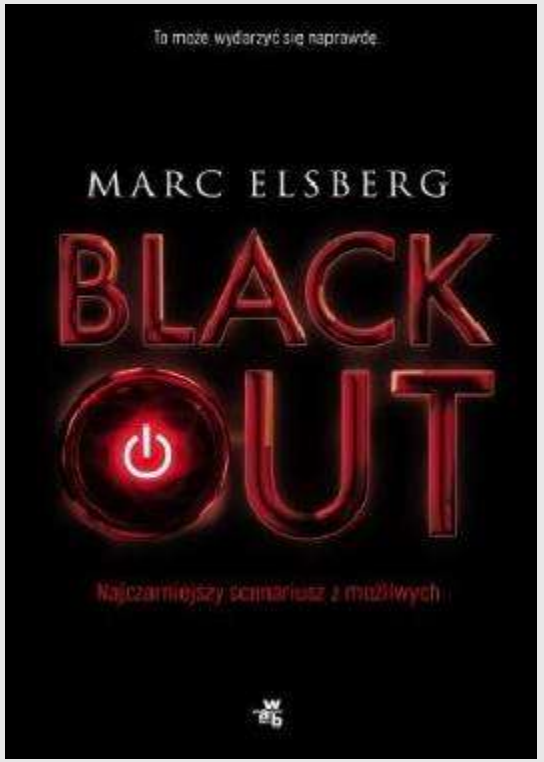
Bezpieczeństwo infrastruktury systemów teleinformatycznych

Tomasz Piasecki
Senior Energy Expert for Global Markets (HQ)
email: tomasz.piasecki@huawei.com

IV Konferencja Naukowo-Techniczna PTPiREE
Pomiary i diagnostyka w sieciach elektroenergetycznych
28-29 maja 2019, Kołobrzeg

HUAWEI

Jak powiedzieć o bezpieczeństwie w 15 minut...?



HUAWEI

Huawei jako globalny dostawca systemów IT/ICT

- sytuacja wizerunkowa Huawei na świecie i w Polsce
- konsekwencje napięć USA – Chiny
- …

…jak (od)budować zaufanie klientów?

