LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

5G Security for Healthcare

08/20/2020

Report #: 202008201000

Agenda

Logo source: 3GPP

- 5G Overview
- Terminology and concepts
- 5G - Components
- Evolution of 5G
- 5G applications
- 5G Implementation
- 5G and Healthcare
- 5G Exploitation and its Effects
- Defending Against 5G Exploitation
- The Future

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

5G Overview

- Fifth generation cellular network technology (Officially called: 5G New Radio)
- Adopted by 3rd Generation Partnership Project (3GPP) - international organization responsible for 3G UMTS and 4G LTE
- Several improvements:
  - Approximately 10 to 100 times faster than typical current cellular connections
  - Faster than residential physical fiber optic cable
  - Can handle significantly greater number of devices simultaneously (IoT)
  - Significantly reduced latency: 20 milliseconds to 1 millisecond
  - Customized networks – Different networks have different needs for speed, bandwidth, etc…
- Potential issues:
  - High speed/capacity means shorter range of each cell tower, more must be deployed
  - Concerns over health issues
  - Eyesores in residential neighborhoods
- Operates on variety of frequencies, including recycled frequencies of decommissioned networks
  - 2G DCS, 3G ESM, PCS, etc…
- Not incremental or backward-compatible
  - No overlap with 4G LTE or WiMax

Image source: Meridian IP Communications

Terminology and concepts

Some important terms and acronyms that we will use in this presentation:

Millimeter waves – Higher spectrum band (typically 24 GHz to 100 GHz), tradeoff between very high transmission speeds but shorter broadcast range.

Small Cells – The backbone of a 5G network; low-power, short-range broadcasts (much smaller than previous cellular networks). The radios are smaller and lower-profile and can be hung up on street lamps, poles, rooftops or other areas.

Massive MIMO (Massive multiple-input, multiple-output) – Groups together antennas at the transmitter and receiver to provide better throughput and better spectrum efficiency.

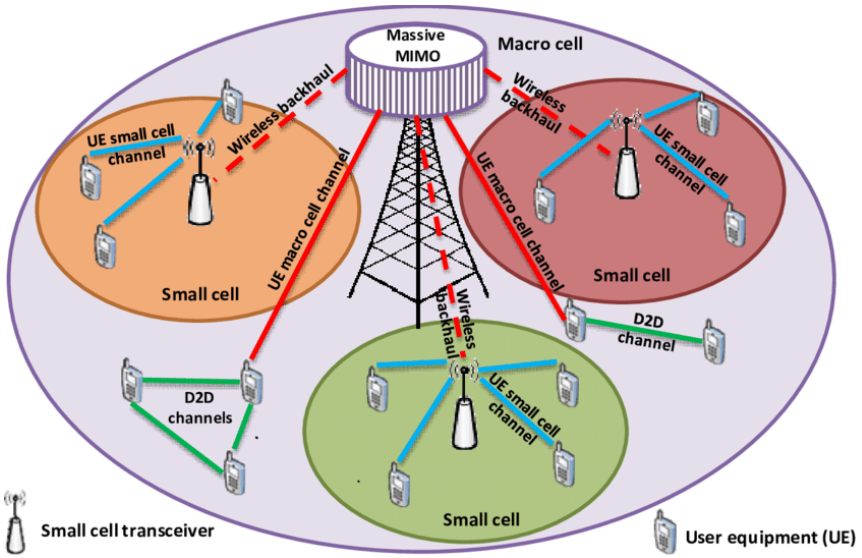
Beamforming – A technology that allows for the directing of a 5G signal in a very specific direction, vice an omnidirectional transmission.

Full Duplex – Data that can be transmitted in both directions at the same time.

User Equipment – The user's mobile device which accesses the 5G network.

One source for further 5G terminology is Keysight's 5g Terms and Acronyms: https://www.keysight.com/us/en/assets/7018-06171/brochures/5992-2996.pdf

Image source: ResearchGate



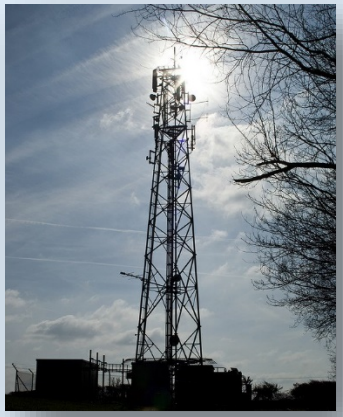


Image source: Wired

Traditional cell tower vs. small cell

Image source: Techspot

Terminology and concepts (continued)

Other concepts and definitions:

Virtual Reality – A simulated three-dimensional world experience that can respond to interactions by the user.

Augmented Reality – Similar to virtual reality, augmented reality does not present a total world experience to the user, but instead presents virtual objects appearing to exist in the real world which can respond to interactions by the user.

