



Office of Commercial & Economic Analysis

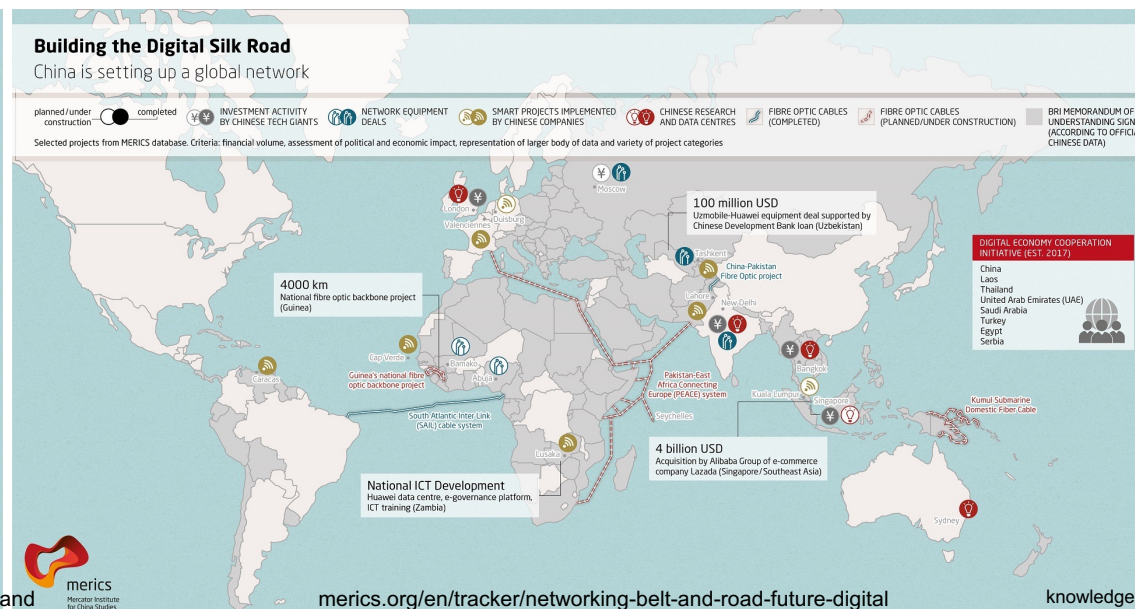
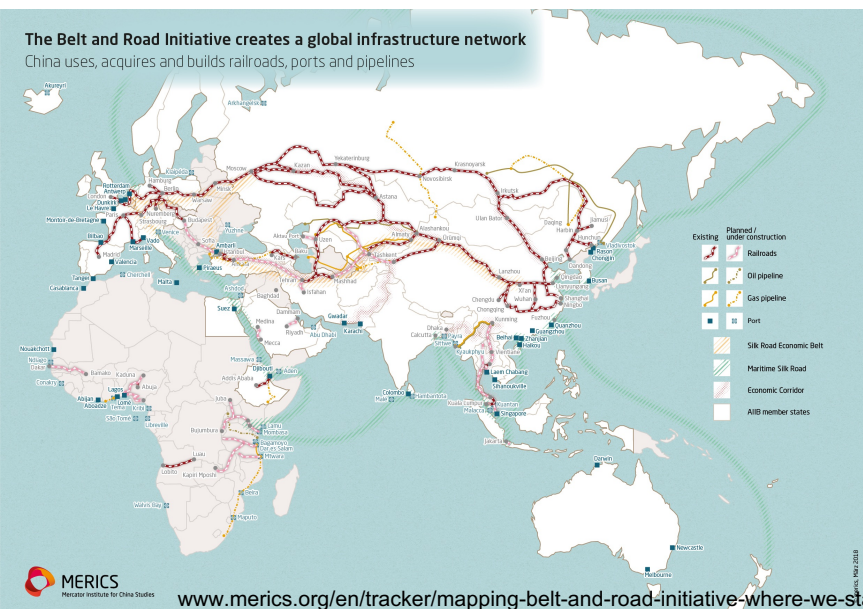
China's Quest for ICT Dominance and Proposed DAF Countermeasures

**Office of Commercial and Economic Analysis (OCEA)
Office of the Secretary of the Air Force**

The contents of this presentation do not represent the official view of the Department of the Air Force nor the Department of Defense

Overall Briefing: UNCLASSIFIED

- **Belt and Road Initiative (BRI)**
Creating a global infrastructure network over land and sea
- **Digital Silk Road (DSR)**
Tapping into BRI countries with digital infrastructure and connectivity
- **Made in China (MIC) 2025**
Focusing to become a leader in manufacturing of 10 advanced technology sectors



■ **Military-Civil Fusion (MCF)**

Reorganizing to ensure that the S&T enterprise supports both economic and military development*

■ **Standards 2035**

China's blueprint for their government and companies to set the international standards for emerging technologies – not only to support China's commercial interests but also their push for “cyber sovereignty” (CCP control over cyberspace)**

■ **China's National Intelligence Law:**

China claims: *“These are independent companies ... they would not be requested to spy or act on demands from their government”* but China's law require Chinese companies to cooperate in Chinese intelligence gathering – 2017 National Intelligence Law, article 7

Timeline:

- 1994-2001 China invites foreign telecom vendors to bid for the China market: test equipment; transfer IP; set up local manufacturing
- 2000 Lucent (US) #8, Motorola (US) #24 in global market value; Nortel (Canada) 35% of TSE300; Huawei and ZTE are basically non-entities
- 2001 North American companies win about 90% of China's new 2G network (\$1B each)
- 2004 Huawei gets \$10B financing from the Bank of China to expand globally
- Mid-2000's Huawei undercuts pricing globally
- 2009 China awards 3G networks to Huawei/ZTE 80% and foreign companies 20%
- 2009 Nortel declares bankruptcy while Lucent, Motorola's network equipment business dwindles
- 2009 China Development Bank provides \$30B line of credit to Huawei for further global expansion

China lifted Huawei to global leadership at the expense of the world's mobile telecom vendors

- ABB (Swiss-Swedish) is #2 globally in robotics/discrete automation
- Early entrant in the China robotics market by setting up value chain, R&D, manufacturing, system service – now #1 in China
- In 2019, ABB began building *“the world’s most advanced, automated and flexible robotics factory - a cutting-edge center where robots make robots.”*
The factory was completed in Dec 2022
- ABB says that this effort is **in direct support of Made in China 2025** and that *“China’s commitment to transform its manufacturing is a torchlight for the rest of the world. Its strategic embrace of the latest technologies for artificial intelligence, advanced robotics and cloud-based computing present a playbook for every country that wishes to have a globally competitive manufacturing base.”*



Is ABB following in the footsteps of Lucent, Motorola and Nortel?!

The China Playbook: The Vision of “Made in China 2025”

FOLLOW & CAPTURE

Identify Priority Technology for Capture

Visit foreign
HQs, labs

Request
foreign IP

Manufacturing
in China

Partner in
China

Invest or
acquire foreign
companies

Theft of
IP,
products

Foreign
universities &
institutes

POSITION FOR DOMINANCE

Chinese
government
financing

Convert above
technology into
products

Insert globally
and into BRI
countries

Create dependency on
China for supply chain
and manufacturing

Use local dominance
for income and data
source

GLOBALLY

Lower global
pricing level

Gain global
market share

Influence global
standards

Produce global
patents

Achieve Global Dominant Market Lead Position
Eliminating Alternative Vendors/Providers

Recent Strategy Tweaks:

- Seek investment in Chinese startups
- Increase basic R&D
- Recruit experts both foreign and Chinese
- Stock up on foreign components
- Move toward independence from foreign supply

UNICORN: Private company (start-up) valued at over \$1 billion

- Chinese unicorns have doubled over the past 5 years (over 300 in 2022)
- Previous (2017): eCommerce, consumer Internet
- Recent (2022): AI, semiconductors, advanced robotics, health tech, green tech, new energy; meanwhile major decrease in eCommerce, fintech, education technology
- Investment control shifted from big tech companies (Baidu/Alibaba/Tencent) to government
 - Managed by state-owned enterprises (SOE); state-backed funds
 - Fusion of state owned and local market-based funding

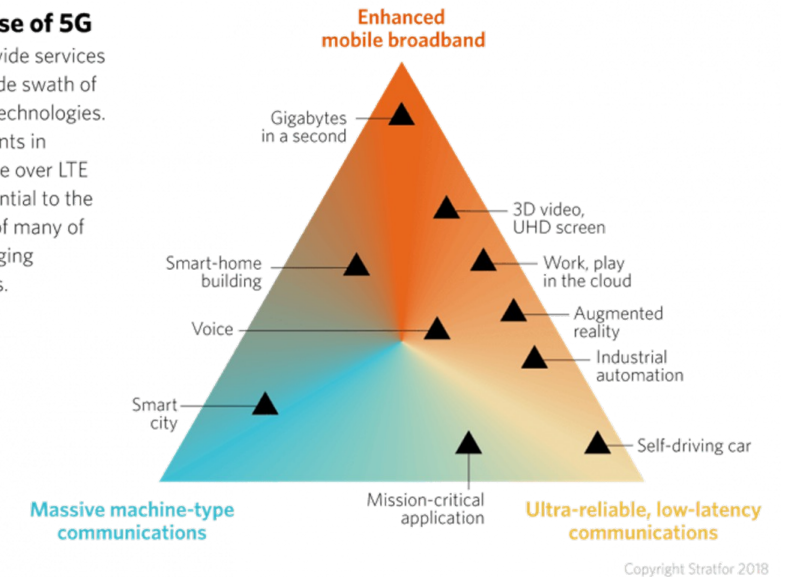


“This seems to mirror Xi Jinping’s focus on national security and national greatness – reducing “disorderly expansion of capital” to assert more control where investment takes the cue from the CCP”*



