Transcript: Eric Xu's Interview with UK Media Outlets

Date: February 13, 2019

Location: Room 106, Executive Training Center, Huawei's Bantian Campus, Longgang District, Shenzhen, China

Moderator: Eric Xu is the Deputy Chairman of Huawei. And he also fulfills the role of one of the Rotating Chairmen. He's been with the company for 25 years, and he is very much in charge of R&D, strategy and the company's technological investments.

For the briefing today, our intention is to focus on strategy and R&D. If you have got questions about the situation in the UK, I understand Eric is happy to deal with those. Okay. Unless Eric wants to make any remarks, we'll start with questions.

Eric Xu: It's pretty challenging to talk with friends from the UK press. Because there are so many things going on related to the UK. Therefore, it is a challenge for me personally whether I can adequately answer your questions, but I will try my best to answer whatever question what you may have. Thank you for coming.

Steve Cassidy, PC Pro: My question is one about how you divide your R&D activities. What is your sort of balance of priority between basic physics and research and customer-led feature development?

Eric Xu: Huawei has established an R&D management and investment system that is similar to that of other industry players but is also somewhat different. Our R&D processes and management system has been put in place with the help of IBM, they provided their consulting services to Huawei. And the name of the process is IPD, Integrated Product Development. We engaged IBM since 1998. They helped us build up our R&D processes and management system, and those systems and processes have been there till today. In these processes and management systems, there are both investments for the future, essentially research and innovation, and also product development that is oriented toward customer requirements. Part of it is also investment into engineering capabilities and techniques, essentially around how to develop the products that we put to the customers. So, there are three parts for R&D related investments, and we have a separate budget for each piece when we look at our annual business plan, and we have dedicated governance teams to make related decisions in terms of how to spend those R&D investments. For the customer requirements oriented part, or what you say the functionalities and the features, the decision-making body is IRB or IPMT, or Investment Review Board and Integrated Portfolio Management Team. Those bodies would make decisions on what to develop, what not to develop, and when to deliver.

Steve Cassidy: How long is that review cycle? Is it once in every six months? Once in every quarter?

Eric Xu: The review cycle is not monthly. It's not quarterly. The review cycle is based on what we call checkpoints in the R&D process. And then for research, innovation or patents producing investments, the decision making body is called ITMT, Integrated Technology Management Team.

In history, the average percentage of research and innovation related investment is around 10% of our total R&D spending. But we have increased this percentage over the recent years to around 20%. And we hope we can get to 30% in the future.

So we have dedicated teams, dedicated budgets, and also a related decision-making body to govern and manage this future-oriented investment, and that's also where a lot of our patents are produced. At the same time, we have a pretty big team, as well as corresponding decision-making mechanism for developing products to meet customer needs in the market.

Take 5G, for example. It was the ITMT who made the decision in 2008 to initiate our research efforts on 5G. I announced this news in the UK that Huawei would invest 600 million US dollars in 5G research. Even until today, 5G research has not been fully completed. But 5G product development, based on our research findings, was started three years ago, and that decision was made by our IRB or IPMT.

Tamlin Magee, Computer World: If there was any point in history where the lights went on for 5G being strategic and a core strategy for the company. You said in 2008 that the technology doesn't exist yet, but in X number of years, we can win over this market.

Eric Xu: It's not as great as you depicted. There is a certain rule to follow, a certain pattern of history when you look at the mobile communications industry that we are in. After 2G, certainly there would be 3G, certainly 4G would follow and then we have 5G. What's in my mind right now is 6G.

After 4G products are out in the market, from a research point of view, certainly our teams would be looking at 5G. Actually, 5G is not a term of any single technology. It's a generation of technologies for mobile communication.

After the research efforts of 4G are completed, naturally our teams would be doing research around the next generation of mobile communication technologies. 5G is the sum of those next generation mobile communication technologies.

The research effort for 5G would be basically completed by 2019, and our research teams will be looking at questions, such as how mobile communication technologies would evolve in the future? What are the technologies that might be put into the category of the next generation, or 6G? So they are going to organize their research and creative activities around those sort of questions. I anticipate that by 2028 or 2029 or 2030, we are going to see 6G as extensively discussed as we are seeing 5G today.

