5G Wireless Networks

MARKET PENETRATION AND RISK FACTORS

5G is the next generation of wireless networks, building upon existing 4G **Long-Term Evolution** (LTE) infrastructure and improving the bandwidth, capacity, and reliability of wireless broadband services. It is intended to meet increasing data and communication requirements, including capacity for tens of billions of connected devices that will make up the Internet of Things (IoT), ultra-low latency required for critical near-real time communications, and faster speeds to support emerging technologies. 5G is expected to bring security improvements and a better user experience, but supply chain, deployment, network security, and competition and choice vulnerabilities may affect the security and resilience of 5G networks.

Select Mobile Network Equipment Components Market Leaders

Data Converter Chip
Market Leaders (2017)[1]
1. **US** Texas Instruments
2. **US** Analog Devices

Field Programmable Gate Arrays (FPGA)
Market Leaders (2017)[1]
1. **US** Intel
2. **US** Xilinx

Ethernet Switch Chips
Market Leaders (2015)[1]
1. **US** Broadcom

Network Processor
Market Leaders (2016)[1]
1. **US** Intel
2. **US** Broadcom
3. **CH** HiSilicon
4. **US** Qualcomm
5. **US** Texas Instruments

Server
Market Leaders (2Q18)[1]
1. **US** Dell
2. **US** HPE
3. **US** IBM
4. **CH** Lenovo
5. **CH** Inspur

Small Cell Antenna Array
Market Leaders (2017)[1]
1. **EU** Alpha Wireless
2. **EU** Ericsson
3. **US** Galtronics

Small Cell Chipset
Market Leaders (2017)[1]
1. **US** Qualcomm
2. **US** Intel
3. **CH** HiSilicon
4. **EU** NXP Semiconductor
5. **EU** Ericsson
6. **US** Cavium

Small Cell Power Amplifier
Market Leaders (2017)[1]
1. **US** Texas Instruments
2. **EU** NXP Semiconductor
3. **US** Qorvo
4. **US** Broadcom
5. **US** Anadigics

US: United States **CH:** Chinese **EU:** European

Market data is based on 4G LTE market share. Additionally, the network architecture and corresponding vendors are intended to be high level. Further granularity would result in a broader list of primary vendors, including additional American-based vendors.

The Cybersecurity and Infrastructure Security Agency (CISA)/National Risk Management Center (NRMC) is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. All NRMC products are visible to authorized users at HSIN-CI and Intelink.

For more information, contact NRMC@hq.dhs.gov or visit https://www.dhs.gov/cisa/national-risk-management-center.

MAJOR COMPONENTS OF 5G NETWORKING

User Equipment

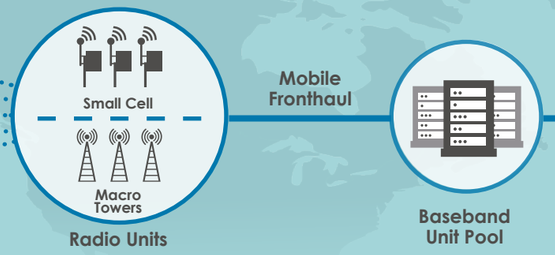
Devices such as smart phones, computers, and Industrial Control Systems (ICS) generate data that is then transmitted to a base station, small cell, satellite, or Internet Exchange Points (IXP). Compromised devices may collect user data and impact local networks and systems, but are unlikely to impact the larger communications network.

Industrial IoT Hardware
Market Leaders (2Q18)[1]
1. **US** Cisco
2. **CH** Huawei
3. **EU** Ericsson
4. **EU** TE Connectivity
5. **US** Qualcomm

Smartphone
Market Leaders (2Q18)[1]
1. **SK** Samsung
2. **CH** Huawei
3. **US** Apple
4. **CH** Xiaomi
5. **CH** OPPO

US: United States **CH:** Chinese **EU:** European **SK:** South Korea

Radio Access Network (RAN)

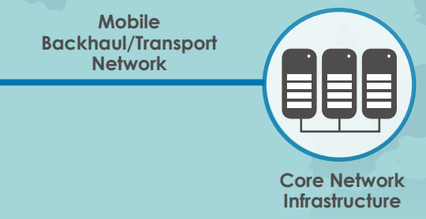


RANs connect wireless or satellite subscriber devices to terrestrial telecommunication networks. Compromised systems may intercept or disrupt data flow and phone calls.

RAN Equipment
Market Leaders (1Q18)[1]
1. **CH** Huawei
2. **EU** Ericsson
3. **EU** Nokia
4. **CH** ZTE
5. **SK** Samsung

Top four vendors account for over 90% of the market.

Core Network



The core network is the backbone of the U.S. communications infrastructure that routes and transports data and connects the different parts of the access network. Compromised core devices may be used to disrupt data and services on a large scale, and impact customers who are interconnected by the access network.

Evolved Packet Core (LTE)
Market Leaders (1Q18)[1]
1. **EU** Ericsson
2. **CH** Huawei
3. **EU** Nokia
4. **US** Cisco
5. **CH** ZTE

Top two vendors account for over 60% of the market.

Service Provider Router and Ethernet Switch
Market Leaders (1Q18)[1]
1. **US** Cisco
2. **CH** Huawei
3. **EU** Nokia
4. **US** Juniper

Top four vendors account for over 90% of the market.

Points of Vulnerability in the 5G Network

SUPPLY CHAIN

ISSUE: The 5G supply chain is susceptible to the malicious or inadvertent introduction of vulnerabilities such as malicious software and hardware; counterfeit components; and poor designs, manufacturing processes, and maintenance procedures.

IMPACT: 5G hardware, software, and services provided by untrusted entities could increase the risk of network asset compromise and affect data confidentiality, integrity, and availability. Even if U.S. networks are secure, U.S. data that travels overseas through untrusted telecommunications networks is potentially at risk of theft, manipulation, and destruction.

DEPLOYMENT

ISSUE: 5G will utilize more information and communication technology (ICT) components than previous generations of wireless networks, and municipalities, companies, and organizations may build their own local 5G networks, potentially increasing the attack surface for malicious actors.

IMPACT: Despite security enhancements compared to previous generations of wireless network equipment and services, 5G networks will need to be properly configured and implemented for those enhancements to be effective. Improperly deployed, configured, or managed 5G equipment and networks may be vulnerable to disruption and manipulation.

NETWORK SECURITY

ISSUE: 5G builds upon previous generations of wireless networks and will initially be integrated with 4G LTE networks that contain some legacy vulnerabilities. Additionally, it is unknown what new vulnerabilities will be discovered in 5G networks.

IMPACT: Some legacy vulnerabilities, whether accidental or maliciously inserted by untrusted suppliers, may affect 5G equipment and networks no matter how much additional security is built in.

LOSS OF COMPETITION AND CHOICE

ISSUE: Despite the development of standards designed to encourage interoperability, some companies (including Huawei) build proprietary interfaces into their technologies. This limits customers' abilities to use other equipment, either in addition to or in replacement of Huawei technology.

IMPACT: Customers who are locked into one technology or service provider may have to choose between continuing to use an untrusted supplier or removing and replacing existing equipment; which may be both expensive and time consuming. Lack of interoperability may also make it difficult for trusted companies to compete, potentially limiting their ability to invest in R&D and eventually driving them out of the market.

[1]Lewis, James. 2018. "How Will 5G Shape Innovation and Security: A Primer." *Center for Strategic & International Studies*. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf. Accessed May 2019.