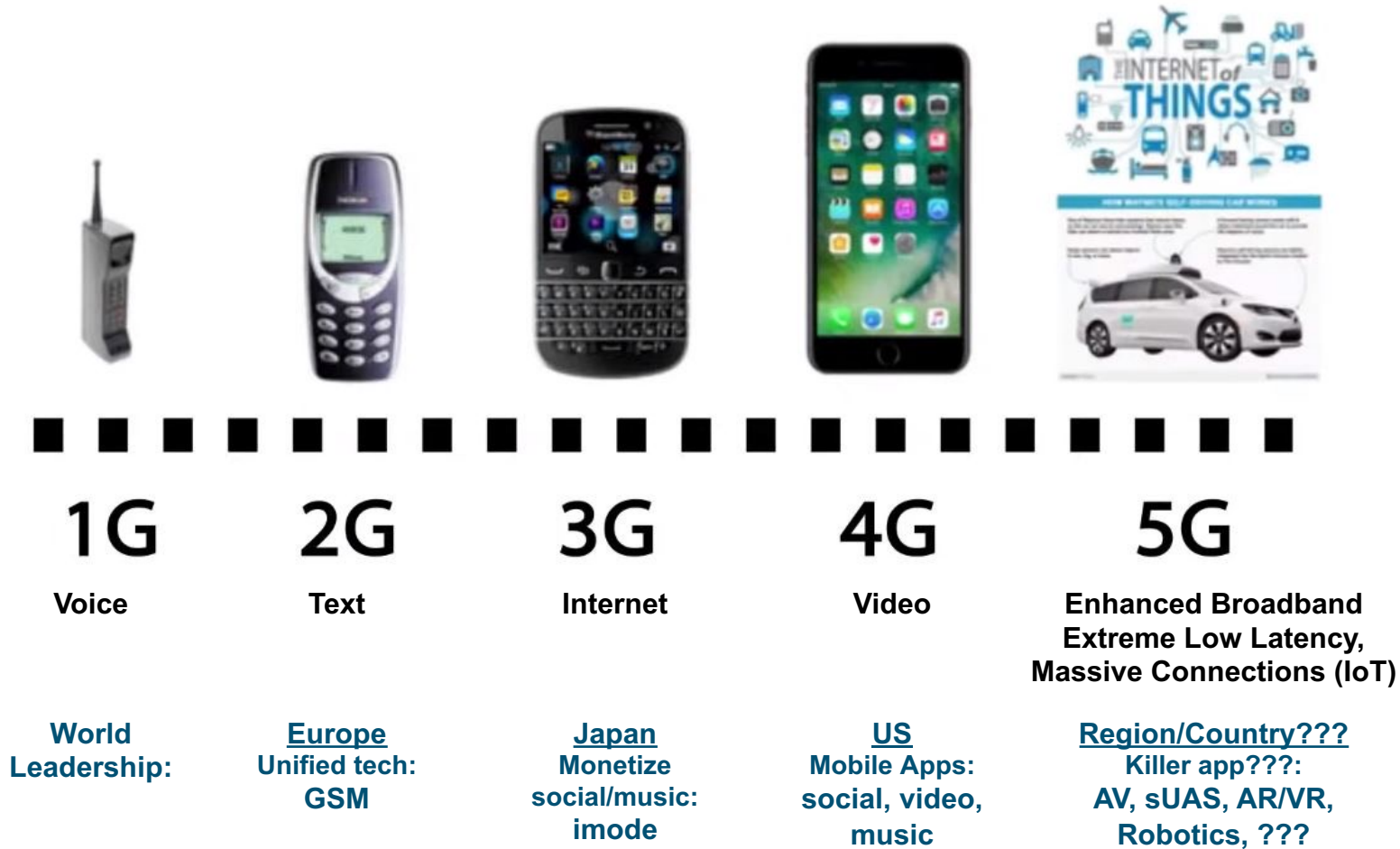
Future Use of 5G

5G will provide services across a wide swath of disruptive technologies. Improvements in performance over LTE will be essential to the future use of many of these emerging applications.

