Written by Dennis Behreandt on December 9, 2019
Published in the December 9, 2019 issue of the New American magazine. Vol. 35, No. 23

Security and Surveillance in a 5G World

The rollout of 5G mobile communications as an upgrade to existing 4G networks promises to deliver a new era in data throughput and bandwidth, enabling new capabilities that will improve economic production, drive job growth, increase prosperity, and enable new, immersive entertainment possibilities. And that's just a few of the many benefits that may be derived from 5G. But just like any technology, 5G can drive negative outcomes in addition to positive ones.

One of the best pro-freedom writers working today recently fielded a question about 5G from one of his readers. Eric Peters reviews cars from a staunchly pro-freedom viewpoint, and he often has useful perspective to share with his readers. Asked what he thought about the dangers of 5G, he replied that his chief concern was its potential impact on our freedoms.

"We're told 5G is harmless — in terms of health — and maybe so," he wrote. "But will it be harmless in terms of our liberty? Our privacy? Our right to be free from ubiquitous monitoring — and control? I have grave doubts about that."

There is already a tremendous, interconnected surveillance regime in place, erected largely on the back of the 9/11 attacks, and revealed most disturbingly by whistleblowers such as William Binney and Edward Snowden. These surveillance regimes, which Binney argues conduct illegal surveillance on all Americans, were built with previous-generation telecommunications and computing technology. With 5G, with advances in solid-state storage, and with continuous advances in cloud computing, algorithmic analysis, and software, near-future surveillance capabilities will dwarf those revealed by the post-9/11 whistleblowers.

When it comes to the surveillance implications of 5G, consider the Internet of Things (IoT), the tech industry's long-desired utopia consisting of every device one owns connected to the Internet and continuously monitored. The world of IoT is one in which every house and car is equipped (i.e., monitored) by an Alexa-like system and in which every possible operational device from door bells (Ring, for example), to televisions, refrigerators, washing machines, door locks, furnaces, air conditioners, and much, much more are wirelessly connected, always sending data back to the cloud reporting on usage, location, viewing habits, and even words spoken in their proximity. Much of this is in place now, but 4G bandwidth limitations are a problem that the increased bandwidth and speed of 5G will eliminate. The all-seeing Eye of Sauron, the surveillance state, will, through this technology, gain the ability to know where everyone is, what everyone is doing, and what everyone is saying at all times, in all places, and in real time.

Span and Depth of Surveillance

Keep in mind, too, that this very near-term future includes an IoT surveillance kit installed in all public places as well — on light poles, at intersections, on public buildings, and more. These will include motion detectors, video cameras, and microphones, capable of transmitting high-definition and even 4K ultra-high-definition imagery, high quality audio and even thermal imagery to the surveillance state. Again, with 5G, this will happen in real time.

This is not speculation — it is something the surveillance state has desired and been working toward for a number of years. As far back as 2012, as Wired reported at the time, then-CIA director David Petraeus openly admitted that the government wanted to watch people through their Internet-connected appliances.

“Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters — all connected to the next-generation internet using abundant, low-cost, and high-power computing,” Petraeus said, “the latter now going to cloud computing, in many areas greater and greater supercomputing, and, ultimately, heading to quantum computing.”

5G is the “next-generation internet” envisioned by Petraeus. As for quantum computing, it’s real and it’s here. Google, for example, has announced its achievement of “quantum supremacy,” the point at which a quantum computer can vastly outperform a “classical” supercomputer, solving problems that classical computers cannot solve in any practical sense.

In October 2019, Google announced in the journal Nature that it had used “a processor with programmable superconducting qubits to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 253 (about 1016).” This processor, dubbed “Sycamore,” takes “about 200 seconds to sample one instance of a quantum circuit a million times — our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years.”

Quantum computing breakthroughs matter for a number of reasons, but in a world of ubiquitous snooping, the most important implication of quantum computing is that it threatens to challenge existing public key encryption systems. These are one of the last remaining defenses against an all-powerful surveillance state, which goes a long way to explaining why the surveillance state is so bent on eradicating the public’s use of encryption.