Otwartość i transparentność

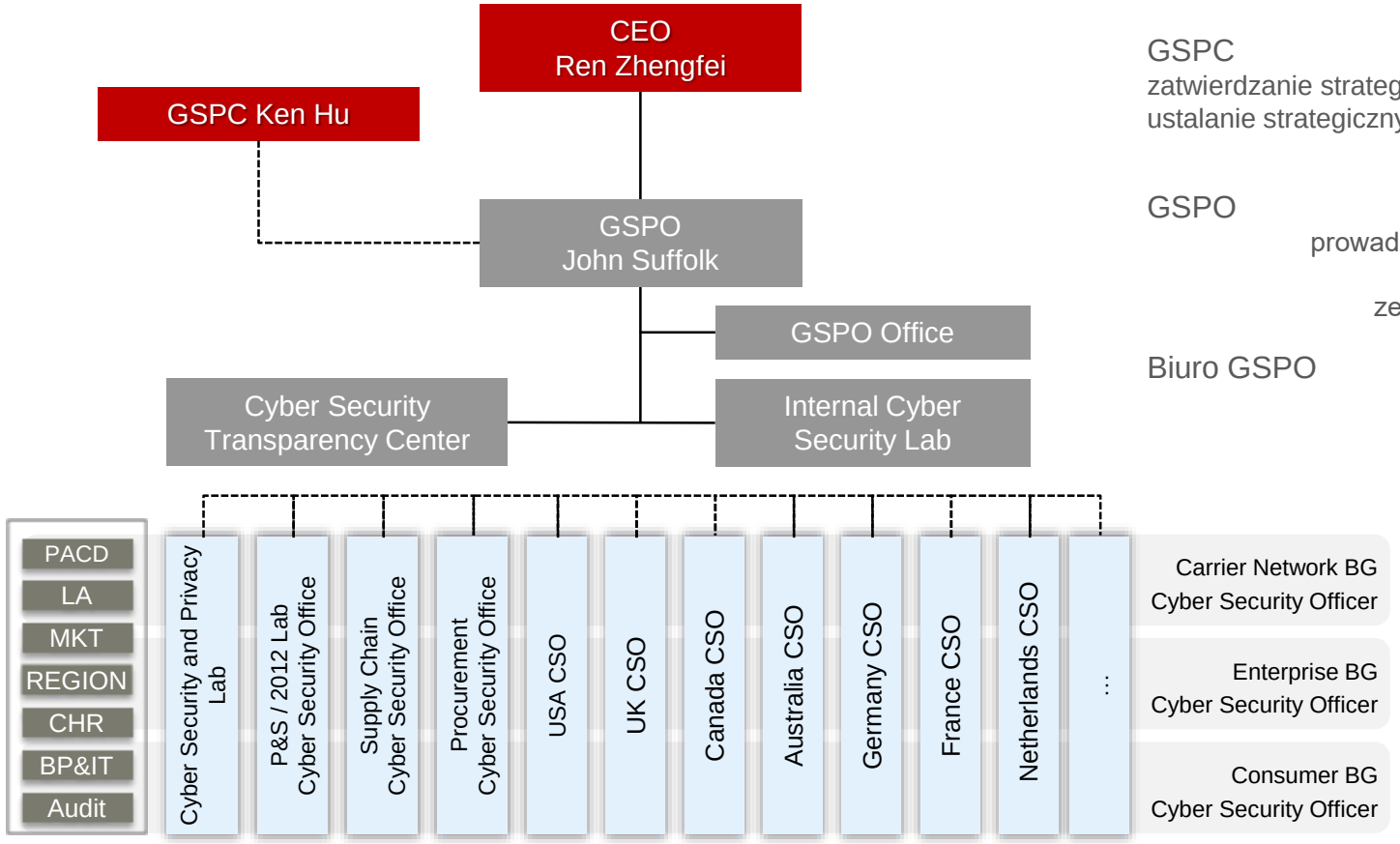
trzy metody (od)budowy zaufania*:

1. komunikacja
2. laboratoria bezpieczeństwa
3. testy

uwaga na marginesie – opisane działania **nie są reakcją na ostatnie kryzysy wizerunkowe, są w praktyce stosowane od co najmniej roku 2010…*

HUAWEI

„Wbudowana” strategia cyberbezpieczeństwa w każdy aspekt działalności firmy



GSPC

zatwierdzanie strategii, planowanie, polityka, mapa drogowa i inwestycje; ustalanie strategicznych priorytetów, audyt.

GSPO

prowadzenie zespołu do opracowania strategii bezpieczeństwa;
wewnętrzne wdrażanie gwarancji cyberbezpieczeństwa;
zewnętrzne wsparcie dla GR/PR oraz globalnych klientów.

Biuro GSPO

koordynacja szczegółowych operacji;
wsparcie strategii i wdrożenia;
audyt i monitorowanie wdrożenia.

Region/BG/BU CSOs

opracowanie strategii i planowanie cyberbezpieczeństwa regionu/BU/BG oraz prowadzenie wdrożeń;

współpraca z GSPO w celu identyfikacji zmian w procesach BG/BU/departamentów, aby zapewnić pełne wdrożenie strategii i wymagań bezpieczeństwa cybernetycznego.