So this is the pattern or the rule of our industry. If you do not work on 5G at all, that means there is no future for you. **For every new generation of technologies, some companies cannot follow up, and some companies will emerge even stronger.**

Robin Pagnamenta, The Daily Telegraph: If you have any response in particular to Mike Pompeo's remarks about the role that Chinese companies can play in the rollout of 5G? Given that we have seen some Germany and France seeming to indicate that they are not

necessarily going to follow the US lead on this, whether that's a sign that China is winning the argument?

Eric Xu: I certainly cannot comment on whether China has won the argument or not. I saw Mr. Pompeo's remarks made in Hungary yesterday, and I saw his remarks in Poland today, but of course it was Chinese that I was reading.

I think Mr. Pompeo's remarks are just yet another indication that the US government is undertaking a well-coordinated geopolitical campaign against Huawei. It's essentially using a national machine against a small company, as small as a sesame seed.

Huawei does not have a long history, but we are a 30 year old company. Serving more than 3 billion people across 170 countries and regions.

What kind of a company we truly are? I think our customers, the partners we work with, and the 3 billion plus people that we serve would have a very good understanding. So we have been wondering, and I think many other people may have been asking this question, is the recent fixation on Huawei truly about cyber security, or could there be other motivations?

Are they truly considering the cyber security and the privacy protection of the people in other nations, or are there possibly other motives? Some other people argue that they try to find leverage for the US-China trade negotiations. Some other people argue that if Huawei equipment was used in those countries, US agencies would find it harder to get access to the information of those people, or find it harder to intercept the mobile communications of those countries or their leaders. I believe in the wisdom of the 7 billion people in the world. I think they clearly can see these different possibilities.

Yuan Yang, Financial Times: I saw your media interview with the German press, and you mentioned that cyber security is partly politics or ideology-related. So if cyber security is about politics, if the US government has political motivations, how would you see the ultimate outcome in, say, five to ten years time down the road, in the sense whether the cyber world, the technology community would be divided into one China-led, the other US-led. Personally, I would agree with you, even though I do not speak on behalf of the Financial Times, whether there is technical viability for that.

Eric Xu: Cyber security in itself is certainly a technical issue that requires expertise to address, and that's also what all the scientists and engineers in the world have been working on, trying to address cyber security.

In that context, Huawei has been working with different governments and industry partners to hopefully put in place agreed standards, so that people can take those standards to measure how secure the products from all of the vendors are.

Recently, we have seen the close coupling between 5G and cyber security, and I think people know clearly what the sources of those coupling are. When we look at major equipment providers for 5G, you have Nokia, Erickson, Huawei, Samsung, and ZTE. As you can see, there is no American company here. China and Europe have been working together, trying to put into place a unified global standard for 5G and also the future of mobile communication technologies, in order to reduce the overall cost and improve return on investment for all of the players in this industry.

Through the concerted efforts of the industry, we are seeing a unified global standard for 5G. That means all of the players can follow this one standard as they develop 5G-related products. But now, some politicians have turned either 5G or cyber security into political or ideological discussions, which I believe are not sustainable. Because I believe technology is technology. Ultimately, it will depend on scientists and engineers to make it happen. I believe scientists and engineers would prefer a unified global standard so that people can follow this standard to develop better products.

Of course, when we look at different countries, they certainly have the option, considering their own specifics to choose the right vendors they see fit when they deploy their networks. That's natural when we look at the history of the mobile communications industry. Huawei's 4G equipment is not deployed in all of the countries in the world. And we certainly do not expect our 5G equipment to be chosen by all customers in all countries. Rather, we would focus on providing good services to the countries and telecom operators who choose Huawei. To give you one example, China Mobile Guangzhou did not choose Huawei’s 4G equipment, even though Guangzhou city is so close to our headquarters. So I think this is quite normal. And you know the market size of Australia is even smaller than China Mobile Guangzhou. Our equipment is not used by China Mobile Guangzhou, so I think it's quite okay that we are not chosen in certain countries. We have limited capacity. Certainly, we cannot serve all customers in all the countries. And certainly we cannot dominate the entire market – even in (some) markets that are very close to our headquarters, our equipment is not used. So this is really normal in our industry. Rather, we would remain focused on serving the countries and customers that are willing to work with Huawei.