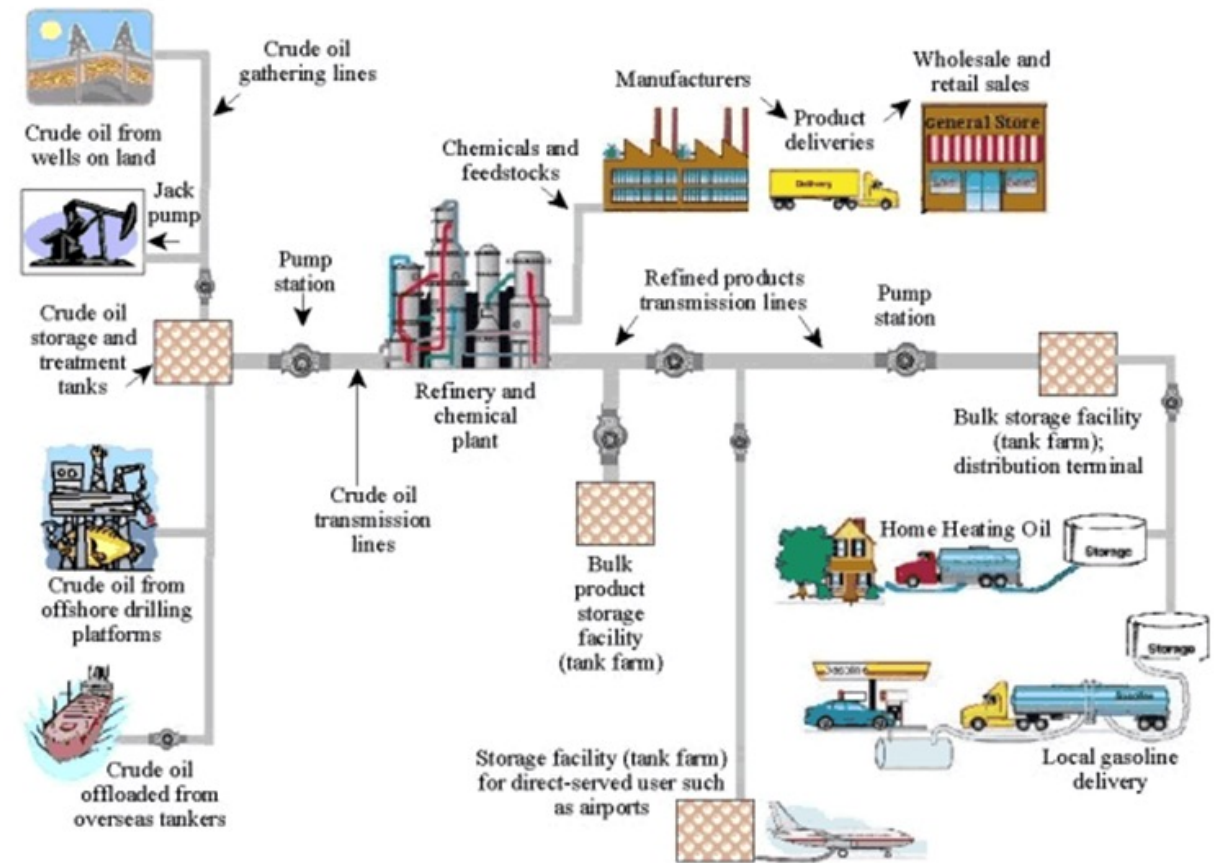
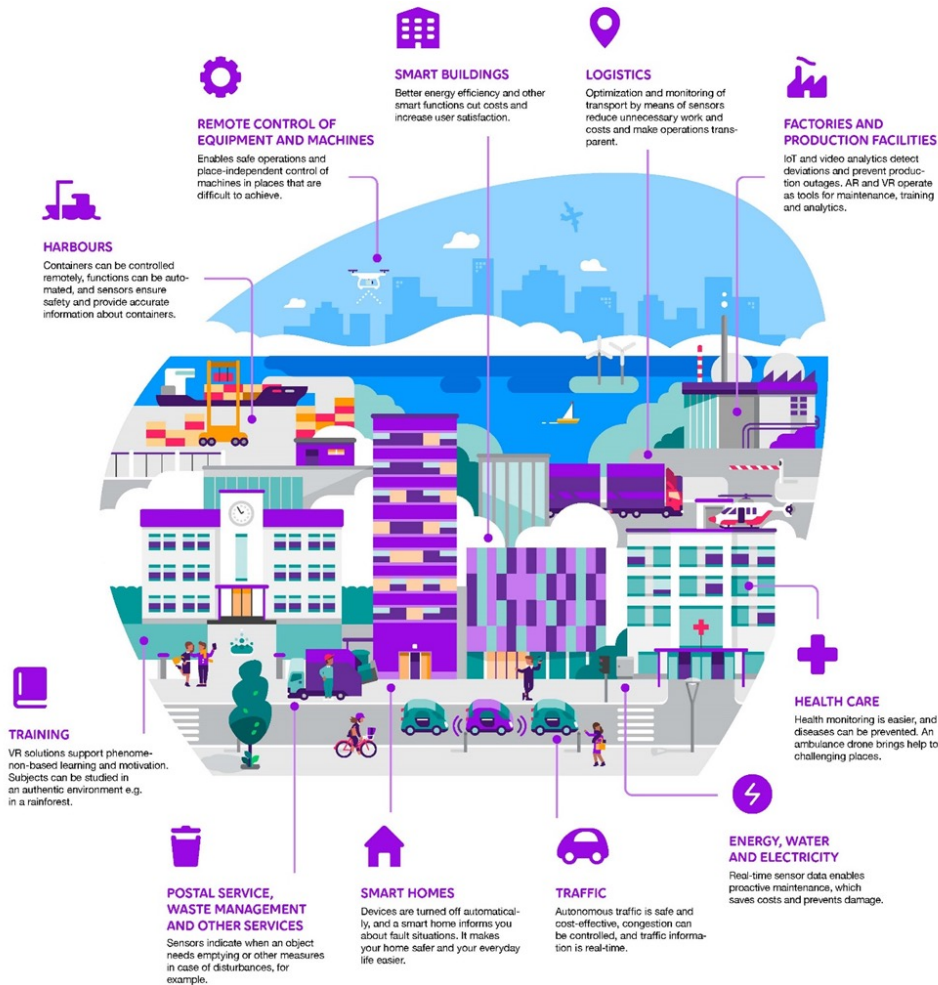


Attributes:

- Extremely high speed data
- Connected to Everything (IoT)
- Almost no time delay (low latency)
- Combined with AI for real-time applications

