APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

7005 52nd Avenue, College Park, Maryland 20742
A University Affiliated Research Center (UARC)

Broadband Wireless Networks: a National Security Imperative

Why it Matters

T. K. Woodward, tkw@umd.edu

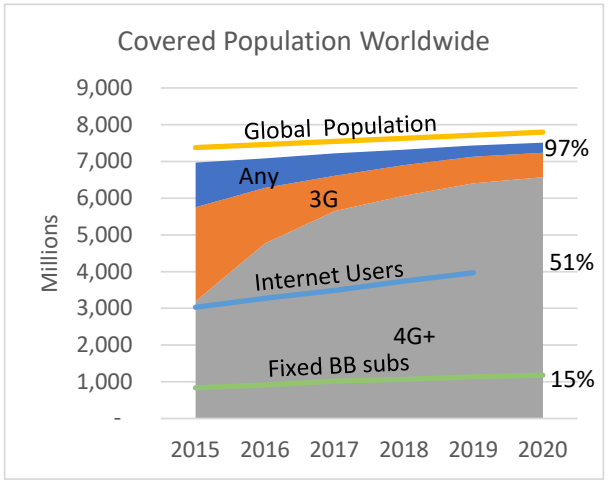

Figure 1. Global mobile coverage, internet users, and fixed broadband subscriptions relative to world population (ITU data, Nov. 2020).

The global spread of mobile wireless technology is one of the great technological achievements of our time. In 2005, after more than a century of stringing cable, fixed telephone subscriptions peaked at just over 1.2 billion, fixed broadband subscriptions worldwide were just under 20% of that (220 million), and the International Telecommunications Union (ITU) did not report mobile broadband subscriptions. By 2020, mobile broadband subscriptions were close to 6 billion and 97% of the world's population was covered by a mobile cellular signal (Figure 1). With multiple satellite ventures planning to deliver broadband from orbit to your smartphone this decade, we can foresee a day that global broadband *population* coverage becomes pervasive global broadband *geographic* coverage.[1,2]

The concerted efforts of a large global industry and massive investments lie behind this remarkable trajectory. For a sense of scale, compare the R&D budgets of leading wireless network equipment companies to components of the U. S. Department of Defense (DoD) budget. Considering both DoD's recent 5G to Next G initiative as well as the whole diversified DARPA budget makes clear that DoD cannot match commercial R&D investments in global mobile network technology. Beyond dollars, this investment represents massive global intellectual resources devoted to the topic, spanning both 3GPP as well as WiFi technologies (i.e. 5G+ technology). [3]

The economic leverage of these networks is vast. For example, as a predominantly tethered application running on desktops and laptops, Facebook (now Meta) had a market capitalization of roughly $40 billion shortly after its 2012 IPO in the early days of the mobile internet. After realignment to a mobile-first emphasis and strategic acquisitions powered huge subscriber growth, its market capitalization flirts with $1 trillion ($T) in 2021. [4] Similar stories exist for many domestic companies including Alphabet (Google), and entirely new ones (Twitter). Overall, massive economic benefits flowed disproportionately to U. S. corporations that built on mobile broadband foundations laid largely by U. S. infrastructure companies.

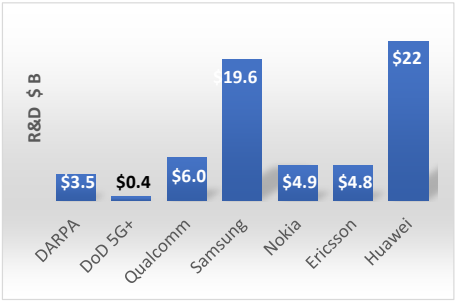

Figure 2. 2020, 2021 R&D Budgets (corporate data, via Statista, Federal Budget data)

[1] D. Oberhaus, Wired, Aug. 3, 2020, "Your phone may soon receive 4G service…From Space," link
[2] X. Lin, et. al. "5G from Space, An overview of 3GPP Non-Terrestrial Networks", Arxiv link
[3] 3rd Generation Partnership Project (3GPP), the collaboration of multiple international standards organizations responsible for mobile cellular communications standards 2G, 3G, 4G, and 5G.
[4] "The Pivotal Tale from Faecbook's History", Brett Hurd, Wharton Magazine, Feb. 20, 2015, https://magazine.wharton.upenn.edu/digital/the-pivotal-tale-from-facebooks-history/