Distributed Denial of Service Attack (DDoS) – An attack which intends to render the target system(s) and/or network(s) unusable by authorized individuals by flooding them with traffic or bogus requests originating from a large number of attacking system.

Latency – The response time of an information system to a user or agent request.

Multi-Factor Authentication (MFA) – A methodology of access control which requires the requesting user to present multiple of the following categories of authentication for access to a resource:

1. Something you have
2. Something you know
3. Something you are

Image source: Allot.com

5G - Components

Three categories of components:

- User Equipment
- Radio Access Network (RAN)
- Core network

Note the number of non-US component manufacturers.

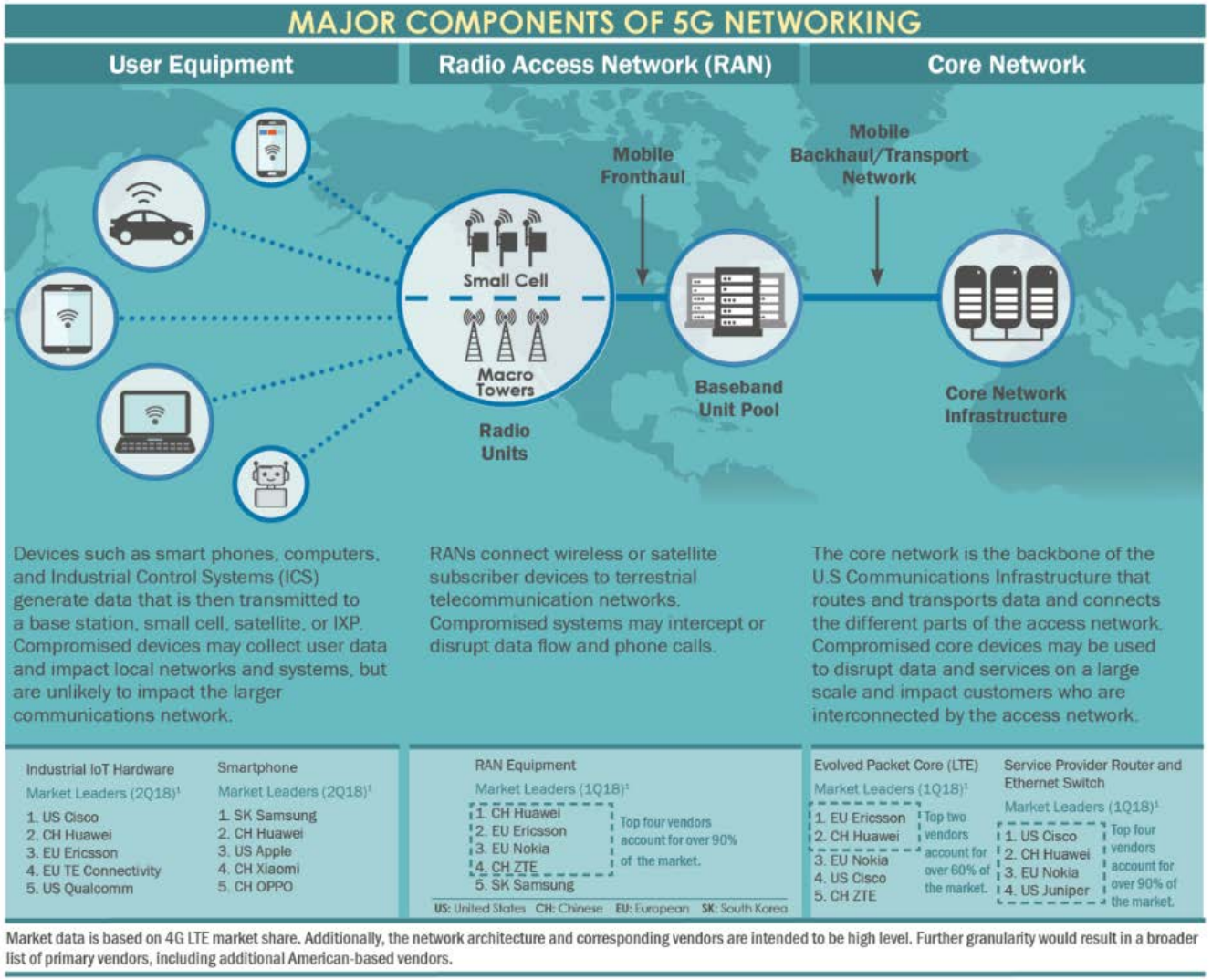


Image source: Department of Homeland Security - CISA

Evolution of 5G

- 5G – How did we get here?
  - Cellular technology is ~40 years old
    - First generation went operational ~1980
  - About a decade between generations
  - Significant new capabilities each generation:
    - Faster speeds
    - Improved memory
    - Improved storage
    - Improved protocols
    - Greater connectivity

