



Kiberbiztonság és adatvédelem Vízióink és gyakorlataink az EU-ban

Infoparlament, Budapest 2019.
Sophie Batas, kibervédelmi igazgató

LEADING NEW ICT

Huawei számokban



180 000
alkalmazott

80 000
K+F mérnök



170+
Ország



14
K+F
központ/labor



No. 72
Fortune Global 500



108 Mrd USD
Forgalom 2018

Piacvezetés



Erős K+F befejtetés – éves forgalom 13%-a

40+

5G kereskedelmi szerződés

100,000+

5G leszállított bázisállomás

5G start

US\$600mn

2009

Research & standards



GSMA Outstanding Contribution for LTE Evolution to 5G

US\$600mn

2016

Product development



Award for Most Notable Partnership between an Operator and Solutions Provider for 5G Trials and Development

US\$800mn

2018

Growing investment



GSMA Outstanding Mobile Technology Award - 5G

Simplified deployment

Lowest energy consumption, lightest equipment, minimum reconstruction required

Simplified sites

"1+1" simplified antenna solution: The unit bit cost is better.

Superior experience

Ubiquitous xGbps experience



Függetlenség



Huawei Technologies magánvállalat, alkalmazottainak kezében van.

Nincsenek külső részvényesek és tulajdonosok, a a Huawei független a kkormánytól .Üzleti döntésekre nincs befolyással a kkormány vagy párt. Egyedül a Huawei vezetői csapata gyakorolja a menedzsment jogokat a vállalatban.

Kizárólag az ügyfelekre koncentrálunk. A Huawei nem okoz kárt egyetlen országnak sem. A Huawei soha nem fogadott el semmilyen felkérést a Huawei termékeinek rosszindulatú felhasználására.

A kínai kormány nem avatkozhat bele a Huawei kiberbiztonsági- és adatvédelmébe. A kínai jogszabályok nem tartalmazznak ilyen kötelezettségeket, hogy telepítsenek hátsó ajtókat, vagy más országokból szerezzenek információkat.

Kiberbiztonsági szabályozás Kínában



Article 18 – A távközlési szolgáltatók és az internetszolgáltatók technikai interfészeket, dekódolást és egyéb technikai támogatást és segítséget nyújtanak a közbiztonsági szerveknek és az állami biztonsági szerveknek a terrorista tevékenységek megelőzésére és kivizsgálására a törvénynek megfelelően...

Article 28 – A hálózatüzemeltetők technikai támogatást és segítséget nyújtanak a közbiztonsági szerveknek és az állambiztonsági szerveknek a nemzeti biztonság és a bűncselekmények nyomozásának segítségével a törvénynek megfelelően.

Article 13- Amint az a kémkedés elleni küzdelemhez szükséges, az állami biztonsági szervek az alkalmazandó rendelkezéseknek megfelelően ellenőrizhetik az érintett szervezetek és magánszemélyek elektronikus kommunikációs eszközeit, berendezéseit ...

LEADING NEW ICT



A nemzetbiztonság érdekében a polgárok és szervezetek... haladéktalanul jelentést tesznek a nemzetbiztonságot veszélyeztető tevékenységekre utaló nyomokról; a nemzetbiztonsági munkához segítséget nyújtanak; az állami biztonsági szerveknek, a közbiztonsági szerveknek és az érintett katonai szerveknek szükséges támogatást és segítséget nyújtanak...

Article 28 – A hálózatüzemeltetők technikai támogatást és segítséget nyújtanak a közbiztonsági szerveknek és az állambiztonsági szerveknek a nemzetbiztonság és a bűncselekmények nyomozásában a törvénynek megfelelően.

- Article 7** – Bármely szervezet vagy állampolgár a törvénynek megfelelően támogatja, segíti és együttműködik a nemzeti hírszerző munkával, és bizalmasan kezeli a nemzeti hírszerzési munkák titkait, amelyek a tudásukra jutottak.
- 14. cikk - Az Országos Hírszerzői Hivatal a törvény szerinti hírszerző munkák elvégzéséhez előírhatja az érintett szervek, szervezetek és polgárok számára a szükséges támogatást, segítséget és együttműködést.

A törvénykezés a fejlett országokéhoz hasonló.

Kiberbiztonsági szabályozás Kínában



Zhong Lun jogi értelmezés
Clifford Chance jogi értelmezés

Ernst & Young riport

- A kiberbiztonsági törvények csak a hálózatok üzemeltetőire vonatkozóan írják elő a nemzetbiztonsági munka segítségét. A Huawei eszközbeszállító.
- A törvények Kínán belülre vonatkoznak.
- A kínai kormány is megerősítette a jogértelmezéseket és a cégektől azt várja el, hogy minden országban az ottani törvények betartásával működjenek.