HUAWEI

Komunikacja

pracownicy R&D
zaangażowani w bezpieczeństwo

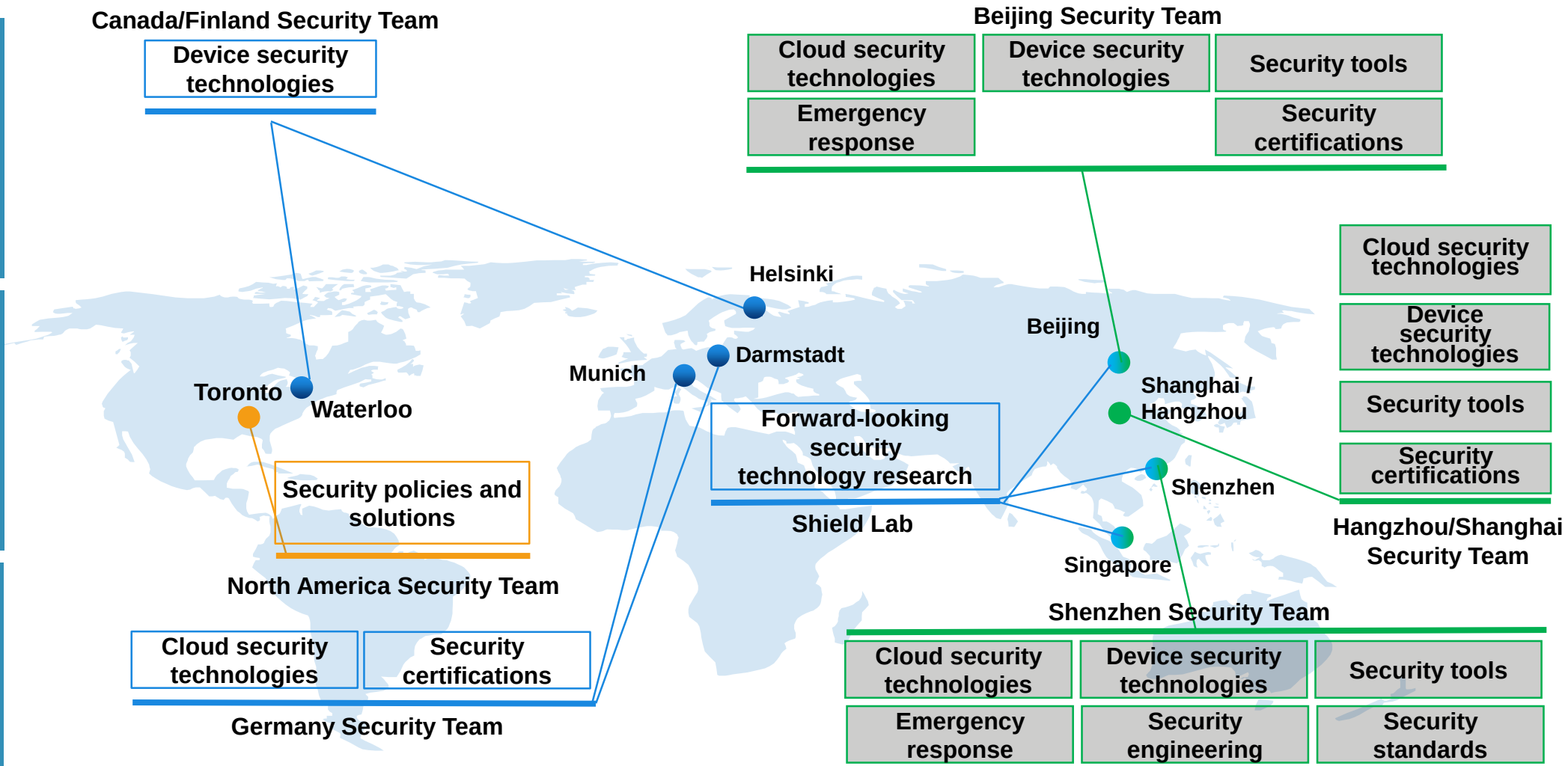
1400

eksperci bezpieczeństwa
z tytułem doktora lub profesora

350

5G: liczba zaakceptowanych zgłoszeń dot. bezpieczeństwa
1 miejsce w świecie

144



HUAWEI

Huawei zainwestuje w bezpieczeństwo 2 mld USD w ciągu najbliższych 5 lat

Komunikacja

Pięć kluczowych filarów cyberbezpieczeństwa i prywatności

Cyberbezpieczeństwo R&D

- aktywny udział w organizacjach normalizacyjnych
- integracja procesów cyklu życia IPD
- wykorzystanie najlepszych praktyk w zakresie bezpieczeństwa przemysłowego (OpenSAMM, BSIMM, Microsoft SDL itp.)

BSIMM

2017: Huawei sklasyfikowany w czołowej 8 firm zgodnie z oceną BSIMM

Cyberbezpieczeństwo dostaw

- kontrola całego łańcucha dostaw, począwszy od materiałów przez produkcję, aż po dostawę do klienta
- globalne zarządzanie logistyką i dostawcami

2018: Huawei uzyskuje certyfikat ISO 28000

Cyberbezpieczeństwo usług

- bezpieczeństwo infrastruktury, aplikacji, danych i personelu
- weryfikacja pod kątem odpowiedzialności
- kodeks postępowania w zakresie bezpieczeństwa i ochrony prywatności

2017: Huawei uzyskuje certyfikaty ISO 20000 oraz ISO 27001

Cyberbezpieczeństwo HR

- personel o nieposzlakowanej opinii
- budowanie świadomości

2018: laboratorium Huawei ICSL uzyskuje certyfikat ISO/IEC 17025

Zarządzanie i informowanie o lukach bezpieczeństwa

- odpowiedzialne informowanie o wykrytych lukach
- terminowa reakcja

PSIRT

rozwój wiedzy na temat najlepszych praktyk w branży w zakresie zarządzania lukami: CVSS, CPE, CVRF, itp.

HUAWEI

Laboratoria bezpieczeństwa

Internal Cyber Security Lab (ICSL)

- powołane w 2010 roku w celu dbania o jakość i bezpieczeństwo produktów
- ulokowane w kampusie Dongguan na północ od Shenzhen
- trzykrotnie certyfikowane na zgodność z ISO 17025
- prawo „veta” przy wprowadzaniu produktu na rynek (w ok. 100 przypadkach miało zastosowanie)
- roczny budżet ok. 9 mln EUR
- testy „black box”, „white box”(testy penetracyjne, analiza kodu źródłowego…)
- zakres działania:
  - zapoznanie ze strategią i podejściem Huawei do bezpieczeństwa
  - demonstracja narzędzi, metod, procedur
  - udostępnia platformę wykonywania testów: wydzielona i niezależna przestrzeń biurowa, odseparowana sieć, drobiazgowa kontrola dostępu itp.

https://www.usine-digitale.fr/article/entre-investissements-et-communications-huawei-essaie-de-rassurer-l-occident-au-sujet-de-sa-politique-en-matiere-de-cybersecurite.N833215

HUAWEI

Laboratoria bezpieczeństwa

European Cyber Security Transparency Centre (ECSTC)

- powołane w 2019 roku
- Rue Guimard 9, 1000 Bruxelles
- centrum komunikacji związanej z bezpieczeństwem

  kompleksowa platforma wiedzy wykorzystywana w komunikacji zewnętrznej, stosowana do prowadzenia polityki informacyjnej, zacieśniania współpracy i zwiększenia wzajemnego zaufania oraz prezentacji korporacyjnych wartości
- centrum wystawowe związane z aspektami bezpieczeństwa

  prezentacja strategii i podejścia Huawei do zagadnień cyberbezpieczeństwa, stosowanych rozwiązań bezpieczeństwa oraz zasobów R&D
- laboratorium testów bezpieczeństwa

  udostępnia klientom platformę dostępu do ICSL w celu umożliwienia np. testów typu „white box”, „black box”…

