RAN will, do you as a company foresee to have in your various networks in the years to

come?

JIMMY ALSTRAND: I think I will answer that question but I make my point first because it relates to Florian's and on the security angle, and I think one aspect of the security aspects to open RAN, and where I think, which I think is important for regulators in particular, is that the security setup, or the model for security in an open RAN solution would be a bit different than the typical historic solution, that we have had. As many of you know, we've undergone an extensive review of the parties that want to provide 5G in Sweden, a security review, and I would say that the regulatory framework that was used in that context wouldn't have allowed for an open RAN solution, I don't think so, at least it wasn't tested by any operators so we can't know for certain, but I don't think open RAN would have been allowed and in particular by the security authorities. Therefore I need, if we want open RAN to be one alternative for the future, then I think the security agencies need to, as they are in certain countries, be involved in the discussion and also educated on how networks are built *et cetera* so that's, and I think that is a role for the telecom regulator to have a discussion with the security authorities. on that. That was related to Florian's but that is also part of an answer to your question Dan. I don't think it can be a solution, at least not in short to medium term, for Telenor Sweden, but Telenor as a group is a different thing. We are definitely exploring different ways of working with open RAN as part of our broader set up since we are so committed to the diversity. But for Sweden I would say not in the short to medium term.

DAN SJÖBLOM: Ok, thank you. Lorelien, yep, please go ahead.

LORELIEN HOET: Sorry, I would just - maybe this just a bit of a like playing a little bit the devil's advocate, because we hear so many different views on this element of supplier diversity, and security. Honestly, I think sometimes yes of course, when thereafter other more suppliers and there's intraoperability, the security discussion becomes different. That's a fact and there are questions that need to be looked at I would like to, nonetheless, place a critical note with the statement that it becomes immediately more challenging. I mean I have heard in the cloud world we hear very often the point that it is important to have supplier diversity precisely for the resilience, so I think we should try to be consequent in that sense.

DAN SJÖBLOM: Yep, thanks, well I think it's not black and white as we have heard, and many aspects come into the resilience and the security discussions that we are having. I think you mentioned a few of them I'm sure that there are, there will be developments and I think also Jimmy's comment about the impact of other agencies than the telecom regulators is something that is going to become more pronounced as we move into digitised societies where telecoms services are really the basis for so many sensitive societal services. As you said, this is it's something which is, I think, we were in the beginning of this phase and much more will come.

Does anyone want to say anything more on open RAN before we move onto our next topic? You seem to be ready to move on, and I will remind the audience that you can still submit questions, if you have any.

Now, we thought we would talk a little bit about the pace of change of legislation, not least in the area of security. This links, as we have heard, to investments, to foreseeability and how much risk is it reasonable to assume that investment is supporting. So, we see a lot, we have seen over the last years many new proposals, regulations ongoing beyond the Code which in itself was a huge legislative programme. There are many, many things coming out on as we talk and cyber security, of course, is very key among those.

A lot of the activity addresses relevant issues. It is useful to add all of these layers of new legislation, no doubt about that. But how is it impacting us, I think that is a little bit of what we want to discuss here and want to hear the views of the panel on the pace and scale of regulatory activity, focusing maybe a little bit on that coming out of the European Commission. Looking, also, at whether we are hitting the right targets and whether there are means to work with regulation in any other way which is putting the burden on the ecosystem, different from what it is from today when, I think, we are all feeling that there are so many changes going on and being an expert on everything that happens is going to become more and more challenging over time.

So with that sort of question, maybe it is logical to ask Julie as a representative of the European Commission, to say something about whether this pace is necessary, useful and continuing. What is your view on this stage of new legislation?

JULIE RUFF: Thank you Dan. Well, so, first of all, of course, not surprised that regulation is not a favourite for industry in general, and we understand those concerns and but I think it's really at the heart of how we are doing things. So, in the Code and the review of the Telecoms Framework is something that was precisely met to clarify the scope and the conditions as much as possible and ensure the predictability and the harmonisation that you have been talking about.

Then we've tried to compliment that with some policies, like, the, what's in the connectivity toolbox, so lots of toolboxes but there is one about how to facilitate the rollout of networks and simplify procedures, et cetera, reduce costs. So we are taking an approach to try to enable as much as possible rather than to put constraints.