Security expert Bruce Schneier offers a great description of the power of current encryption technology. “To encrypt a message, we combine it with a key to form ciphertext,” he notes on his website. “Without the key, reversing the process is more difficult. Not just a little more difficult, but astronomically more difficult. Modern encryption algorithms are so fast that they can secure your entire hard drive without any noticeable slowdown, but that encryption can’t be broken before the heat death of the universe.”

Except, possibly, by quantum computers. These, Schneier says, “promise to upend a lot of this.” Nonetheless, Schneier indicated that he remained optimistic about the potential of hardening encryption against quantum computation. “Cryptographers are putting considerable effort into designing … quantum-resistant algorithms,” he noted. Of course, by the same token, Google and others are putting considerable effort into developing quantum computing.

Quantum computing is neither the greatest threat nor the most near-term threat to encryption. That is represented by the surveillance state itself and its ongoing effort to legislatively and otherwise create backdoors in communications systems.

In a recent column, NSA whistleblower Edward Snowden called attention to efforts made by the United States, the U.K., and Australia to “do away with end-to-end encryption,” or E2EE. Increasingly used, Snowden noted, by the likes of Facebook, Google, and Apple, E2EE works with keys held “on the specific devices at the end-points of a communication” such as smart phones. “In short,” Snowden points out, “E2EE enables companies … to protect their users from their scrutiny: by ensuring they no longer hold the keys to our most private conversations, these corporations become less of an all-seeing eye than a blindfolded courier.”

Note that this is in keeping with the spirit of the Fourth Amendment that asserts that the government shall not pry into the personal papers of citizens without a search warrant. Without encryption, bulk data collection means that government snoops (and corporate ones, too) can review private-citizen communications at their leisure. This, they frequently take pains to assure us, is because they need to protect us from bad actors and criminals such as terrorists, organized crime, drug dealers, and money launderers, along with assorted other nebulous threats.

Snowden, however, thinks the motivation to undermine encryption protocols is motivated by other, darker considerations:

The true explanation for why the US, UK and Australian governments want to do away with end-to-end encryption is less about public safety than it is about power: E2EE gives control to individuals and the devices they use to send, receive and encrypt communications, not to the companies and carriers that route them. This, then, would require government surveillance to become more targeted and methodical, rather than indiscriminate and universal.

Interestingly, while the surveillance state wants to undermine privacy protections for individuals, in the rapidly forthcoming 5G world, it remains concerned about its own privacy and security from other nation states, principally China.

This is because China is neck and neck with the West, and arguably even ahead of the West, in developing and deploying 5G infrastructure, both at home in China and in much of the rest of the world.

The chief corporate lever of this advantage is Chinese electronics giant Huawei. Concerns about the company being a non-official part of the Chinese communist government start with company founder Ren Zhengfei, who served nine years in the People’s Liberation Army starting in 1974. The company says this is no big deal. His military service, they say, is just “like many other business leaders in the US and elsewhere” who also served in national military organizations.

But the situation with Huawei is murkier than just the relationship, whatever it might be, of Ren Zhengfei with Beijing. There is also the rather mysterious situation with the company’s ownership. In a report dated April 17, 2019, Professors Christopher Balding of Fulbright University Vietnam and David Weaver of George Washington University Law School point out that Huawei is “100% owned by a holding company, which is in turn approximately 1% owned by Huawei founder Ren Zhengfei and 99% owned by an entity called a ‘trade union committee’ for the holding company.”

While Huawei claims that it is an employee-owned company, Balding and Weaver find that doubtful. "Given the public nature of trade unions in China, if the ownership stake of the trade union committee is genuine," they write, "and if the trade union and its committee function as trade unions generally function in China, then Huawei may be deemed effectively state-owned."