While U.S. software and internet companies dominate their global markets, the story behind the infrastructure that powers them is quite different. In 2005, the market situation for wireless network equipment in the United States (Figure 3) was strikingly different from that for overall network equipment globally in 2021 (Figure 4). The net revenues of U. S. network equipment suppliers from 2011 to 2021 *contracted* from over $10B in 2011 to $4.1B in 2021, even as the overall market grew to over $100 billion.[5,6] Today, the U. S. is devoid of major domestic radio access network (RAN) suppliers. As disturbing as this erosion of the domestic supplier base may be, it is doubly concerning to see it replaced with compromised supply chains from companies under foreign state control, some with close ties to their respective militaries. Networks constructed by these companies have been accused of significant cyber vulnerabilities and back-door access that can expose critical communications data to state or non-state hacking.[7] Supply chain compromise is a key element of asymmetric threats to DoD systems.[8] Compromise of the 5G+ international supply chain is even more pernicious, since many deployment decisions lie beyond the reach of DoD acquisition processes. Given that 3G technology had commercial introduction in about 2002,[9] Figure 1 reminds us that what happens today has consequences that reverberate for decades.

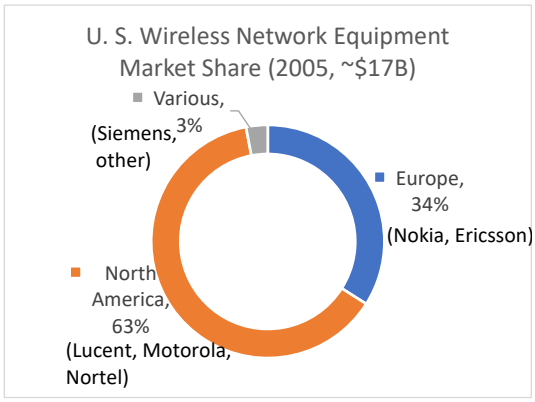

Figure 3. 2005 U. S. Wireless Network Equipment market share by region of origin. (Ovum, 2005)

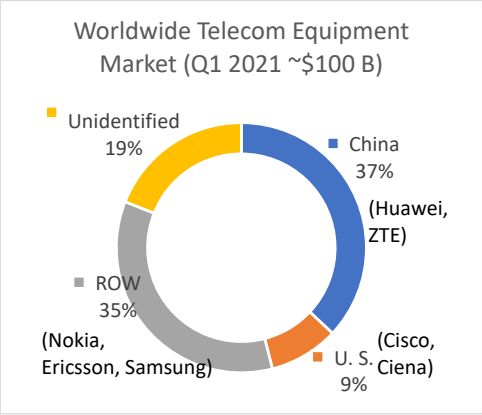

Figure 4. Q1 2021 Global Telecom Equipment market share by country of origin. Aggregate market estimated at ~$100 billion. (Dell'Oro)

Forthcoming mobile networks will penetrate even deeper into our society. 5G+ technology moves beyond traditional best-effort broadband to address new areas in high-reliability and low-latency applications, along with massive sensor integration of the Internet of Things (IoT) used in smart cities and connected homes. Consequent markets in medicine, autonomy, augmented reality, and intelligent environments ranging from our cities to our homes and cars will all experience transformational change. In one of many analyses, the World Economic Forum estimates 5G to contribute $13.2T of economic impact across these markets by 2035.[10] It remains to be seen where the economic benefits of 5G+ innovations will flow; Tik-Tok, Alibaba, Tencent, and Huawei, or Facebook, Google, Microsoft, and Intel? It's safe to say that the situation now is quite different than in 2005, or 2012. At best, the U. S. is conducting a massive, high stakes experiment in economic and national security, and at worst has already ceded control of a critical technology to others.

As with many powerful technologies, 5G+ is now critical to both economic and national security. Beyond the sheer economic impacts described, it has direct relevance to defense missions. The same technology that can deliver cloud-gaming and support self-driving cars can also empower small unit reconnaissance drones, rapid deployment logistics, factory automation, breakthroughs in training and telemedicine, robotic assistants, and mobile command post command and control. As the most heavily networked fighting force in the world, the U. S. has already operationally demonstrated the leverage of broadband networks and smart phone technology with