So that is one side and then there is the security area, where I heard several remarks. Well, I think, the effort around creating this 5G security toolbox was precisely to try to have a common understanding of the risks among Member States. A common methodology to analyse those risks and then a common set of measures that can be used. We are seeing that Member States are committed to apply this methodology and at the same time, we can't avoid that there will be variations in the modalities. First of all, because there are different ways of doing things on security but also because there are different analyses of the risks and threats at national level which necessarily have to be taken into account too. But I mean still, there is a lot of effort that has been invested to try to make this as consistent as convergent as possible and we will try to continue to work towards that.

Then this is the bit the same, also, objective we had with the proposal on NIS2. Bringing telecoms into that framework has the objective of, sort of putting things in a consistent framework together with the regulations on cyber security for other critical infrastructures which are also all interrelated, and we do not think this will lead to any major disruption or new rules for the providers necessarily. It's really very much just a change of umbrella at EU level and governance [audio interference] framework on cyber security which should see the opportunity also to the supervisory authorities which are in charge today to become part of this community and I think it is very important to create those bridges so the telecom regulators and the cyber security authorities and everyone is part of the

discussion at EU level on this.

But this is very much something that will affect the EU co-operation, whereas at national level we do not see that this will have a major disruptive impact on the current way of doing things. So, yeah. I think that is all I wanted to answer to this question.

DAN SJÖBLOM: Ok thank you, Julie, and with that I think I will open up comments from the remainder of the panel about the pace and scale of new rules coming your way. Yih-Choung.

YIH-CHOUNG TEH: Yes, I mean for me this is a question, I think, of trade-offs and timing. At least I would say those are the things that we need to be very, very mindful of. You know, obviously Jimmy has the operator perspective but what I would observe is that there are lots of pressures at the moment. So obviously on security where in the UK we have been concerned about high-risk vendors and we have quite a lot of Huawei equipment in our networks and a big debate about how quickly some of that should be reduced and eventually removed. So a reduction to 35% over the three years and by 2027 for that to not be in our 5G networks. That obviously drives costs for the operators, but then as we have just been discussing with open RAN, we have a long-term view of the security concerns that aren't just going to be dealt with by prohibiting certain equipment, but that, of course, requires a different sort of investment, and that adds costs as well when we then look at those new technologies. And, of course, we want to say at the same time well we want to have the rollout of 5G networks as quickly as possible. So please get on and spend money and do that too. And we just had a spectrum auction in the 3.6 to 3.8 Ghz, arguably it didn't result in as high payments as some people thought, but nevertheless that's another cost. I am mindful as a regulator you have to have a good understanding of the commercial reality of how all these things are going to get squared. As you were saying Dan earlier, when it comes to the security issue we work very, very closely with the National Cyber Security Centre so we understand what the level of threats are and that risk assessment. And somehow the government has to consider those things in the round when we think about some of those trade-offs and the timing of how realistic I think some of these things are. So that would be my broad observation.

DAN SJÖBLOM: Thanks. Maybe for the audience it would be interesting to say a few words on no longer being part of the European Union. How are you relating to what comes out of the process in Brussels, so moving forward. Is that something that you can address in sort of general way?

YIH-CHOUNG TEH: Yes, very generally. I mean we implemented the NIS Directive that was whilst we were still within the European Union. We have updated guidance and revised some of that recently and we spend a lot of time working with operators of central services in that domain it is really, really important and I think the security issues will increasingly be in that domain.

I like to think that despite the fact that we have left the European Union that we continue to have very good relationships with BEREC and other regulators, including yourself and other panel members, and for me that is critically important even if we are in a slightly different course now. It goes to some of the points about harmonisation. I think, political developments are interesting where there is a certain degree of national focus but as we have discussed whether it is cyber security threats or whether global supply chains, I am not sure those are, you know, very good respecters of national boundaries. So, if anything, I would say the fact that UK has left the European Union makes me want to work all that harder in terms of our international partnerships and our relationships. I think that becomes even more important because some of those fora are not ready made for us the way that we have had for many, many years.