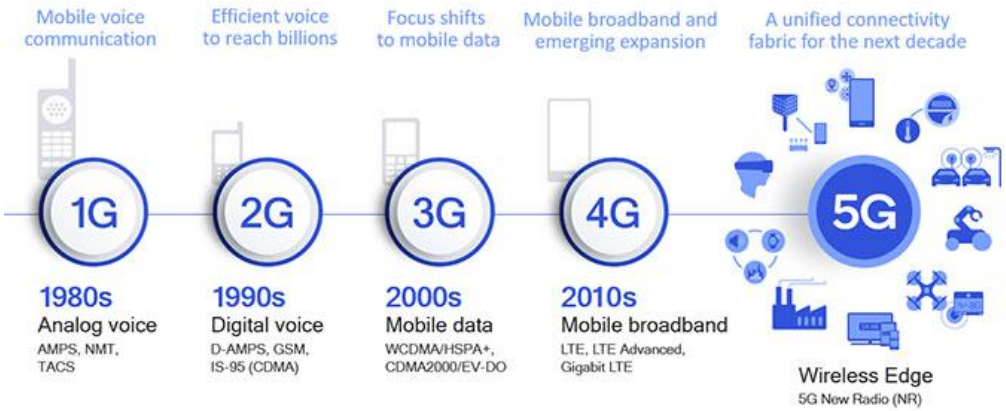


Diagram source: System One

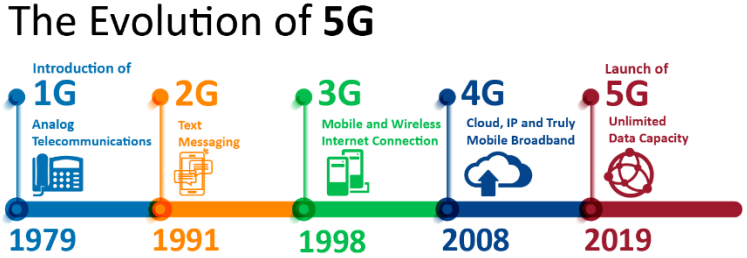


Diagram source: System One

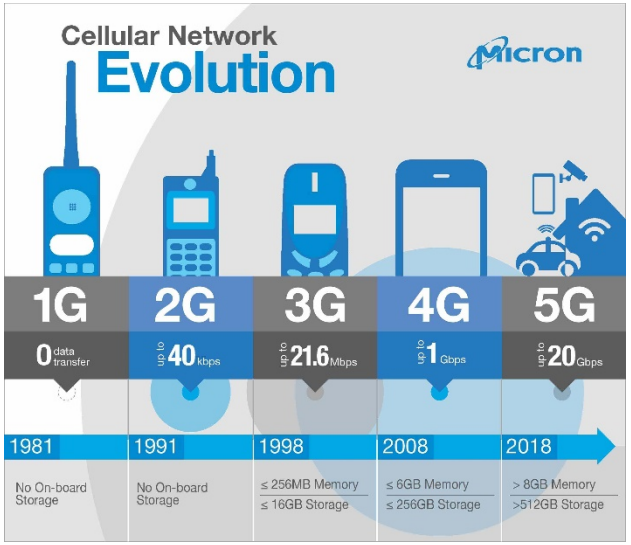


Diagram source: EE Times

Evolution of 5G (continued)

- Dramatic increases in speed over the generations:

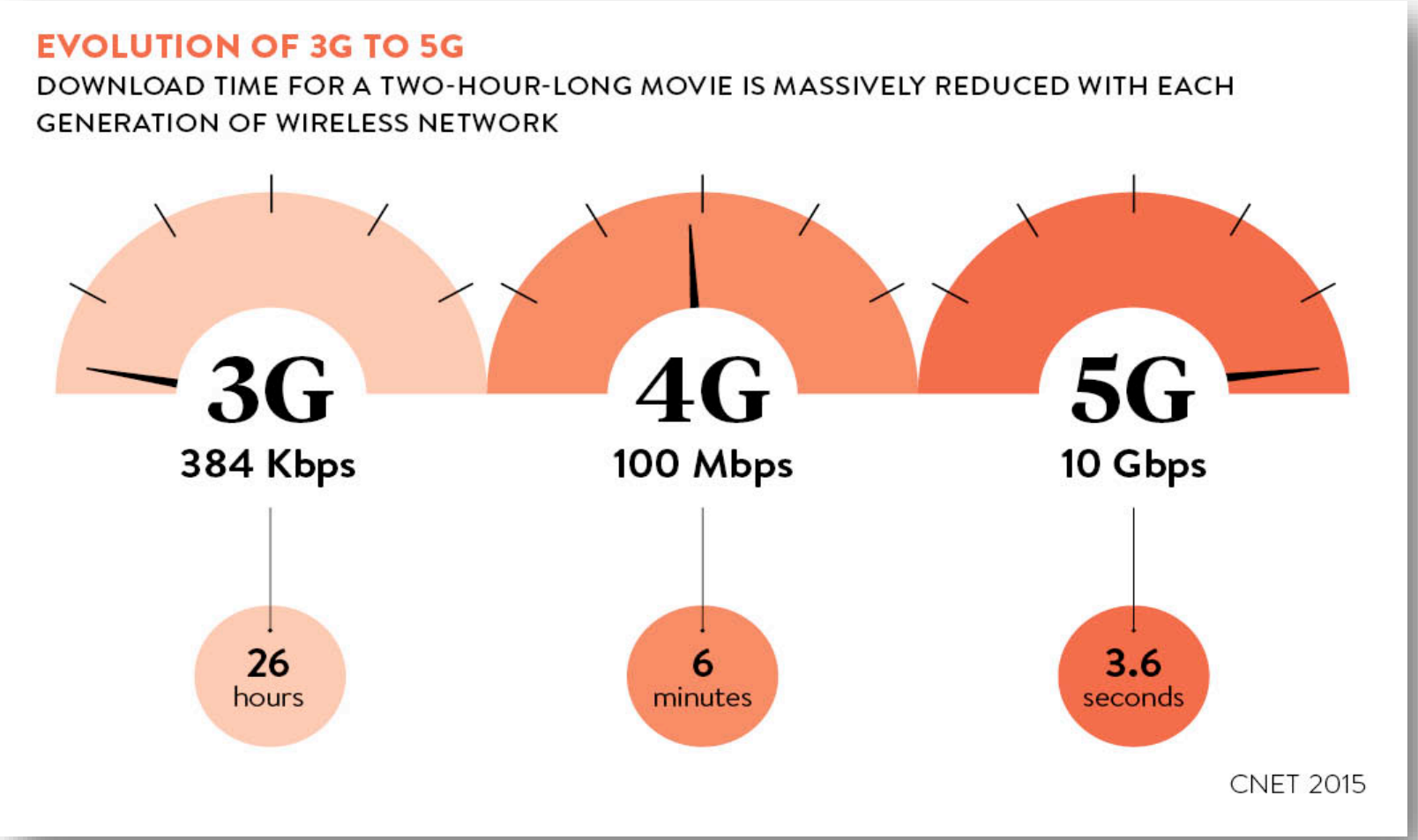


Image source: Raconteur

5G Applications

- Not available to many yet, but when it is…
  - Self-driving cars
    - Autonomous, intelligent, constant transmission of data for safety/navigation
  - Augmented reality
    - Enhanced real-world; interactive overlays
  - Virtual reality
    - Entire world constructed virtually; constant transmission of data for interaction/navigation
  - Increased Internet of Things (IoT)
    - Physical devices and everyday objects with sensors
  - Internet service – replacement for broadband? (Verizon)

Image source: EMF Explained

Image source: Machine Design

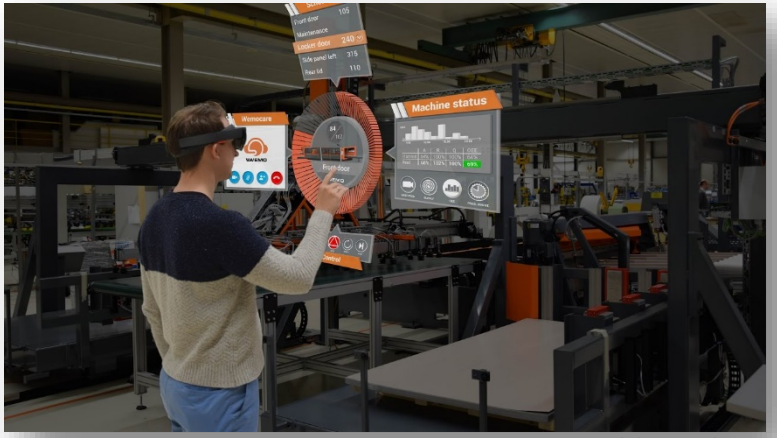


Image source: GOVRPRO

5G implementation

- Maps of existing 5G infrastructure:
  - T-Mobile, AT&T and Verizon are the three big providers
  - Verizon has deployed infrastructure to parts of 35 cities
- 5G phones and other mobile devices are now widely available

