

Global standards the key to 5G

Story by



Sophie Batas

Director for Cybersecurity and Data Privacy, Huawei

Biography

The CEPS debate, sponsored by Huawei and the Italian I-COM Deep-In Research Network, focused on a key message: that security is used as an instrument of protectionism to safeguard key technologies and infrastructures.

This point was particularly emphasized by Jan-Peter Kleinhans, Director of the German think tank on technology and society, *Stiftung Neue Verantwortung*, when he posed the questions: “How can we deploy a highly resilient and trustworthy infrastructure our future can rely on? What are the rules of the game for an operator or vendor to deploy infrastructure in Europe?”

As Jan-Peter himself explained, Europe is in the early stages of building up those rules. It has only just started to think more thoroughly about mobile network infrastructure and the resilience it should request from vendors. And this is the point here: in the end, the debate is not so much about cyber security, but technological leadership. The risks are there, no matter who the vendor is. We collectively need to look at the supply chain.

“What’s Europe’s role in this?” he added. “Where’s our constructive role in an ICT and software-defined (environment), where you need to be able to build innovative technology and not just create rules out of thin air.”

European approach to cyber security

Huawei has already answered this question: we fully support a European approach to security, based on global security standards and reliable and trusted certification schemes. In this process, we have demonstrated our transparency and cooperation with various local initiatives aimed at building trust. We are also contributing to standardisation organisations like 3GPP, GSMA, etc.

Paul Triolo, head of the geotechnology practice at EuroAsia Group, was another speaker to stress the global nature of cyber security and data privacy. “I don’t think this is a zero-sum game, where one side wins and the other loses. For example, Artificial Intelligence is an enabling technology and part of a broader system.”

Paul pointed out that there is actually a tremendous amount of research collaboration in the ICT sector between China, the US and Europe, a fact that is often ignored.

Huawei is just one of many companies which brings its own Intellectual Property and standards to the international standardization process, which settles on a general global standard that everybody can build to. As he says, that’s not something China or any other country can dominate. Similarly, in Europe, which is taking the lead on AI ethics, it would be unfair to exclude Chinese companies from the global debate on setting AI guidelines.

As all the participants at the CEPs event seemed to agree, there is no such thing as a zero-risk environment. Whatever the risk is, or wherever the threat is coming from, we need to move the discussion towards about how to mitigate those risks.

5G is now. So, we need global security requirements quickly, we need to implement security and privacy by design, and we need a Trusted Cyber Security Architecture. That’s the discussion we should be having at this moment in time.