Oscar Williams, New Statesman Tech: There were reports over the weekends from Politico that Donald Trump is considering an executive order to ban Huawei equipment in the US. I would be interested in hearing your thoughts on what impact that would have on America's ability to roll out 5G and how worrying that is – the prospect of having a global superpower drop the support for Huawei. How worried you are about the prospect of a country of America's size banning Huawei?

Eric Xu: First, I want to share with you that Huawei's infrastructure equipment is basically not present in the US market. And even smartphones now are virtually not present there. In history, Huawei's 4G equipment served rural carriers in the United States, providing universal services to people living in remote rural areas. I saw those stories from the press that you mentioned, but no matter how the outcome turns out, I think it would not have a major impact on Huawei's business. Because, as I mentioned just now, we have virtually no business presence in the US, and we don't have the expectation to build up a major presence there.

Martyn Landi, PA: In respect of the UK, at the end of last year, we had the head of MI6 and the defense minister both sort of made vague suggestions that they weren't sure about Huawei's security. And I saw recently the Prince's Trust said it was going to stop accepting donations from the company. I just wanted to get your perspective on how frustrating that side of it is, in terms of still having to deal with things like this, given everything that we have just spoken about as well.

Eric Xu: The UK government has had concerns about the security of Huawei's equipment. That's the very reason that Huawei has worked together with the UK government in putting in place the CSEC, Cyber Security Evaluation Center, to embark on partnerships to address those concerns. So, this is a model of open collaboration between the UK government and Huawei to address the concerns around Huawei equipment deployed in UK networks.

Just this morning, I saw an article authored by Robert Hannigan, who was the director of GCHQ, published on Financial Times. That article well explained all the questions you raised and I would suggest you look at it. In order to protect cyber security of the UK and well serve the British people, GCHQ has put in place a whole series of systems and mechanisms to ensure solid management and regulation of mobile communication networks. And I also agree with what Robert said on the subtitle, that technical judgments should be made on a clear-eyed view of the potential threat. It should not be simply politicized. I think Robert does a better job in answering your question than I do.

And then the second part of the question the Prince’s Trust stopped accepting Huawei's donation, I think Huawei does not feel frustrated about that. We made the decision to make donations to the Prince’s Trust based on our great respect to the outstanding achievement they have made in helping young people. It had nothing to do with politics. And it is to our regret that they made this decision based on partial and groundless conversations surrounding Huawei, without talking to Huawei in advance at all. If we take a step back, I think there will be no impact on Huawei if the Prince’s Trust accepts or not accepts Huawei's donations. But again as I mentioned just now, we pay our greatest tribute to what the foundation has done in the past in helping young people.

Tamlin Magee, Computer World: I find it interesting that Huawei has a good historic relationship with two of the five-eye countries, in particular, being Canada and UK. So I'm curious if you could expand a little more on the relationship between Huawei and the intelligence agency of the five-eye countries. I'm speculating here, but I assume if they have the capabilities to intercept fiber communications, then they probably have the ability to intercept communications from a box, so I'm just wondering to what extent Huawei has already cooperated with the intelligence agencies of the five-eye countries.

Eric Xu: I'm not very clear about Huawei's cooperation with the intelligence agencies of the countries that you mentioned, but I know Huawei's engagement with the GCHQ in the UK. Huawei's collaboration with the UK is a constructive collaboration. It's not simply yes or no. But rather, it's based on respective priorities as we work to find technical and regulatory solutions so that the partnership can proceed.

Huawei's collaboration with the UK government and also the UK industry has been a role model of China-UK cooperation. Huawei's investment and development in the UK, and its engagement with the UK government have been taken as a case study when people look at governmental and people-to-people engagement between China and the UK.