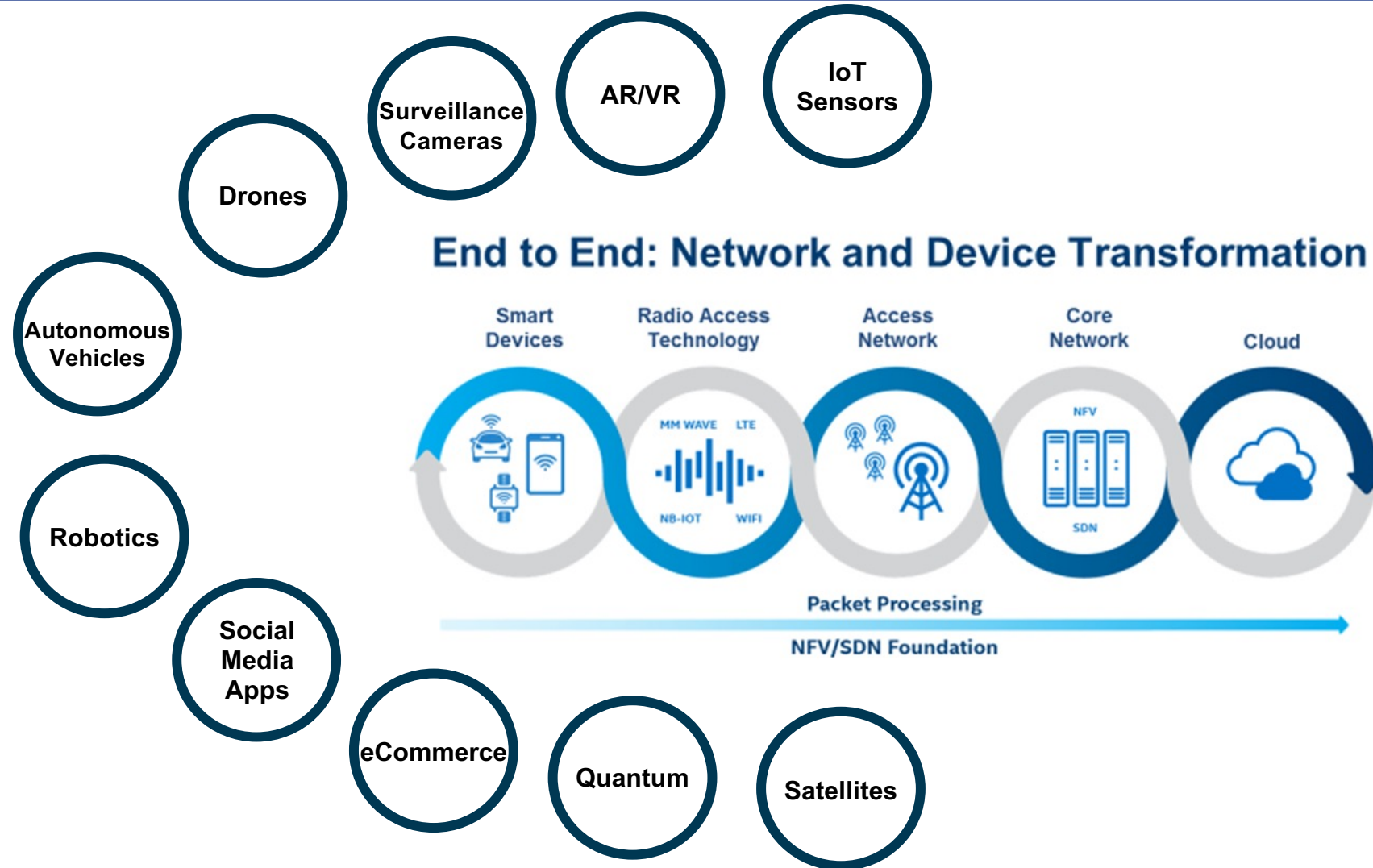


Generational leadership has led to economic and innovative leadership

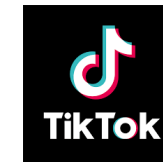
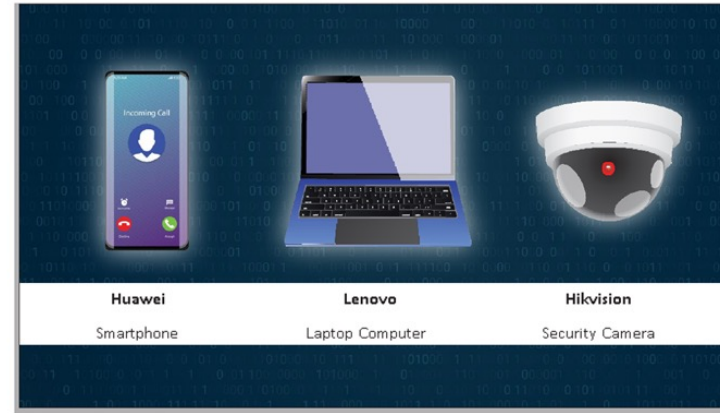


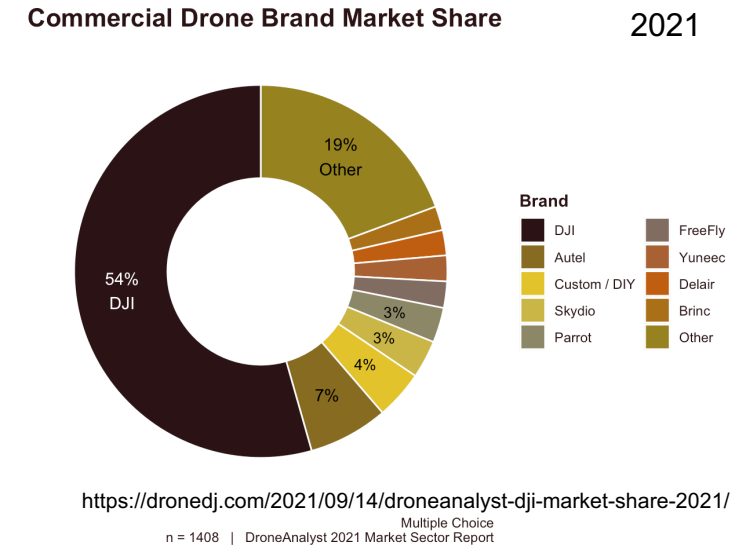
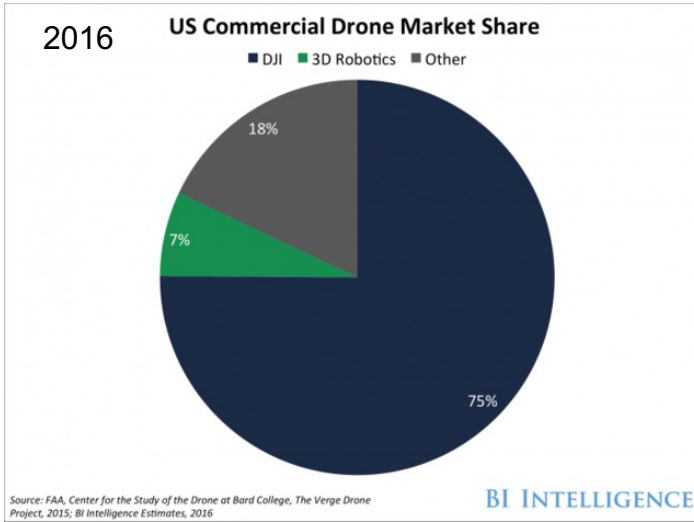
Potential Example: Oil end-to-end process monitoring and automation

The 5G Ecosystem Is Much More Than Just Basic Infrastructure



- End User Devices (phones, laptops)
- Surveillance Cameras
- Small UAS
- IoT
- Mobile Apps
- Cloud





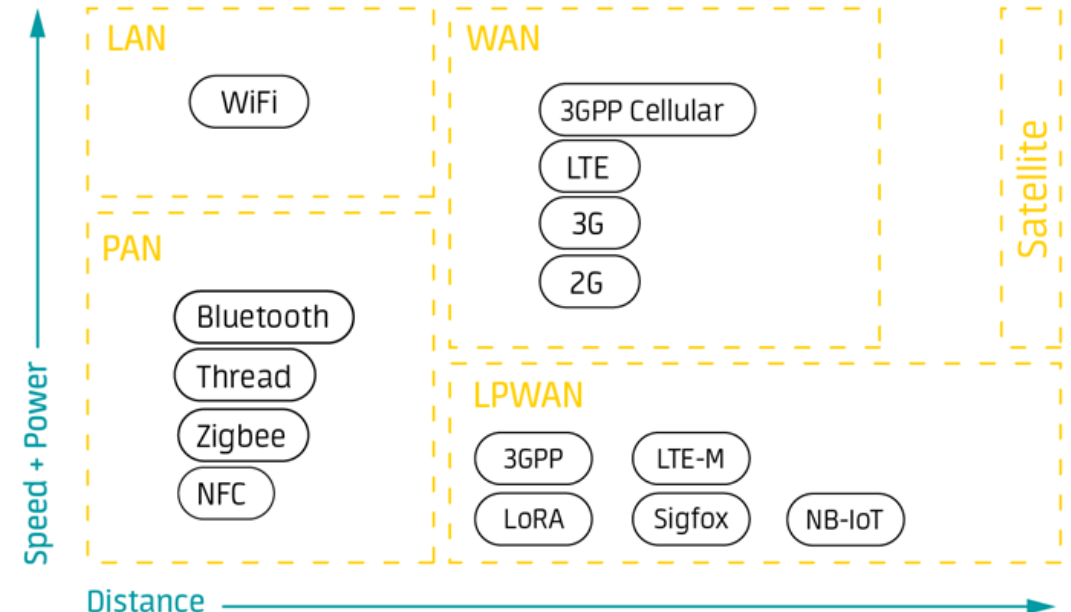
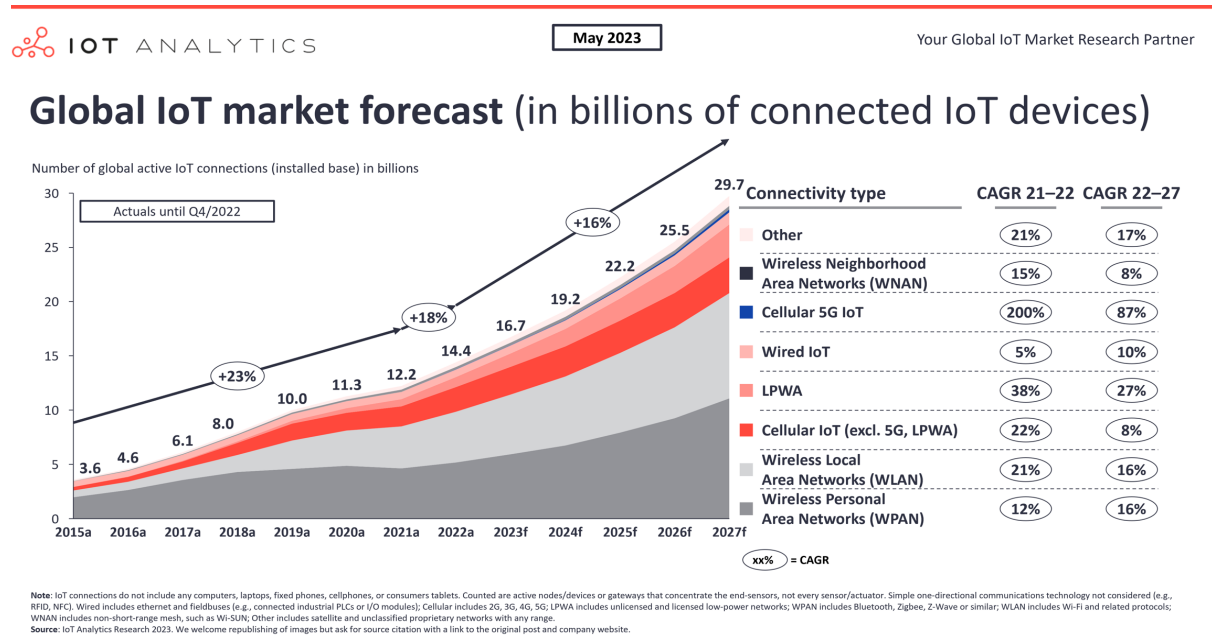
Timeline of Restrictions on DJI:

- 2017 - U.S. Army stopped use
- 2019 - Congress used the NDAA to prohibit Chinese UAS for DoD
- 2020 – Commerce added DJI to Entity List
- 2021 – American Security Drone Act prohibited USG acquisition
- 2022 – Countering CCP Drone Act had FCC add DJI to their Covered List
- 2023 – American Security Drone Act proposed by Congress
- 2023 – States seeking restrictions



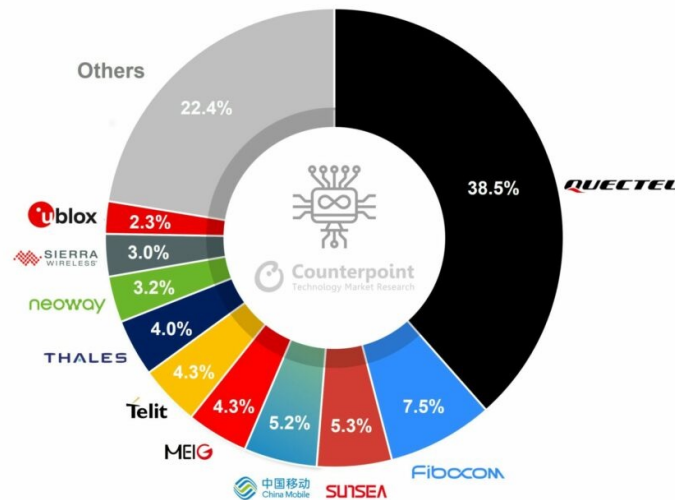
- DoD selected 6 non-Chinese companies to build a short-range reconnaissance aircraft for the U.S. military
- This effort expanded to DIU's Blue UAS program to validate drones for USG acquisition
- Currently, DIU has 16 validated products on the approved list: www.diu.mil/blue-uas
- These vendors need scale to reduce price and increase feature capability: it is vital for USG and allies/partners to shift to trusted vendors
- For security recommendations from CISA: www.cisa.gov/resources-tools/resources/secure-your-drone-privacy-and-data-protection-guidance

- IoT is growing rapidly with 29 Billion devices forecasted by 2027
- Large variety of configurations and architecture choices
- Low power non-cellular connections will continue to be predominant
- Low power Wide Area Networks (LPWAN) includes cellular (NB-IoT, LTE-M) and non-cellular (LoRa, Sigfox)
- Broadband and Critical Use Case IoT (4G/5G) will grow to become 60% of cellular IoT by 2028
- Reduced capacity (RedCap) devices based on 3GPP Release 17 are just now being announced and will contribute to Broadband IoT growth*



China's Dominant Position in Cellular IoT

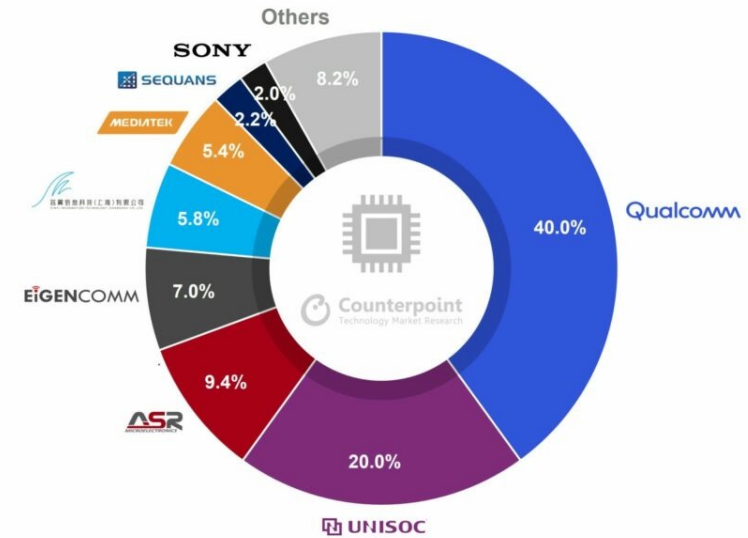
Global Cellular IoT Module Shipments Share by Vendor, 2022



Source: Counterpoint Research Global Cellular IoT Module and Chipset Tracker by Application, Q4 2022

- Chinese companies make up the top 5 Cellular IoT **module** vendors with over 60% market share
- Significant consolidation:
 - Automotive (heavy customization; lower margins) 2019 Telit automotive to TUS (China); 2020 Sierra Wireless to Rolling Wireless (Fibocom China); Thales and uBlox only non-Chinese left in automotive
 - Telit and Thales have merged to become Telit Cinterion (UK)
 - Semtech (US) acquired Sierra Wireless (Canada)