If that's true, then Huawei can be expected to conduct operations in conjunction with Beijing's geo-strategic aims. And since Huawei is one of the top developers and manufacturers of 5G equipment, that means the company could, in fact, build in the backdoors that would allow the communist government of China to spy on anyone — and any nation — that allows Huawei equipment to form part of the 5G system.

Even in our era of extreme political polarization, there seems to be some bipartisan agreement about the threat potentially posed by Huawei.

Republican Senator Marco Rubio (Fla.), for one, is convinced that Huawei is a significant threat via the potential for it to conduct espionage through its 5G technology. "Huawei is a Chinese state-directed telecom company with a singular goal: undermine foreign competition by stealing trade secrets and intellectual property, and through artificially low prices backed by the Chinese government," he told tech news website The Verge. "The US must be vigilant in preventing Chinese state-directed telecoms companies … from undermining and endangering America's 5G networks," he continued. "Future, cutting edge industries like driverless vehicles and the Internet of Things will depend on this critical technology, and an action that threatens our 21st century industries from developing and deploying 5G undoubtedly undermines both our national and economic security."

Across the aisle, Democrat Senator Mark Warner (Va.) indicated to The Verge that he also thought Huawei a security threat. "There is ample evidence to suggest that no major Chinese company is independent of the Chinese government and Communist Party — and Huawei, which China's government and military tout as a 'national champion,' is no exception," Warner said. "Allowing Huawei's inclusion in our 5G infrastructure could seriously jeopardize our national security and put critical supply chains at risk."

In a report published on June 12, 2019, the Congressional Research Service (CRS) also pointed to the national security risk presented by all Chinese telecom firms, including Huawei.

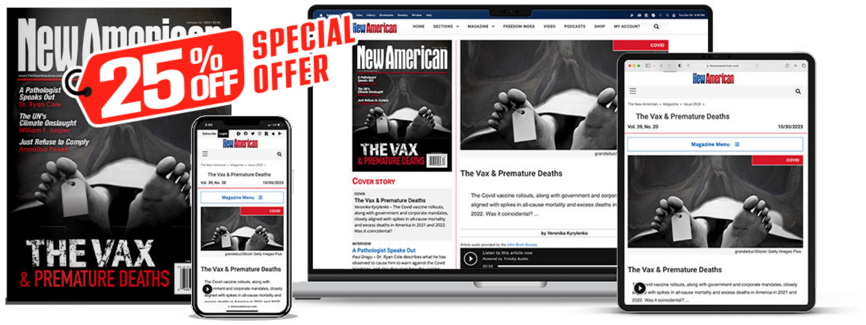
The CRS report pointed out that experts have noted that vulnerabilities in Chinese 5G equipment could be "intentionally introduced for malicious purposes." According to the report, "China's National Intelligence Law, enacted in June 2017, declares that 'any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of.' Some analysts interpret this law as requiring Chinese telecommunications companies to cooperate with intelligence services to include being compelled to install backdoors or provide private data to the government."

Many Opportunities, Many Challenges

It is inevitable that as technology becomes more powerful, more advanced, and more widely dispersed, it will have ever-greater potential benefits and ever-greater potential for disaster. In this, 5G mobile communications technology is in keeping with other technical advances made beginning at the start of the 20th century. Chemistry gave us the ability to make fertilizer out of thin air, allowing for the rapid growth of population without starvation (except for those starvations that were engineered by socialist governments), but it also introduced new dangers. Nuclear power provided vast amounts of energy — both for economic gain and military destruction. The development of computers has allowed the rapid expansion of many industries and spawned entirely new ones that drive the economy, while also enabling increasingly disturbing social trends and the surveillance state. 5G will be no different. It offers to accelerate innovation, speed production, and allow faster and more sophisticated communications while, simultaneously, it supercharges all the bad aspects of the electronics and telecommunications innovations that it builds on.

Photo credit: AP Images

This article originally appeared in the December 9, 2019 print edition of The New American.


25% OFF
SPECIAL OFFER
New American
THE VAX & PREMATURE DEATHS