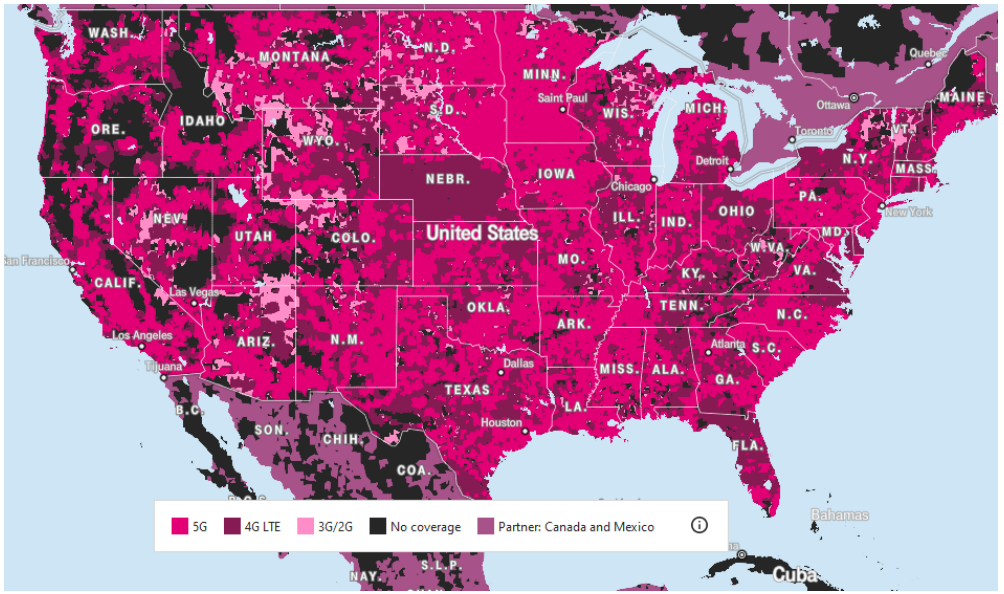


Image source: T-Mobile

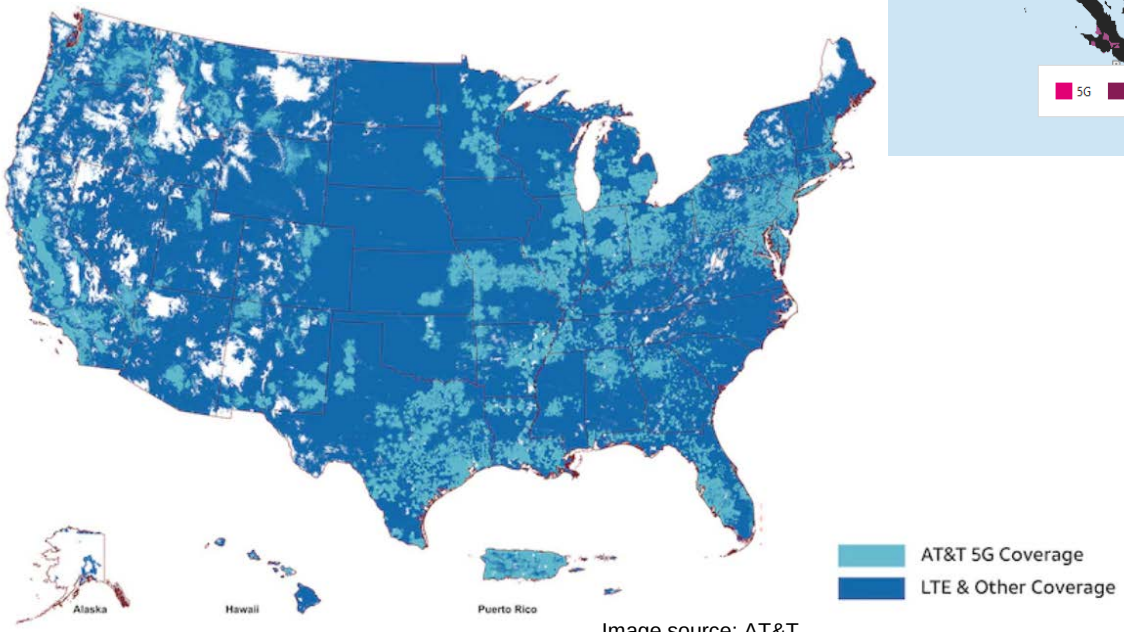


Image source: AT&T

5G and Healthcare

What are the top 5G capabilities that will apply to healthcare?

- Speed
- Capacity/hyperconnectivity
- Low latency
- Massive device connectivity
- Data-driven insights

"Healthcare will benefit from 5G technology from countless aspects; it is basically the field that might experience the most changes." - The Medical Futurist

"…at the Austin Cancer Center, the PET scanner generates extremely large files — up to 1 gigabyte of information per patient per study. When someone needs a remote consultation, it could be difficult to send over such a huge file quickly with the currently existing networks. In the future, that might change for the better and lead to more frequent remote consultations." - The Medical Futurist

What areas of healthcare will be most impacted by 5G capabilities?