Global Cellular IoT Chipset Shipments Share by Vendor, 2022

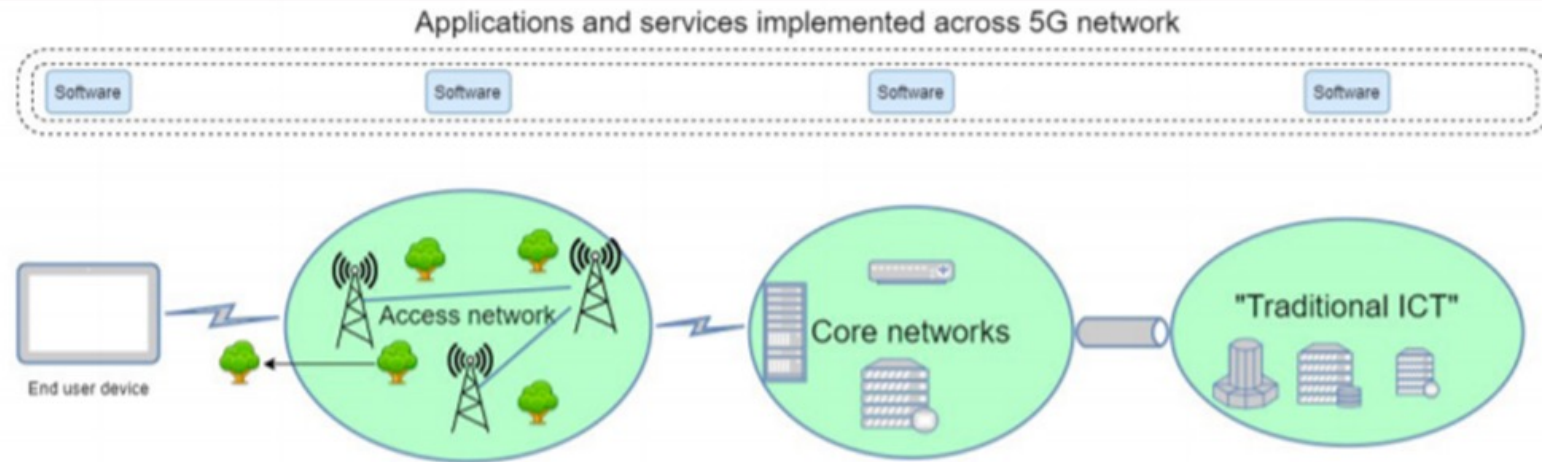


Source: Counterpoint Research Global Cellular IoT Module and Chipset Tracker by Application, Q4 2022

- Although Qualcomm (U.S.) leads in **chipsets**, Chinese companies are emerging quickly; Huawei's Hisilicon's position is being taken by Unisoc and new successful low-cost/high-volume NB-IoT vendors Eigencomm and Xinyi Semiconductor
- IoT **Platforms** (SW tool to build and manage IoT) are led by the U.S. (Microsoft, AWS, Google Cloud) but they still depend on components/devices from China
- Chinese IoT Platform companies are being promoted by the Chinese government (tuyu, Alibaba Cloud, Baidu IoT Core, Huawei)

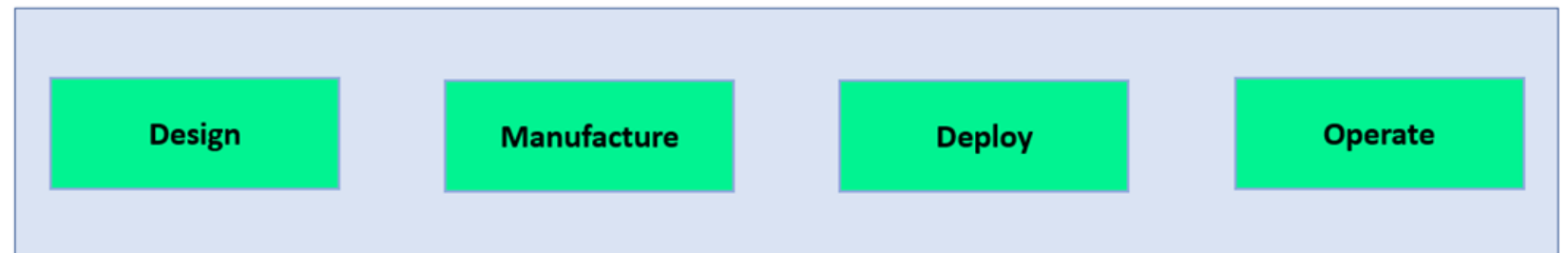
■ The end-to-end network view:

- End devices
- Radio Access Network
- Core Network
- Backhaul/transmission



■ The design through operate view:

- Design
- Manufacture
- Deploy
- Operate



1. Design holistically upfront
2. Develop trusted relationships

3. Initial and ongoing testing
4. Rollout in phases

- **Promote – to stay ahead and foster our innovative engine**
 - Rollout rapidly in phases – don't wait for the final product
 - Buy commercially available for speed to market – adapt for military use
 - Develop the enhanced capabilities (sUAS, AR/VR, IoT, robotics, etc.)
 - Integrate satellite capabilities – this can be an alternative ICT solution in developing countries*
 - Support standards development – to enhance security and military related applications
 - Collaborate with trusted vendors, operators and integrators – design and implement together
 - Collaborate with trusted allies and partners – complement capabilities and build scale for safe solutions
- **Protect – Establish safeguards and proactive design/controls**
 - Design with security end-to-end at the forefront
 - Verify supply chain purity – incorporate into requirements/contracts (incl. OCEA Due Diligence support) and keep untrusted HW/SW/devices/apps out of DAF networks
 - Identify supply chain vulnerabilities/chokeholds and propose workarounds – such as DIU's Blue UAS verified vendors/products; scale with trusted suppliers
 - Educate DoD and industry to prevent inadvertent tech transfer (incl. AFOSI support)
 - Take Zero Trust approach – “never trust, always verify”

*<https://breakingdefense.com/2022/02/its-not-just-5g-chinas-telecom-strategy-needs-to-be-counteracted-in-space/>