**Huawei Rotating Chairman Eric Xu on Hot Topics: Companywide Program for Enhancing Software Engineering Capabilities, R&D Operations, Cyber Security, and US Issues**

–Eric Xu's Interview with UK Media Outlets on February 13, 2019

During an interview with 6 UK media outlets on February 13, 2019, Huawei Rotating Chairman Eric Xu gave straight replies to questions about recent hot topics. Key points are as follows:

* **Enhancing software engineering capabilities: "**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… It's not just about addressing the requirements coming from NCSC; this is something that Huawei must be doing for our long-term development… We think of this as the cornerstone that enables Huawei to realize our long-term aspiration."
* **5G:** "5G can bring benefits to the general public, enabling them to enjoy much better digital experience. It's certainly not an atomic bomb, because 5G will not hurt people."
* **US$2 billion fund:** "This US$2 billion budget is just an initial fund… I hope through our efforts in the next three to five years, we can truly build products that would be trusted by governments and by customers, so as to support and sustain Huawei's long-term development."
* **Cyber security:** "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."
* **Future:** "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 profits today without a long-term future for the company."
* **Huawei in the UK:** "Huawei's collaboration with the UK government and also the UK industry has been a role model of China-UK cooperation."

**1. PC Pro: My question is 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 investment management system that is similar to that of other industry players but is also somewhat different. Our R&D process and management system is called IPD, Integrated Product Development. This process was established in 1998 with the help of IBM, who provided consulting services to Huawei. In this process and management system, there are both investments for the future, essentially research and innovation, and also investments for 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 our customers. So, there are three parts of R&D related investments, and we have a separate budget for each piece when we look at our annual business plan. We have dedicated governance teams to make 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. IPMT makes decisions on research into future-oriented innovative technologies. Those bodies would make decisions on what to develop, what not to develop, and when to deliver.

**2. PC Pro: How long is that review cycle?**

**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.

For research, innovation or patents producing investments, our decision-making body is called ITMT, Integrated Technology Management Team. In history, the average percentage of research and innovation related investment was 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 decision-making mechanisms 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 that made the decision in 2009 to initiate our research efforts on 5G. We announced the 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 and IPMT.

**3. 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 2009 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? Our research teams 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.**

**4. 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 is 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.

**5. 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.

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 in Shenzhen. So I think this is quite normal. The market size of Australia is even smaller than China Mobile Guangzhou. The market size of New Zealand is even smaller than Yiyang, a small city in China which is my hometown. 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 in Shenzhen, our equipment is not used. 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.

**6. New Statesman: 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.

**7. 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 HCSEC, 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 is 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.

**8. Computer World: I find it interesting that Huawei has a good historic relationship with two of the Five Eyes 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 Eyes 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. This model 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 openness and 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.

**9. 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 and 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.

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.

**10. PC Pro: But that's what I mean about convergence, because that's over the air. And people's concerns are about the infrastructure.**

**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 the network. In UK networks, Huawei only provides base stations. And for network layers above the base stations, Huawei doesn't provide any equipment. As Robert said in his article, Huawei does not enter the "core" part of the network.

The network layers above the base stations are provided by other vendors, and have nothing to do with Huawei.

**11. Financial Times: Huawei only provides base stations in the UK. Essentially there is encryption of data transmitted from user devices into base stations. Is that information decrypted as it is transmitted from base stations to other network layers?**

**Eric Xu:** As for encryption or decryption, that's the business of telecom operators or governments.

**Financial Times: Is the encryption done through your equipment?**

**Eric Xu:** The keys of encryption are in the hands of governments or telecom operators, certainly not in the hands of Huawei.

**12. Financial Times: 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. Is this third-party component issue related to Huawei's corporate culture, or are there 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 Wind River. 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 Wind River. 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 databases from Oracle, which is not possible.

After this issue was brought up in the report, we talked to Wind River. And they told us that VxWorks and the very versions that we were using at the time in the UK networks are extensively used in other industries in the UK, some of which are even more sensitive compared with the telecommunications industry. Therefore, in our software development process, we use operating systems and databases 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 it is simply impossible for one company to do everything on its own.

Some people may question why Huawei would need three to five years to improve our software engineering capabilities. What's the purpose of the additional 2 billion US dollar investment?

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 HCSEC with the UK government, it was primarily to address the concerns of the UK government that there might be backdoors in Huawei's products. Then we delivered our source code to HCSEC, which were then checked by British nationals with DV clearance. They looked at the source code and found no backdoors in our products.

The fact that we delivered the source code to the UK HCSEC and the extensive testing that HCSEC has done verified that there is no backdoor in Huawei's equipment. That is something Robert also talked about in his article, saying that GCHQ 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 in the UK when Huawei decided to deliver our source code to the UK for testing.

