Building trust in the Intelligent World

Story by

Mark Smitham

Senior Manager of EU Public Affairs, Huawei
Biography

As the world becomes more connected we must grow together to bring digital to all and leave no one behind.

Digital technology is now part of our economies, societies and daily lives in an increasingly Intelligent World. Digital technologies and infrastructures, like 5G and AI, present new opportunities for economic growth and new threats to the security of digital communications. Huawei's new processor is optimized for computing power of Artificial Intelligence algorithms. Cyber security challenges are particularly different for AI. Development of artificial intelligence services takes place across three phases: learning, training, and application.

Data integrity, privacy, and confidentiality

During the learning phase a corpus, or library of data is prepared specifically for the appropriate rules to achieve the goal of the algorithm. Data integrity is especially important during this phase. We want to ensure the data is not tampered with. Attackers can inject adversarial data to affect the inference capability of AI models or add a small perturbation to input samples to change the inference result. In training an AI model, the algorithm will run over the corpus of data from the learning phase. The model needs to be robust. Training samples typically do not cover all possible outlier cases and exceptions, resulting in a weak algorithm. Therefore, the model may fail to provide correct inference on adversarial examples. For scenarios in which users provide training data, attackers can repeatedly query a trained model to obtain users' private information. Cyber security challenges in the last phase for business application of an AI service focus on confidentiality. Service providers generally want to provide only query services without exposing the training models. However, an attacker may create a clone model through a number of queries. The code of applications, models, platforms, and chips may have vulnerabilities that attackers can exploit. Further, attackers may implant vulnerabilities in models to launch advanced attacks. Due to the unexplainable nature of AI models, security vulnerabilities are difficult to discover. A typical cyber-attack on AI could therefore attempt to evade the algorithm and somehow cheat the AI service in some way. The attacker may attempt to poison the algorithm to achieve different results from the AI service. Cyber-attackers could try to steal an AI model. Or a cyber attacker may aim to inject a vulnerability into the AI service to exploit later or somehow weaken the AI service.

Trustworthy networks and AI services

Huawei offers secure products to help our customers build cyber resilience and provide trustworthy networks and AI services. Our 11 technical assistance centres worldwide with more than 4,500 Huawei engineers and over 700 service staff provide non-stop support to ensure our equipment never causes large-scale network breakdown. In 2018, we ensured smooth communications for more than 3 billion people, and supported the stable operations of over 1,500 networks in more than than 170 countries and regions. We guaranteed network availability during more than 300 natural disasters and major events such as the magnitude 7.7 Sulawesi earthquake in Indonesia, the FIFA World Cup in Russia, the Jakarta Palembang Asian Games, and the Shanghai Cooperation Organization summit.

Unblemished cybersecurity record

Huawei has an unblemished cybersecurity record. In over 30 years of operations, Huawei has probably been the most scrutinised of all companies. Huawei will always prioritize security and privacy over: costs, schedules and functions. Over the next five years we will invest a further US$2bn to ensure our security engineering practices continue to be industry-leading. We follow industry best practice with a Cyber Security Framework to identify threats, protect against attacks, detect intrusion and other events, respond to those attacks and seamlessly recover from them. Identify. Protect. Detect. Respond. Recover. IPDRR. This cyber security framework is an industry best practice that can equally be applied to the cyber security challenges of artificial intelligence. Development of these methodologies is not done in isolation. Public and private collaboration is essential for strong cyber security in all digital technologies. Cyber security should be based on facts available through transparent cooperation. Facts should be objectively verifiable. Thorough verification should be based on global, internationally-recognized standards and industry best practices.

Public and private sector collaboration essential

Cyber security and privacy protection challenges are complex and public-private sector collaboration is essential. We have been working with the UK government since 2010 through the Cyber Security Evaluation Centre in the UK and have now established a total of six security centres worldwide for the evaluation and independent verification of the security of Huawei's products. Our security management system has passed BS7799-2/ISO 27001 certification, and Huawei's products have passed more than 200 security certifications, including CC, FIPS, PCI DSS, CSA STAR, and O-TTPS. By relying on objective third-party standards to test the security of technology made by any vendor, we can ensure that decisions about security are based on facts, rather than emotions or political rhetoric. That’s why Huawei joined the Paris Call for Trust and Security in Cyberspace. In becoming a Paris Call member, Huawei joins 564 other entities who have made a public commitment to strengthening the security of digital products and digital systems.

Making digital products more secure

Launched by the French government in November 2018, the Paris Call is a declaration of commitment to work collaboratively on one of the world’s most challenging issues. Working together to make digital products more secure.

Strengthening collective defences against cybercrime. Promoting cooperation among stakeholders across national borders. We also pledge adherence to international norms of responsible behaviour in cyber space. Huawei invests significantly in research aimed at making our products and solutions as secure as possible, and is committed to ensuring security for all customers and users. We support global collaborative action on improving defences against cybercrime, including openness, transparency and internationally agreed standards. Huawei will continue building trust-based relationships with partners, in order to enable the Intelligent World and create opportunities for all.

Digital for All

That’s why we are pleased to see that building trust in digital technologies together is a priority for the G7 summit this year. Cyber security is not just our business, it’s everyone’s business. Decisions at the G7 summit will contribute towards strategy in public and private sectors to balance innovation and regulation. Everyone needs to trust that new, digital technologies continue to guarantee respect for their fundamental rights. We need an inclusive approach for a healthy and competitive market that can deliver sustainable economic growth and bring real benefits to people and society at large. Together, we can pass the benefits of digital technology to everyone.

Press contacts

Jakub Hera-Adamowicz +32 499 641 839 Yingying Li +32 470 779 011