[5] According to Dell'Oro group, as quoted in link
[6] IBIS World, Telecommunications Networking equipment manufacturing in the US – Market Size 2003 – 2027, link
7 See, for example 'Criticism of Huawei' Wikipedia link and references therein
[8] C. Nissen, et. al., "Deliver Uncompromised", MITRE white paper, Aug. 2018, link
[9] See, for example, Wikipedia, https://en.wikipedia.org/wiki/3G
[10] World Economic Forum, "The Impact of 5G: Creating New Value across Industries and Society", Jan. 2020, Link

the 'remote advise and assist (RAA)' capability that empowered partners to engage and defeat ISIS formations with a far smaller and agile U. S. support footprint than we could conceive of even a few years earlier.[11] In the future, as network capability and coverage continue to expand, DoD will be presented with more opportunities that will be essentially impossible to realize with prior DoD models of full custom networks. At the same time, engagement with commercial technology and networks will present new risks to security, trust, and reliability, as well as threats arising from our adversaries' use of the same technology. Already significant, as 5G+ networks become ever more entwined with great power competitions such as China's Belt and Road initiatives, security issues associated with compromised international network supply chains will grow. Addressing these issues should be at the top of any roadmap of technical challenges for the defense communications enterprise.

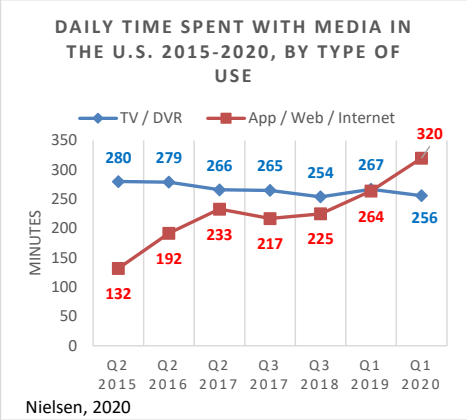

Figure 5. Daily time spent with media, by type (src Nielsen, via Statista, Aug. 2020)

Beyond traditional domains of conflict, broadband networks create an entirely new 'information domain' within which more and more human social interactions transpire, and which define the core mission of organizations like ARLIS (Applied Research Laboratory for Intelligence and Security). Such a 'brave new world' of information, understanding, belief and behavior establish qualitatively new realms for state and non-state competition and conflict far richer than what was previously exploited by historical single-message propaganda states. We now face an engineered cacophony of the multitude to which we are increasingly addicted. Over just the last 3 years we have seen a crossover in the time people in the United States spend with broadband networks (apps, web, and internet on computers, smartphones and tablets) compared to spent watching live or time-shifted television (Figure 5). The same challenges of identity, privacy, trust, and security play out in this environment as in real-world conflict, and they happen all the time. The U. S. Project ARES and related efforts to fight ISIS in the cyber domain, and recent Solarwinds cyberattacks illustrate the double-edged nature of issues that arise.[12,13] All these interactions take place over modern mobile network infrastructure.

The breathtaking scope of broadband wireless networks has taken them into the realm of critical technologies like energy, nuclear, or aerospace. Clearly, now is the time to take action to arrest and reverse troubling trends and engage with 5G+ technology for the benefit of both our national and economic security. Positive steps have been taken with the establishment of the 5G to Next G cross-functional initiative hosted in the DoD and reaching across the government with bipartisan buy-in from Congress and the White House. The initiative has articulated a coherent strategy and is executing on a plan to to deliver it and to change the competitive landscape so that trusted supply chains can lead in the 5G+ era.[14,15]

More must be done to engender both DoD utility as well as a vibrant 5G+ domestic industry. We must also master 5G+ technology in a way that preserves security, privacy, and trust in the use of these networks. History teaches us that once lost, leading economic positions in infrastructure technology are not easily recovered. While opportunities to address the gaps pointed out here are welcome, we must also find ways to change the competitive landscape in the 5G+ industry. Just as networks are fundamentally cooperative, global in scale, and complex in administration, successful 5G+ initiatives need more engagement and cooperation across government and industry than ever before. While there is much to do, recent activity gives cause for optimism that we will marshal the resources and take action to ensure the U. S. remains at the forefront of the 5G+ era.

---

[11] Deane-Peter Baker, Ethics and Information Technology (2019) 21:1–10, link

[12] "How the U. S. Hacked ISIS", D. Temple-Raston, National Public Radio, Sept. 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis

[13] "Inside the Solarwinds cyber exploit", D. Temple Raston, National Public Radio, April 16, 2019, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

[14] Department of Defense DoD 5G Strategy, May 2020 link

[15] Department of Defense DoD 5G Strategy implementation plan, Dec. 2020 link