- Telehealth/telemedicine
- Remote Patient Monitoring
- Augmented/Virtual Reality
- Large file transfers
- Data analysis

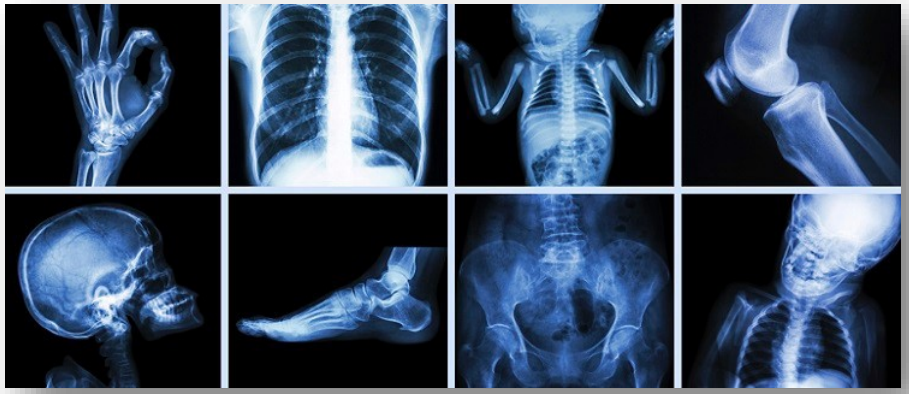


Image courtesy of Medium.com

5G and Healthcare (continued)

- Wearables and Internet of Medical Things (IoMT)
  - Transmit real-time patient health data to doctors (remote patient monitoring)
  - According to Anthem, 86 percent of doctors say they increase patient engagement with their own health
  - Predicted to decrease hospital costs by 16 percent in the next five years
  - The market for IoMT generally, and wearables specifically, is expected to increase significantly – its already happening!

Image source: ResearchGate

5G and Healthcare (continued)

- Telemedicine
  - According to a study by Market Research Future, the telemedicine market is expected to grow at a compound annual growth rate of 16.5 percent from 2017 to 2023
  - 5G technology is expected to enable telemedicine due to the low latency it offers
  - Furthermore, 5G is expected to make telesurgery possible, due to the low latency that it offers as well as its enhancements to robotics, which would then aid surgery