DAN SJÖBLOM: Thank you. There was a little bit of a side issue but I thought it would be interesting for you to say that to the audience and that sounds very sensible indeed. So back to the question on the amount of regulation coming your way and what about you industry representatives, how are you coping with engaging in these new areas. Jimmy, please.

JIMMY AHLSTRAND: Yes, first let me start, it's often assumed that industry players want, less regulation is good regulation, but I wouldn't say that. We think that good regulation is good for serious actors such as ourselves. So, we are not hostile to regulation as such. We think that keeps bad actors away from the trade, which is good for everyone.

However, the speed of change is a problem within itself. I think we have just in this country, four or five different major regulatory changes within the supply chain kind of field for telecom operators, and when you try to build a network as I mentioned should work for a decade or more, of course you need to do changes during that time, but when regulatory changes are put in that make you change your network in a way, that then are prohibited, it creates problems. I think, the consistency between different regulations could be, could be better actually. For example, national regulations compared to the EU toolbox agenda, that is why I called for a bit more harmonisation before. Not total harmonisation because we, of course, understand that different nations must make their own judgment on what is best for them, but some harmonisation and consistency over time is needed.

DAN SJÖBLOM: Thank you. Florian, no? Lorelien?

LORELIEN HOET: Yeah. I can fully subscribe to what Jimmy said. Again, I think really, what the Commission has done within this proposal to try to look at this holistically and I think we really need to do that. All sectors are getting digitalised. So there needs to be a set of foundational requirements that are similar across all these sectors, and through I hear that BEREC - the telecommunications sector is special because it is the foundation but that also goes for other industries, like cloud or energy and every regulator will think that his or her sector is special. I am closely involved in the DORA negotiations, with the financial regulations and DG FISMA and they think the finance sector is also very special. So it's, if you end up doing this in a very fragmented way, sector by sector, you will have overlaps and inconsistencies. We have seen those already between this and EECC in the past where we have seen some countries implementing both.

So really we think working first at the foundational layer, horizontally and then look sector by sector which additional add-on elements are still required, is really the best way forward, and of course Jimmy I understand your point that you say, you cannot throw away the existing telecom regulation and that needs to be accounted for in this, or somewhere. The existing framework cannot, must be respected or changed in due timing but I do insist on the needs, I think, the Commission has really chosen the right way forward with the NIS2 proposal and to make a plea, I think we should even extend that to

the financial services but that is another discussion.

DAN SJÖBLOM: Thank you, it's good to hear that everyone is special. Florian do you want to comment on this?

FLORIAN DAMAS: Yes, indeed so. I also support Jimmy's message when it comes for the need for more harmonisation and regulatory consistency. I will just give one example about the NIS2 proposal. So, we have the Connecting Europe Facility II emphasising on the importance of having cross-border 5G and fibre network and deploy digital services over these networks. The question is directly about the NIS2. If we include now communication networks and services to which supervision will be, which competent authority will be the supervisory for these specific cross-border networks and that's one of the questions that we have for now. Just to be pragmatic.

DAN SJÖBLOM: Ok. Did I see Jimmy asking for the floor again?

JIMMY ALSTRAND: To add to that the competence of the authorities. To us I think we both understand each other Lorelien, but for is it's having the telecom regulator as our main regulator and having the telecom regulation in the EECC brings us more clarity, we think, perhaps dependent also on the history of the regulation and that it has been built over quite a long time, and we can't really foresee the exact consequences of moving it. However, we do see a need for regulating other parts of the supply chain, within for example the framework of NIS2, so we have a coherent regulation, which is not putting all the regulatory burden on one part of the supply chain, but rather covering all different parts of it, or the most important.

DAN SJÖBLOM: Ok so we have -

LORELIEN HOET: Just answering that, we are both in the telecoms framework and in the cloud computing so I think we will be in scope, if that reassures you.

JIMMY ALSTRAND: That's good.

DAN SJÖBLOM: I think that's also something which is not unique to this discussion about NIS2. The way that digitisation is affecting our societies it's quite often stretching boundaries. We find many of the things we are discussing now with the DMA and the

DSA proposals also, are little bit new to us in the sense that they don't really fit with the traditional agency structure that we're used to, sort of putting things simply. I think it calls for more collaboration and more co-operation moving forward that this might be another area. I want to get back to Julie on NIS and see if she has any updates for us on what is to be expected as we move forward here with the NIS in terms of timing if not in substance.