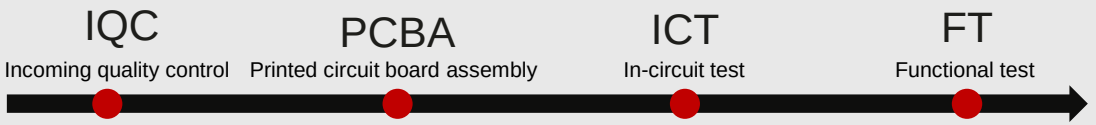
https://www.itproportal.com/news/huawei-launches-european-cybersecurity-centre/

HUAWEI

Laboratoria bezpieczeństwa

Linie produkcyjne

- prezentacja aspektów cyberbezpieczeństwa w odniesienia do procesów łańcucha dostaw i produkcji (zapobieganie naruszeniom, weryfikacja integralności, kontrola antywirusowa itd.) w rzeczywistym środowisku linii produkcyjnej Huawei



Laboratoria bezpieczeństwa

Współpraca zamiast izolacji: Huawei Cyber Security Evaluation Centre (HCSEC) UK

- otwarte w 2010
- efekt uzgodnień rządu UK i Huawei:
  - zarządzania postrzeganymi ryzykami wynikającymi z zaangażowania Huawei w części krytycznej infrastruktury krajowej w Wielkiej Brytanii.
  - zapewnienie oceny bezpieczeństwa dla szeregu produktów używanych na brytyjskim rynku telekomunikacyjnym
- jako jedyni wdrożyliśmy taki mechanizm weryfikacji, z którego powstaje publiczny raport
- procent wykrytych podatności: znacznie poniżej „branżowej średniej”

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

HUAWEI

Laboratoria bezpieczeństwa

Współpraca zamiast izolacji: Germany-Huawei Cyber Security Innovation Lab

- otwarte w 2018
- efekt uzgodnień rządu Niemiec i Huawei z 2017 roku, które finalnie doprowadziło do podpisania porozumienia o współpracy
- strona rządowa:
  - zatwierdza i wystawia odpowiednie certyfikaty
  - definiuje wymogi bezpieczeństwa dla nowych technologii
- Huawei:
  - zapewnia platformę i wsparcie dla prowadzonych badań,
  - weryfikuje i rozwiązuje problemy

HUAWEI

Testy

- udostępniane zasoby:
  - narzędzia i środowisko testowe
  - dokumentacja projektowa
  - **kod źródłowy oprogramowania**

Testy

Porozumienie
(umowa handlowa)

Huawei

- zapewnia zasoby
- dostarcza produkty do badań
- udostępnia dokumentację
- weryfikuje istnienie problemów w raportach innych firm
- rozwiązuje wszystkie zidentyfikowane problemy w produktach

klient

- definiuje wymagania
- chroni IPR Huawei
- przeprowadza testy „black box” lub „white box” (samodzielnie lub poprzez firmę trzecią)
- może użyć własnych narzędzi programistycznych
- musi zgłosić Huawei wszelkie luki lub anomalie wykryte podczas oceny

HECSC

- kod źródłowy jest przechowywany w siedzibie firmy Huawei, klienci mogą przeglądać i testować kod źródłowy zdalnie za pośrednictwem „cienkiego klienta” na platformie HECSC
- zapewnia niezbędne szkolenie dotyczące produktu i środowiska

HUAWEI

Cyberbezpieczeństwo R&D

szczególna rola standardów w produktach:

- potwierdzenie bezpieczeństwa przez zgodność oferowanych rozwiązań z międzynarodowymi normami
- publikowanie własnych innowacyjnych specyfikacji jako międzynarodowe standardy

HUAWEI

Zgodność ze standardami – przykład PLC-IoT

- szerokopasmowa komunikacja PLC (2-12 MHz)
- przepływności do 3,47Mbps (basic) / 24,65 Mbps (extended)
- zastosowanie standardów:
  - specyfikacja Huawei PLC-IoT opublikowana 7 maja 2018 roku jako międzynarodowy standard IEEE 1901.1
  - algorytmy szyfrujące bazujące na AES-256 (AES opisane jako międzynarodowy standard FIPS-197 od roku 2001)
  - dziedziczenie zaawansowanych mechanizmów bezpieczeństwa z IEEE 1901 (specyfikacja opublikowana 30 grudnia 2010)