A kiberbiztonság kezelése a Huawei szerint: tényalapú, bizonyítható, egységes

Tények

Az elmúlt 30 évben megbízható
lekövethetőség



170+
ország



3+ milliárd
ember



1,500 távközlési
hálózat

Verifikációk

Kiberbiztonsági laborok nyitása,
hozzáférhetőség a technikai ellenőrzési és
értékelési platform



Banbury, UK
November 2010



Bonn, Németország
November 2018



Brüsszel, Belgium
March 2019

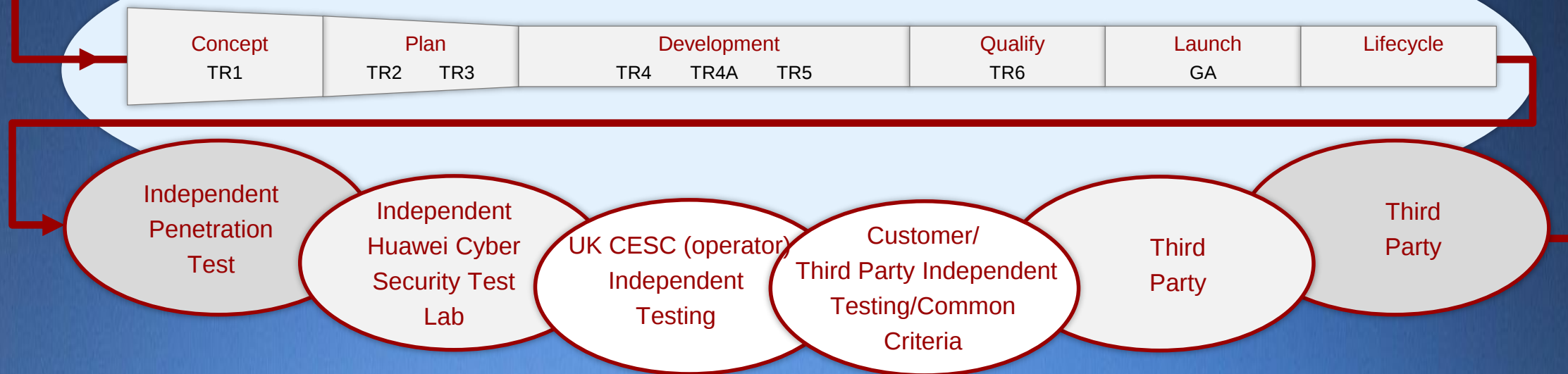
- Kiberbiztonság és adatvédelem: nincs helye feltételezésnek és ideológiáknak.
- A tényeket és a bizonyítékokat ellenőrizni kell, az ellenőrzésnek nemzetközi, globálisan elfogadott szabványokon kell alapulnia és a legjobb ágazati gyakorlatokon
- Az együttműködés világszinten kulcskérdés, átlátható és egységes mechanizmusok szerint kell működnie.

A verifikáció a folyamataink része

A „sok szem és sok kéz” elvet valljuk, mert ez biztosítja, hogy folyamatosan fejlődjön a tudásunk a technológiában, az emberekben és a folyamatokban, ami egy win-win helyzetet teremt végül – ennek részesei kell, hogy legyenek az ügyfelek, a kormányok és a vállalatok.

Amit megtanulunk, megtapasztaltunk, az frissíti az összes Huawei folyamatot, szabványt és irányelvet, és minden termékre és szolgáltatásra vonatkozik.

IPD: integrált termékfejlesztési folyamat



Tanúsítványok – Huawei hozzájárulások



Termékbiztonság



Common Criteria
ICT, 39 items



FIPS 140-2
Encryption
Modules, 20



PCI
Payment Card
Industry, 14



CSA
Cloud Security, 3



ePrivacy
GDPR based, 1



ISO27001
Information
Security
Management



ISO28000
Supply Chain
Security
Management



ISO9001
Quality
Management
System



ISCCC
Qualification of
Information Security

Biztonság Menedzsment

Biztonsági szabványok



- 17 elnök vagy alelnök
- 3GPP SA3 2018-ban: No.1 közreműködő, 251 elfogadott javaslat, 5G biztonsági architektúra elfogadott javaslat

Együttműködés: partnerség a globális kiberbiztonsági ökoszisztémával



A kormányoknak és az iparágnak együtt kell működniük egységes biztonsági szabványok kidolgozásában annak érdekében, hogy minden hálózati eszköz és szolgáltatás azonos szintű biztonságot érjen el.

Az ágazati ökoszisztéma-együttműködése a kiberbiztonság területén



Top hozzájárulás az NFV Security Group-ban



Fő hozzájáruló a SA3-ban, vezető szerep az 5G biztonsági szabványosításban



Igazgatótanácsi tag



Igazgatótanácsi tag



Executive vállalati tag



4 munkacsoport kidolgozását javasoltuk; elnököljük a DOTS és a I2NSF munkacsoportokat

A jövő: EU 5G biztonsági tanúsítványok



A „Cybersecurity Act” 2019. április – honosításai

Ez létrehozza az első EU-szintű kiberbiztonsági tanúsítási keretet, amely biztosítja a közös kiberbiztonsági tanúsítási megközelítést az európai belső piacon, és végül a digitális termékek és szolgáltatások széles körében javítja a kiberbiztonságot.



Közös kidolgozása a NESAS-nak a 3GPP-n és a GSMA-n belül.

A NESAS egy olyan önkéntes rendszer, amely a mobilipar számára olyan alap- és átfogó biztonsági auditot nyújt, amely igazolja, hogy a hálózati berendezések megfelelnek a biztonsági követelményeknek, és hogy a hálózati berendezések gyártói termékfejlesztési és életciklus-folyamataik során megfelelnek a biztonsági előírásoknak is.

A GSMA-nak van egy akkreditációs testülete, amely a tervek felügyeletéért és fejlesztéséért, valamint az akkreditáció meghatározásáért felelős.



Köszönöm szépen!

LEADING NEW ICT