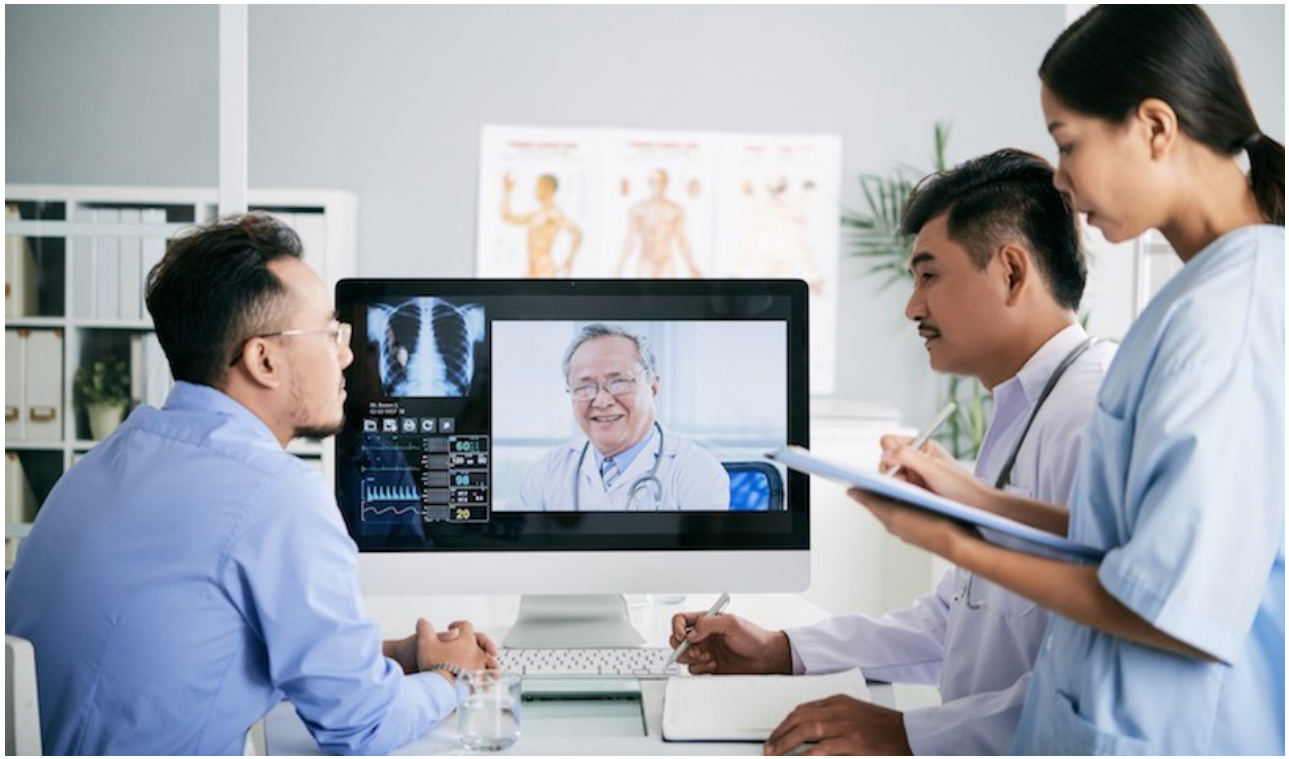


Image source: AT&T Business

5G and Healthcare (continued)

- Other ways 5G will positively impact healthcare:
  - In the future, language translators will be able to video conference with the patient and doctor using models at the network edge with low latency.
  - Robotics autonomously or semi-autonomously performing medical procedures
  - Better leveraging of Artificial Intelligence tools
  - Better access to more specialists for collaboration

Image source: China Daily

5G Exploitation and its Effects

- How can 5G be attacked?
- Generally, attackers can leverage greater seed and lower latency
  - Data Exfiltration
    - Opportunities to access more data exist due to hyperconnectivity
  - Stealthiness
    - Many more connected devices means additional opportunities for security through obscurity
  - Disruption:
    - Dependency on low latency equates to vulnerability to disruption
      - The more you need instant communications the more significant the impact when you don't have them
    - Egregious possibilities exist with telesurgery and other medical procedures performed by robots
    - DoS and DDoS attacks
    - Jamming 5G networks

Image source: The Fast Mode

5G Exploitation and its Effects (continued)

TLP: WHITE

CISA

Cybersecurity and Infrastructure Security Agency
July 2019

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

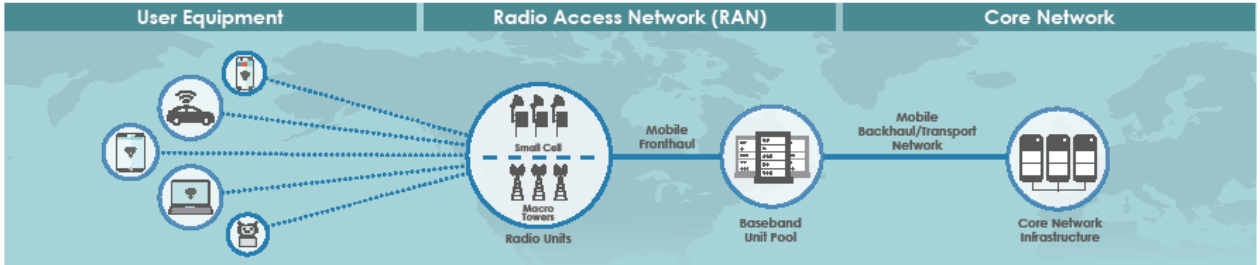
US: United States CH: Chinese EU: European

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



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.

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

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.

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

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.

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

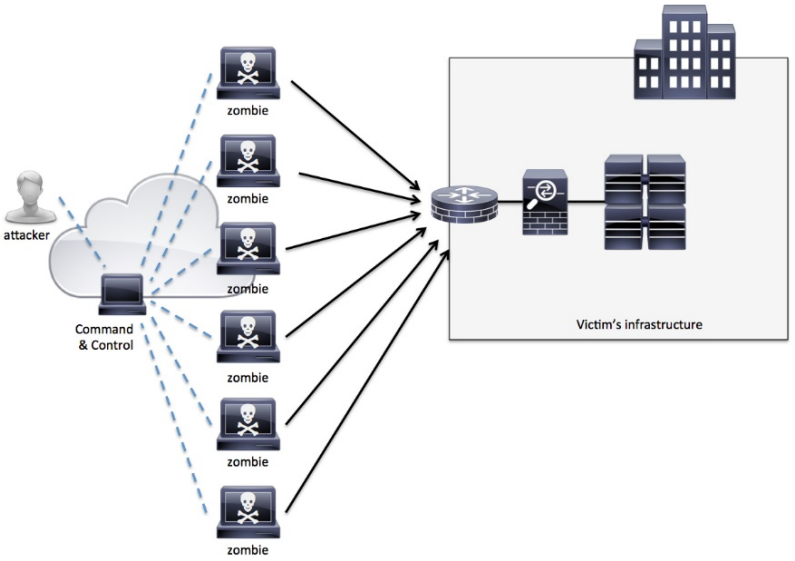
ISSUE: Despite the development of standards designed to encourage interoperability, some companies (including Huawei) build proprietary interfaces into their technologies. This limits customers' abilities to use other equipment, either in addition to or in replacement of Huawei technology.