JULIE RUFF: Thanks, well in terms of timing I mean I am not the one sitting in those negotiations, but I hear that it's progressing well, so the Council finished the first part of the work reading through all the whole proposal, and so ready also to go to the next phase and so is the Parliament. So they are also advancing. So I think we will see you know important steps taken after the summer on this. Well, cannot predict when it will end, but it's going well, and I think we see a lot of support overall, for the approach that has been proposed by the Commission so we're confident that we can you know overcome the different issues that have been raised, because there was also indeed some issues and some things to clarify a bit further, one of them is being is indeed the articulation with sectoral frameworks, so this is something that we will work a bit on.

But to come back again to the specific point of telecoms, and you know again we really would like to try to reassure that we do not see the scenario that you fear materialising, in the sense that here we're talking about very high level requirements, in the Code, versus also quite high level requirement in the NIS Directive and what has happened over the past years is that the national regulators have developed that into practical measures and guidelines, and we really see that those guidelines will fit equally in whatever, regardless of the umbrella instrument at EU level. Of course, I mean technology evolves, security threats evolve, so things might need to be adjusted, but we're not talking about revolution here, and NIS2 of course includes a number of a couple of new requirements such as, I said, the spotlight on supply chains security, but that goes also into the direction that you mentioned, that you would like to see the whole environment considered, so that is a bit of a new dimension. But overall for the rest the basic security requirements that are set out in this proposal, are fairly in line with what was in the Code, and there's also no prescription as to who should regulate or not at national level, so there's no reason to

suggest that something to change should change as a result. So it's something that the NIS2 doesn't address, and it's for Member States to continue to determine how this is being done. But we see benefits, we see that it can bring all the actors together under this common umbrella, that instead of having to find complicated ways of making sure everyone is round the table, because we have different fora, *et cetera* for discussion, we would clearly have one place the NIS co-operation group where the discussions can take place, which really facilitates the consistency that you are calling for. Also, at other levels of operational co-operation, CCER et cetera, we have all this governance framework it's in the NIS community, and context so we would just encourage you to take another look at what is proposed and consider also those positive improvements.

DAN SJÖBLOM: Thank you Julie. Jimmy?

JIMMY ALSTRAND: Yes, and I understand that perspective, but I think also from our perspective, we need to think of the regulation, the NIS2 regulation or NIS regulation, but NIS2 in this context in relation to not only the EECC but also to different national security regulations, and that makes the situation even more complex for us. I am not convinced that it will create less complexity for us, even if it might do that on other parts. I also do not agree that it's basically the same requirements. At least as we read it in the proposal for example, there are new reporting obligation that would be quite complicated for us to live up to, and we think for example that reporting should prioritise significant actual incident and not potential ones, such as reporting on threats, because that's very hard to define basically. So we think that there are both issues that we have with the substance of the proposal, but also with organisational setup and the regulatory framework as such, where we prefer the existing one.

DAN SJÖBLOM: Ok, this turned a little bit into a discussion about the NIS2 proposal in particular. I don't know if anyone in the panel has further questions, or comments on that proposal or more generally the topic of the amount of new regulations that we're working on. Yeah Lorelien?

LORELIEN HOET: Maybe just one additional thought, it has been mentioned several times by Jimmy, also by Florian, that harmonisation across borders is also important and

I think we, I mean this is important of course to avoid the red tape and administrative burden, but this is also truly important in order to stimulate the digital single market. I think that is maybe not sufficiently taken into account sometimes in practice. How important it is to have a basic level of security requirements across Europe that is sufficiently harmonised in order to allow innovative services to take up.

DAN SJÖBLOM: Ok perfect. I don't see any raised hands so I think we can, with some 20 minutes left on, oh Florian. Please.