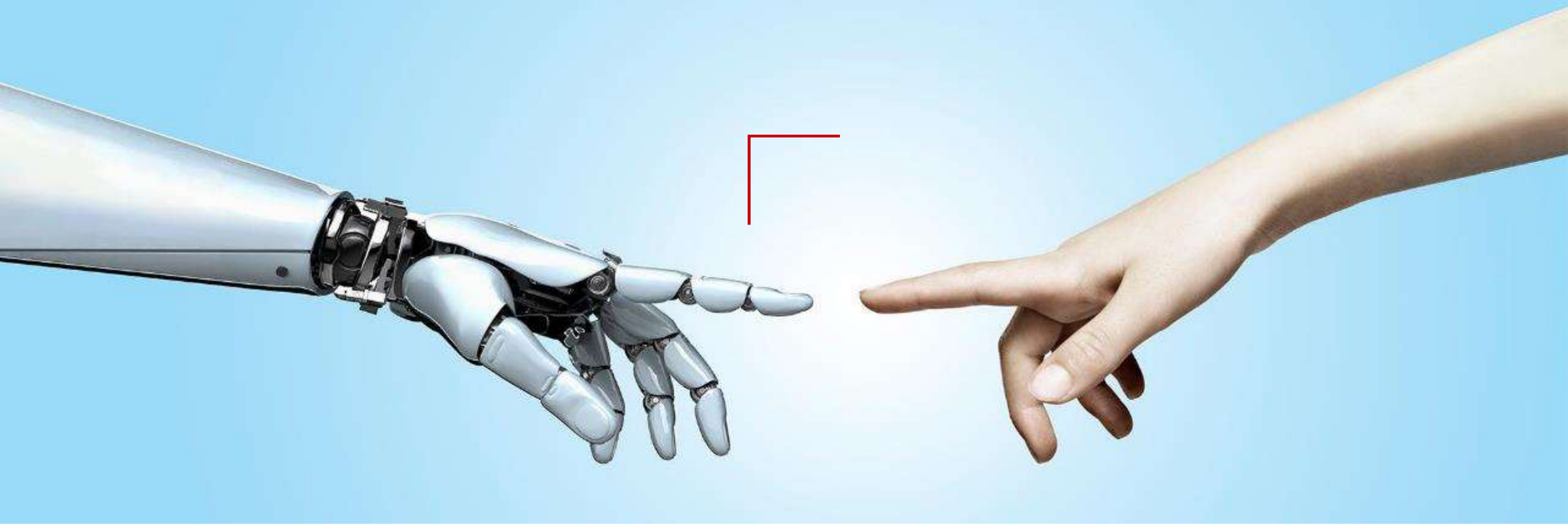
HUAWEI

Uwagi końcowe

- stosowanie powszechnie stosowanych komponentów open source / third party może być (słusznie) postrzegane jako ryzyko:
  - *przykład: luka w bezpieczeństwie bibliotek OpenSSL [2014]…*
- niewiele firm na świecie jest w stanie postępować do tego stopnia otwarcie i transparentnie jak Huawei, by udostępnić do audytu kod źródłowy rozwiązań funkcjonujących w infrastrukturze krytycznej:
  - *pytanie#1: czy kraj pochodzenia dostawcy powinien być kluczową przesłanką kwestionującą bezpieczeństwo rozwiązania?*
  - *pytanie#2: czy najlepszą metodą rozstrzygania wątpliwości nie powinna być możliwość weryfikacji kodu źródłowego (vide: _NSAKEY [1999] …)?*

HUAWEI

Q&A



HUAWEI

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.