This is a constructive and friendly model of cooperation that has helped to address and bridge the differences of values and cultures of the east and the west, and has allowed Huawei to constantly invest and develop in the UK, and allowed our telco customers to be able to use Huawei's technologies, products, and solutions in serving the British people. Because we have seen many cases where in light of differences of values and cultures, parties tend to either go to confrontation or either yes or no without middle ground. It has been quite difficult for related parties to find a constructive and friendly model of collaboration that well addresses each other's concerns and priorities.

Huawei has been enjoying very good collaboration with the UK. This is largely because the UK has been a strong advocate of free trade. The UK uses clear rules and rational regulation to address potential concerns that they may have. And I believe that's a cornerstone for the UK to become a nation of openness and freedom.

Steve Cassidy, PC Pro: I think my question is about "convergence". This morning, we see an enterprise division, which is an IP network service platform. In that space, people are becoming very interested in network monitoring and forensics on networks, because it's difficult, and that's where all of the traffic is. In the telco space, in the communication company space, there's more than just that network. There is ATM, and there is other standard available. But the requirements of the government, to be sure, that you are well behaved are the same as the requirements of the enterprise. Yet the tools are very different. Do you see a convergence come where 5G traffic uses enterprise standards to travel and, therefore, can make use of enterprise disclosure. Do you think that helps to solve the problem of just a box running with a light on the front of it and no one knows what traffic it generates, which appears to be where the fear comes from? So is the work in enterprise helping to solve problems in telephony infrastructure, if that's a question?

Eric Xu: If all cyber security challenges are technical issues, I think certainly we can find technical or regulatory solutions to address them. And as we all know, cyber security represents a challenge that everyone in the world faces. Therefore, people have paid special attention to cyber security as they work on the selection of 5G-related technologies, as they work on the definition of 5G-related standards. 5G, from technologies chosen, from a standard point of view, is more secure than previous generations of mobile communication technologies, 2G, 3G, or 4G. I think that’s something people can easily verify when they talk with experts from either 3GPP or GSMA. And information being transmitted through 5G networks has 256-bit encryption built into that. That means people have to use quantum computers, which are not there yet in today's market, to possibly crack those transmitted information.

Steve Cassidy, PC Pro: Well, yeah, but that's what I mean about convergence, because that's over the air. And people's concerns are about the infrastructure. That's very different pieces of the same path.

Eric Xu: If you look at 5G, you have signal coming out from mobile phones and up to base stations and then moving up to IP network. In UK networks, Huawei only provides base stations. And for network layers above the base stations, Huawei doesn't provide any equipment. That's also written in Robert's article. At the time the decision was specifically made not to have a single vendor, like Huawei, to provide the entire network, and the network layer above the access was provided by other vendors. We only provide the base stations.

Yuan Yang: So this is actually a follow-up question on Steve's question. Huawei only provides base stations in the UK. Essentially there is encryption of data transmitted from user devices into base stations, and whether Huawei decrypted that information as you further transmit that information from base stations to other network layers.

Eric Xu: Either it’s encryption or decryption, that’s the business of telecom operators or governments.. The keys of encryption are either in the hands of governments or telecom operators, certainly not in the hands of Huawei.

Yuan Yang: So I notice in the 2018 report from NCSC, they pointed to the areas of improvement of third-party components used in Huawei's products. Some people argued that this is related to Huawei's corporate culture. It seems Huawei is more willing to take in components from different sources as you build your products compared to European companies. In some extreme arguments as in the indictment from the US authorities, Huawei even encouraged employees to get technologies from other companies. So you have a US$2 billion R&D budget, to address this third-party component issue. Whether this third-party component issue is related to Huawei's corporate culture, or if there are any other reasons, how do you plan to address those challenges in the next couple of years?

Eric Xu: First, I would say your understanding is not correct. The third-party software that you are referring to is called VxWorks. It's an operating system that is provided by an American company called WindRiver. We thought using an operating system from a US company would make it easier for the UK government to believe in, and then it turned out it's not the case.

For any product, no matter it is hardware or software, you have to rely on an operating system as you do product development. For example, developers use either Windows or Linux as they develop application software, so we have to use an operating system as we develop base station software. For Huawei base stations that are deployed in the UK, we chose VxWorks from WindRiver. Of course, there are other third-party software and open-source software as well.

What the OB report was essentially saying is that Huawei has to improve in certain areas in the way we manage third-party software. It is not saying that those software cannot be used at all, because if that's the case, that means all of the companies may have to reinvent the wheel, or redevelop the software that is built into their products. That means you have to rebuild Windows, Linux, and database from Oracle, which is not possible.

After this issue was brought up in the report, we talked to WindRiver. And they told us that VxWorks and the very versions that we were using at the time in the UK network are even more extensively used in other industries in the UK, some of which are even more sensitive compared to the telecommunications industry.

Therefore, in our software development, we use operating system and database from third parties. We also use open-source software. That has nothing to do with our corporate culture. That is something which is absolutely natural for all companies as long as they work on the development of products, because, as I mentioned just now, you cannot reinvent all the wheel. And I understand that some people may question why you would need three to five years to improve your software engineering capabilities. What's the purpose of the additional 2 billion US dollars investment? And I think I might need a while to well address this question. I am not sure whether you are willing to spend that time with me.

At the time when we established the CSEC with the UK government, it was primarily to address the concerns of the UK government, whether there are back doors in Huawei's products. Then we delivered our source code to CSEC, which are then checked by British nationals passing DV clearance by the GCHQ. They looked at the source code and found no backdoors in our products.

The fact that we delivered the source code to the UK CSEC and the extensive testing that CSEC has done verified that there is no backdoor in Huawei's equipment. That is something Robert also talked about in his article, saying that NCSC has not found any backdoor in Huawei's equipment.

The concerns some countries have right now around backdoors have long been addressed in the UK.

And I think this whole discussion around the backdoor was long addressed when it comes to the UK from the time that Huawei decided that we'd deliver our source code to the UK for testing.

And then the next step of CSEC is to look at Huawei products to see how strong Huawei products are, to prevent themselves against attacks, penetration, and possible threats. That's the second stage or security that people talk about.

Then we spent eight years to improve Huawei products' defensive capabilities against a possible attack and possible penetration, and to improve the resilience of Huawei equipment. Through the efforts of those past years, Huawei today is the strongest in terms of those dimensions, and that is not something that we ourselves claim. It's based on objective and extensive assessment and testing by Cigital, a US company who specializes in this area. Cigital is a specialized company working on software security engineering maturity assessment. They started evaluating Huawei products on product security since 2013. They do this annual testing and review out of 12 practice areas. Huawei ranks among the top across the industry in nine practice areas. And in the rest three, Huawei performs better than industry average.

But we are also aware that the threat environment of the security keeps changing, and the technologies around attack and penetration keep evolving, and the hackers are becoming stronger. If you only have strong security capability or strong defense against possible attacks and penetration, that's like a coconut, where the shell is very tough. But what if the shell was cracked? It should not be like a real coconut, where you only have water inside. Then the areas of focus for this collaboration with the UK has been expanded, not only to look at the shell of the coconut, but also what's inside, essentially the resilience of the equipment, not just the outcome but also the high quality and the trustworthiness of the product development process, so the scope was expanded from security to resilience, from only outcome to outcome plus process.

And remember, CSEC has access to Huawei's source code, so they can easily tell whether those source codes are written in a way that's readable, easy to modify, and whether the code base is robust. We are like "naked" in front of CSEC.

And then CSEC is saying, all right, your code base is not beautiful. You know, this is a code base that has been there for 30 years. And this is the characteristic of the communications industry. It's like Windows software as well. The legacy code base keeps building up, and they are saying Huawei needs to improve our code readability and modifiability as well as the process of producing code, so that we deliver high quality and trustworthiness on both the outcome and the process.

And then that's how the focus and the scope have been expanded to include the process of software production, or, in other words, software engineering capabilities and practices. And then the idea was to take a solid and robust standard that is future-proof in measuring and in asking for improvement of our legacy code base that has been there for 30 years. Certainly, security risks, software techniques are different, and people's coding skills are different. There are naturally gaps versus the requirements for the future, so that means all of the legacy code has to be refactored, or, in plain English, rewritten. As you can imagine, the investment is massive, and this also has impact on the project schedule in terms of functionalities and features we deliver to our customers today in the market.

On this specific topic, there has been a long strong debate between Huawei and NCSC in the sense that we wanted to focus on the incremental, the new code, instead of refactoring all of the legacy code. Almost all of the Huawei executives had been involved in this debate with NCSC, and over the course, we ourselves have been getting a deeper understanding of what it means by legacy code refactoring, by building high quality and trustworthiness into the development process as well. We realized that this is definitely not just about addressing the concerns of the UK; it carries a lot of weight and to a certain degree is the foundation to Huawei's future development.

Because, as we know, "cloud, intelligence, and software defines everything" is becoming more and more prevalent, the future world will see software as a very key part of that. In order to get the trust from our customers or government authorities, we have to not only ensure high quality and trustworthiness of the outcome but also of the process when producing those software. We think of this as a foundation or cornerstone in order for Huawei to realize our long-term aspiration. I personally went to talk to NCSC twice and I realized we could not continue to confront each other. It’s not about addressing requirements coming from NCSC; this is something that Huawei must be doing for our long-term development. Then I managed to persuade other executives on the leadership team, and we came to a Board resolution to embark on a comprehensive software engineering transformation program.

Yuan Yang: When did that happen?

Eric Xu: This was by the end of last year. Actually, the debate in our board room for that decision was quite fierce, and in the end, we had the board decision to fundamentally enhance our software engineering capabilities and practices, with the objective of building high quality and trustworthy products. This transformation will take three to five years to complete. Essentially, we will take the future standards, future requirements to rebuild our process of software production, and we are going to follow those future standards as we work to refactor our legacy code.

From that point of view, while you have to at the same time work to satisfy customer requirements that are imminent while working on code refactoring, you definitely need to have additional R&D budget.

That's where the $2 billion comes in. Essentially, that would be used primarily for legacy code refactoring, training or reskilling of our R&D engineers, et cetera.

Unfortunately, I am the responsible person for this transformation program; that means I will have a lot more work to do in the next five years. And I have spent a great deal of time recently working on this program.

And the $2 billion is just an initial starting fund. Definitely it would not be enough. I hope through our efforts in the next three to five years, we can truly turn out products that would be trusted by governments and by customers, so as to support and sustain Huawei's long-term development.

For this reason, our founder and CEO, Mr. Ren, sent out an all staff letter as the very first corporate document issued in 2019. It's about comprehensively enhancing software engineering capabilities and practices to build quality and trustworthy products. And I can give you a simple analogy to explain what is high quality for the process.

I guess you may like Chinese food. But you may not have visited and checked the kitchen. I guess you would not know what kind of moves, what kind of activities that a chef follows in order to produce the Chinese food that are set on the table. Now it's about going into the kitchen and setting out a whole set of procedures, processes, standards, and behavior guidelines so that the chef can follow in order to produce the tasty food. If the chef does not follow specific steps or activities in the process, maybe the food in the end would not be as tasty, and then you have to identify which specific moves that the chef did not follow, correct it and then the food would be tasty again. So that's essentially what our software engineering transformation program is about.

It's about delivering high quality and trustworthy software code in the end, and also high quality and trustworthiness of the software production process.

It's a very challenging journey, I would say, but this is something that we have to deliver. I think that this is my answer to your question, why does it take three to five years, why $2 billion, which I believe certainly would not be enough. Frankly, I don't know how much money that would be needed in order to support this transformation program. But we certainly enjoy one advantage, in the sense we are not a public company, so it would be totally fine that we make less money today. As long as there is a future, it’ll be our greatest victory. And many of our employees hold company shares. I think that they would understand this choice. They would prefer lower profitability today for the longer term future instead of more dividends today without a long future for the company.

Oscar Williams, New Statesman Tech: Are you able to estimate at all how much it might cost to entirely rewrite your code base? I know you said that 2 billion was an initial estimate, but are you able to put a number on how much it could cost in the long term?

Eric Xu: We’re in the process of doing that. You know, we are working on the high-level plan for the whole transformation program. After we have that number, I'll let you know. And our timeline is to hopefully complete the high-level plan by the end of March.

One additional thing I want to say is that these issues, these challenges are not unique to Huawei. I think these are challenges that all companies in our industry have to work on. The only difference is the extent of improvement that would be needed,, but I do believe no company is perfect here, and on top of that the whole landscape I think is dynamically changing as well. Any company who voluntarily delivers their source code to UK for review by British nationals with DV clearance would certainly expose quite a number of issues.

Robin Pagnamenta, The Daily Telegraph: Sorry to return to the issue of cost, but the ultimate cost could be a multiple of $2 billion? And I'm sorry if I missed a key segment there, but could you just summarize the role that CSEC will play in vetting and monitoring the new code and the timeline?

Eric Xu: All of the refactored code, as long as they go into Huawei equipment that is deployed in UK networks, would be reviewed and tested by CSEC. Therefore whether the outcome in the end would be good or not, I believe NCSC would certainly know that. And, of course, from NCSC's point of view, they would say, all right, these are all the expectations and hopes for the future. I hear you, but I need to really see with my own eyes what you deliver in the end. But when we put in place CSEC in the first place, the very objective is through this model of open collaboration, to identify issues and areas of improvement so that we can take actions on. It's certainly not just aboutfinding backdoors which do not exist as being tested and verified.. We invested 6 million euro in CSEC in 2018, and of course we want them to identify any areas that we can take actions to improve. That's the very purpose. From my personal point of view, this model can also push our internal R&D teams to improve, as it is a way of verifying how well our R&D teams are doing.

Tamlin Magee, Computer World: I'm just wondering your opinion on the internet, considering its history in sort of military intelligence, as a tool for American military intelligence. Do you think this is just a case of the mask slipping and technology being more overtly political than ever before, more obviously political than it had been previously, and if you think so, how will this be a problem and how will you address it?

Eric Xu: Technology has always been linked in one way or another with politics. What is politics? People can politicize one thing if they want to, and they can not politicize one thing if they don't want to. Then how to address it in the end? I believe that humanity has gone through such a long history, such a long journey, and I believe there are a lot of people who have the right wisdom. For sure, technology advancements bring benefits to humankind. Especially, take 5G for example. 5G can certainly bring benefits to the general public in the sense that they can enjoy much better digital experience. It's certainly not an atom bomb, because 5G, in whichever case, would not hurt people.

And then for privacy protection, there is already GDPR from European Union. The UK is still part of that right now. Even after Brexit, I believe UK will come up with your own standards for privacy. As long as players follow those standards, the privacy will be adequately protected for people in the UK and across Europe. Any company who violates the stipulations in GDPR would be subject to severe punishment. So we highly appreciate standards and regulations such as GDPR. It is open, transparent, and nondiscriminatory. It applies to all the players. Everyone has to follow, and those who violate would get punished. I think from technical point of view similar standards can be set up for cyber security. With standards that are open, transparent, and nondiscriminatory, there will be clear guidelines for all of the players. Those who follow keep doing business, and those who violateget punished. It is as simple as that. If it's related to politics or ideology, that is totally based on suspicion or assumption. What if I say you will kill someone in the future? I think no one can rule out that possibility 100%. So that to a certain degree would describe what Huawei is facing today.

Yuan Yang: You mentioned that Asia represents a very important market for Huawei from 5G point of view, and the maturity of European market is not that high when it comes to 5G adoption. Then can you give us some hint in terms of which specific countries in Asia that will really adopt 5G in a very big way? And how much market share that will contribute to Huawei's 5G business contribute and in what timeline?

Eric Xu: I think I talked about this in the past. To me there are three types of markets when it comes to 5G adoption: one, markets with strong demand for 5G. Those countries include China, Japan, Korea, and some GCC countries.

The second category is developed countries in Europe, and the US as well. These countries do not currently have a strong demand for 5G, and they are not that developed yet, even on 4G rollout. Do you know the number of base stations in France and how that compares to the number of base stations in the city of Shenzhen? The total number of 4G base stations in France is smaller than the number of base stations deployed by China Mobile Shenzhen—just one operator.

The third category is largely the developing markets, where we do not see real 5G demand at this point of time. Therefore, Huawei's revenue from 5G in the next few years would primarily come from countries in the first category, and from very few countries in the second category.