FLORIAN DAMAS: I mean I would like also to emphasise on international co-operation, since we're looking at the security aspect. Member States and also EU authorities should really follow topped greatest extent possible international and European standards as well as voluntary industry initiatives in regard to network security and risk management, and the one I want to point out is for example, the GSMA NESAS, which stands for Network Equipment Security Assurance Scheme. The overall objective is to provide an industry wide security assurance framework and security baseline to facilitate improvements in security levels across the whole mobile industry. I see benefits, major benefits for different stakeholders. For national policy regulators and the European Commission, I see that as a security assurance scheme readily available for their use and increase effective security while not negatively impacting the industry, but also it helps to avoid fragmentation of security requirement, across the global market. There are also really benefits not only for mobile networks but also for equipment vendors. So NESAS is designed to be recognised and adopted by regulatory authorities and the scheme provides the methodology, the security requirements and test cases necessary to support a robust security framework.

DAN SJÖBLOM: That was almost perfect on cue, because I was going to say that I suggest we move for the last part of the panel into a little bit of a discussion on what we can do in order to better achieve international co-operation in practice and focusing maybe a little bit on this area of security and resilience, that is sometimes a little bit challenging as we have heard more national initiatives there than in other areas. On areas such like technical harmonisation, normally thinking it's easier to collaborate and I think the fact is there for a long time. But when it comes to threat analysis and things like that

that may be different in different countries, what is your view? How can we do this better? I think it's a good panel to discuss this because I we have three representatives of really global companies here and we have a regulator who is not an EU regulator, and we have a regulator who is part of the European Commission. So I think we're in good company for a discussion. Can we take the international co-operation/harmonisation further in this area, and how can we achieve that in practice? Does anyone feel prepared to give an initial thought, I think Florian you may already have given yours, I think, but others - maybe if you just confirm it's more on the technical side if I understood you well.

FLORIAN DAMAS: Yes indeed, it's more the technical factors, absolutely Dan. I mean maybe I can add one point is that maybe the NIS2 could actually formally task NESAS with developing guidelines on security measures to map, to be mapped against relevant standards and certifications. That would be as a means to demonstrate compliance for both essential and important entities. I think that would be an important task which we would support.

DAN SJÖBLOM: And maybe if I ask the industry representatives here a little bit. How much is this discussed in your companies that you have different developments? I mean, is this seen as a major issue or is it something that you are coping well with or in between, where are we? Lorelien.

LORELIEN HOET: Yes, for us no surprise. This is obviously an important topic and I think as Microsoft we have on several occasions pleaded publicly for more international co-operation in this area. We also need to be realistic of course. I mean we cannot - we can hardly expect that, I mean, this is something that doesn't happen overnight. Of course, it would be better if all the standards were the same across all the world for us, but that's not realistic and that wouldn't also fit with national sovereignty, so but at least within Europe and especially for digital services which are cross-border, we think it is really, really important to work with stronger harmonisation and that will allow Europe to have a stronger voice in the international discussions we believe, and, yeah so...

DAN SJÖBLOM: Thank you. I think I saw Julie?

JULIE RUFF: Yes, thank you Dan. I maybe I just react right now on that point and that

point by Florian about certification and standardisation. So this is actually happening. So we have the Cyber Security Act which allows us to develop certification schemes for the EU. So EU-wide certification scheme, and earlier this year we've tasked ENISA to start preparing a certification scheme for 5G networks. In our discussions, the discussions that we had with Member States we clearly came to the conclusion that a good approach will be to take into account what has been already developed by industry, so it is really something that we want to partner with industry in moving forward with this scheme.

Of course, we want to build on international standards in all the work that we do on certification as much as possible. It's in our interests and we know it's in industry's interest that we take this global perspective, but of course we will also need to take into account the perspective of the regulators and then the needs from a public interest perspective.

So this is only just starting now, but it is a very important process. At the same time we need to be clear about what certification can and cannot do, so you know, according to the toolbox clearly there is a role for several different measures that should be applied jointly and certification is there and we can convince that it can help support, help address certain technical risks up to a certain level. So we are working towards that, to have this tool as well as the others, available. We think it is the best way to do this jointly instead of having every Member State develop its own certification approach. So for that we are already looking at something fully harmonised down the line, and at least that's our goal. But, yeah, again, I mean that doesn't take away the need to address other types of risks that were identified in the coordinated risk assessment that we did with Member States, but that is clear at this point. So, we will look forward to continue the dialogue with you also while we progress in this process.

DAN SJÖBLOM: Thank you Julie. Maybe a question more for you Julie, can you say anything about what the Commission is doing in terms of discussing these kinds of issues with partners outside the Union?

JULIE RUFF: Yeah, sure. I mean, obviously, 5G security, as we know, is central, key topic for also our partners, our main partners. So it has become almost a standard agenda point you know in every discussion that we have around digital. We are

discussing also security issues. We are discussing 5G and 5G supply chain developments. So, there is clearly there an interest from our side but also from the side of our partners to talk together and see how best to reach common goals, common objectives, but, of course, there is also a different level of maturity in terms of positions.

So, now we have the 5G toolbox and we can engage on that with third countries, whether it is to co-operate or to also share our experience and knowledge in this area. We were doing a lot on this front. But then moving back to the topic as we discussed earlier about open RAN, about generally evolutions in network approaches, there I think we feel like we need to develop our European way maybe before we can move forward like, really constructively. This is something, as I said, we are working with experts in all sorts of fields to determine what's in the best European interest and then of course, while at the same time being very mindful and interested in what others are doing. Thank you.

DAN SJÖBLOM: Perfect, thank you. Anyone else on the panel? Yeah, please, Yih-Choung Teh.

YIH-CHOUNG TEH: Thanks Dan. Perhaps a less technical answer to international corporation and you know I believe that is critically important for us. But I thought two practical examples, maybe I will give you three. When it comes to open RAN and diversification and I think, we really, really value the Five Eyes partnership we have other countries on security matters. For example I was speaking to the FCC chairwoman just a couple of weeks ago about open RAN and our teams are working very closely together, and I know she is about to join us shortly.

Secondly, on security risk. I am sure people will have seen the FluBot spyware issue we've had recently, text messages are sent to Android phones. So we have been working very closely with Google in how we think about combat that. Finally, a little bit of a different example I guess, but as many of you will know we are preparing to take on new duties beyond the telecom space into online safety. That, of course, is a really challenging endeavour and very much a global one. So, I was speaking with the Microsoft CEO in the UK just a couple of weeks ago. For example, about the Digital Crimes Unit which I think is an amazing resource that Microsoft has with its Windows footprint across

the world to be able to detect issues, scams, fraud that is happening earlier and so I think these partnerships are absolutely critical in terms of how we pool our resources together to essentially make a lot of these online challenges more feasible as we look to make the internet a safer place.

DAN SJÖBLOM: Thank you. So, I think we are slowly going towards the end of this panel, I think it has been a very - it provides a lot of insights for me. I don't know does anyone want to have a last go at any of the topics we have been discussing? Jimmy, please.

JIMMY AHLSTRAND: Yes, yes, a short comment on the last discussion that we had. Of course, we absolutely support international standards and certifications and also working together on the European level but I think what was mentioned about the Five Eyes co-operation, for example. We must also be prepared if countries are not ready to give up authority to the European Union in certain areas then we should open a more bilateral co-operations as well. That would make it easier for us to build different cyber security threats or build technical solutions to counter cyber security threats.

DAN SJÖBLOM: Perfect, thank you. Just scanning the panel here. I think, I don't see anyone really seeking the floor. So, I think I will give you a digital big hand of applause for your contributions to the panel. Thank you very much. I think we've heard quite a lot of common ground. I think on open RAN there is a lot of interest, it holds certainly potential. It may not be a silver bullet and we need to continue to work with it and see how it fits with other policies, with installed basis and many things like this. We have also had, I think a good discussion on the amount and need for more regulation, more cross-cutting regulation and the impact that digitalisation has on the type of regulation that we will see. We had a specific deep dive into these two and it will be interesting to see how that continues to play out in the debate amongst legislators in Brussels, I am sure we will all follow that closely and now finally, I think we all share the common ground that more international co-operation, both inside and outside of the EU will be needed. I also should just repeat that I very much look forward to more reports on the sandbox activity that the UK is setting up for testing some of these new open applications. So, again, my great thanks to the panel, and I believe I have to hand over to the BEREC Chair

Michel Van Bellinghen, for the next point on the programme. Thank you very much.