And then the next step of HCSEC was to look at Huawei products to see how strong Huawei products are to prevent themselves against attacks, penetration, and other possible threats.

Then we spent eight years to improve Huawei products' defensive capabilities against possible attacks and possible penetration. 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 that is specialized in this area.

Cigital is a specialized company working on software security engineering maturity assessment. They started evaluating Huawei products on product security in 2013. They do this annual testing and review in 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 security threat environment keeps changing, and the technologies around attack and penetration keep evolving, and the hackers are becoming stronger. If you only have strong security capabilities 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 our collaboration with the UK was expanded to look at not only the shell of the coconut, but also what's inside, which is essentially the resilience of the equipment, not just the outcome but also the high quality and the trustworthiness of the product development process. The scope was expanded from security to resilience, from only outcome to outcome plus process.

And remember, HCSEC 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 being "naked" in front of HCSEC.

Now HCSEC is saying that our code base is not beautiful. You know, this is a code base that has been built up by Huawei over the past 30 years in the communications industry. It's like Windows software as well. 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 has been shifted to the process of software production or what we call software engineering capabilities and practices. The idea is to take a solid and robust standard that is future-proof to measure and ask for improvement of our legacy code base that has been there for 30 years.

The security risks we faced and the software techniques we used in the past were different from today, and people's coding skills have also improved compared with the past. There are naturally gaps versus the requirements for the future. If we want to refactor and even rewrite the legacy code built up over the past 30 years, the investment that will be required 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. We only wanted to focus on the new code, instead of refactoring all of the legacy code. Almost all 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 and by building high quality and trustworthiness into the development process. 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" are becoming more and more prevalent, the future world will see software as a very key part of that. We must ensure that our software is trusted by our customers or government authorities. To do that, we have to ensure high quality and trustworthiness of not only the outcome but also of the process when producing those software. We think of this as the cornerstone that enables 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 just about addressing the requirements coming from NCSC; this is something that Huawei must be doing for our long-term development. After returning from the UK, 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.

**13. Financial Times: 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 trustworthy products. This transformation will take three to five years to complete. Essentially, we will take the future standards and 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.

We have to work to satisfy the requirements our customers have now while working on code refactoring, so we definitely need to have an additional budget. That's where the US$2 billion comes in. Essentially, that would be used primarily for legacy code refactoring, training or upskilling of our R&D engineers, and so on. Unfortunately, I am the person responsible 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 this US$2 billion budget is just an initial fund. Definitely it would not be enough. I hope through our efforts in the next three to five years, we can truly build 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 open letter to all employees 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.

I can give you a simple analogy to explain what is high quality for the process. Many people like Chinese food, but few may have visited and checked the kitchen or know what kind of moves and 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 code of conduct 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 transformation program for enhancing our software engineering capabilities 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 questions as to why the program will take three to five years and why the US$2 billion is only the initial fund.

Frankly, I don't know how much money that will be needed in order to support this transformation program.

But we certainly enjoy one advantage. 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 profits today without a long-term future for the company.

**14. New Statesman Tech: Are you able to estimate at all how much it might cost to entirely rewrite your code base?**

**Eric Xu:** We're in the process of doing that. 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 more thing I want to say is that these issues mentioned just now 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 the UK for review by British nationals with DV clearance would certainly expose quite a number of issues.

**15. The Daily Telegraph: Sorry to return to the issue of cost, but could you just summarize the role that HCSEC 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 the UK networks, they would be reviewed by HCSEC. 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.

When we put in place HCSEC, the very objective was to identify issues and areas for improvement so that we can make progress. It's certainly not just about finding backdoors which do not exist. We invested 6 million euros in HCSEC 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.

**16. 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 cannot politicize one thing if they don't want to. How can we address this?

Humanity has gone through a long journey, and there are a lot of people in every country who have the right wisdom. For sure, technology advancements bring benefits to humankind. This is particularly true for 5G. 5G can bring benefits to the general public, enabling them to enjoy much better digital experience. It's certainly not an atomic bomb, because 5G will not hurt people.

And then for privacy protection, there is already GDPR from the European Union. The UK is still part of that right now. Even after Brexit, I believe UK will come up with its own standards for privacy. As long as players follow those standards, privacy will be adequately protected for people in the UK and across Europe.

Any company that 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 it, and those who violate it would get punished.

I think from a 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 players. Everyone needs to follow the standards, and those who violate them will get 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.**

**17. Financial Times: 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?**

**Eric Xu:** To me there are three types of markets when it comes to 5G adoption.

The first type is markets with strong demand for 5G. Those countries include China, Japan, South Korea, and some GCC countries.

The second type 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 only.

The third type is largely the developing markets, where we do not see real demand for 5G at this point of time.

Huawei's revenue from 5G in the next few years will primarily come from the first type of markets, and a small proportion of our revenue will come from the second type of markets.