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.

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/181204_Lewis_5GPrimer_WEB.pdf. Accessed May 2019.

Defending Against 5G Exploitation

Image source: Cisco



- How to defend against 5G threats? Start by asking questions:
  - Who is your 5G provider?
  - What service-level agreements do they offer?
  - What technical controls do they provide?
  - Who will be responsible for ongoing assessment and maintenance of your 5G network?
- Fully update crisis/risk management plans
- Redundancy is critical
  - DDoS protection (zombies ~> botnets)
- Customized 5G networks
  - The one-size fits all approach to security will not work
  - Individual risk assessments become an even more important component of implementing security
- Medical device security becomes very important
  - Access Control!
    - Multi-Factor Authentication
    - Password Managers
  - Updating software/firmware
- Monitoring Network Segments
  - AI/ML will have a role in countering the massive data

The Future

- 6G
  - Academy of Finland funding "6Genesis" - an eight-year research program to conceptualize 6G
  - Summit began in March 2019
  - What is it and why will the world need it?
  - Likely to be significant improvements in:
    - Virtual reality
    - Augmented reality
    - Artificial intelligence
    - Latency
    - Speed
    - ???

Reference Materials

References

5G Brings Benefits, But Also Heralds Fresh Security Threats

https://www.forbes.com/sites/forbesbusinesscouncil/2020/08/11/5g-brings-benefits-but-also-heralds-fresh-security-threats/#797c6cb777f1

5G disinformation: It's time to tell the truth

https://www.euractiv.com/section/5g/opinion/5g-disinformation-its-time-to-tell-the-truth/

The Backbone of 5G Networks: A Guide to Small Cell Technology

https://www.telit.com/blog/5g-networks-guide-to-small-cell-technology/

What to Expect from 5G in Healthcare

https://healthtechmagazine.net/article/2020/02/what-expect-5g-healthcare

CISA: 5G Adoption in the United States

https://www.cisa.gov/5g

CISA: OVERVIEW OF RISKS INTRODUCED BY 5G ADOPTION IN THE UNITED STATES

https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf

CISA: 5G Wireless Networks Market Penetration and Risk Factors

https://www.cisa.gov/sites/default/files/publications/pdm19028_5g_risk_characterizationc_v14_05july2019_0.pdf

DDoS to Loom Large in the 5G Era

https://nsfocusglobal.com/ddos-to-loom-large-in-the-5g-era/

Get ready for upcoming 6G wireless, too

https://www.networkworld.com/article/3285112/get-ready-for-upcoming-6g-wireless-too.html

3GPP Approves Plans to Fast Track 5G NR

- https://www.lightreading.com/mobile/5g/3gpp-approves-plans-to-fast-track-5g-nr/d/d-id/731018

References

5G IoT: Literally a Matter of Life or Death

https://threatpost.com/5g-iot-literally-a-matter-of-life-or-death/145161/

How 5G Will Transform Business

https://www.zdnet.com/topic/how-5g-will-transform-business/

AT&T 5G: Our tests yield the wildest speeds yet

https://www.cnet.com/news/at-t-5g-our-tests-yield-the-wildest-speeds-yet/

5G Networks Spark Concerns For Enterprise Risks

https://threatpost.com/5g-networks-spark-concerns-for-enterprise-risks/145224/

Cutting through the 5G hype: Survey shows telcos' nuanced views

https://www.mckinsey.com/industries/telecommunications/our-insights/cutting-through-the-5g-hype-survey-shows-telcos-nuanced-views

How 5G massive MIMO transforms your mobile experiences

https://www.qualcomm.com/news/onq/2019/06/20/how-5g-massive-mimo-transforms-your-mobile-experiences

Industry Voices—5G has the potential to transform healthcare for rural communities

https://www.fiercehealthcare.com/tech/industry-voices-5g-has-potential-to-transform-healthcare-for-rural-communities

Report: 5G has the potential to revolutionize robotic-assisted surgery, improve availability of healthcare

- https://www.fiercehealthcare.com/tech/report-5g-has-potential-to-revolutionize-robotic-assisted-surgery-and-improve-availability

How the One-Two Punch of 5G, IoT Pushes Edge Computing

https://www.cpomagazine.com/data-privacy/how-the-one-two-punch-of-5g-iot-pushes-edge-computing/

Poland proposes tightening 5G security standards

https://uk.reuters.com/article/us-poland-5g/poland-proposes-tightening-5g-security-standards-idUKKCN1UC1UP

Questions

Upcoming Briefs

- Pulse Secure VPN Vulnerability an Incident Case Study
- CIS 20 Controls and HPH

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Health Sector Cybersecurity Coordination Center (HC3) Background

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Questions

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV