Introduction
A robust, trustworthy, and stable free market global supply chain for communications equipment is essential to the advancement of high-speed broadband and the applications that drive economic growth. Free and fair enterprise lowers costs for consumers and maximizes innovation. That is why any Made in USA mandates, government interventions, or rent-seeking that artificially advances certain companies, unfairly restricts foreign manufacturers, or otherwise unnecessarily distorts the marketplace should be viewed with skepticism. Unfortunately, the Chinese government’s behavior has cast a harmful shadow of suspicion over the entire global marketplace—especially over Chinese vendors—which requires a comprehensive, vigilant, and fiercely objective oversight response from policymakers in the United States.

A company’s being Chinese-based may not by itself be problematic, and many Chinese firms bring to mind positive experiences for US companies and consumers. But recent national security concerns require increased due diligence from government and industry.

In recent years, Huawei and ZTE’s behaviors confirmed national security concerns, and these vendors are in the process of being excluded from the US market. Service providers must now “rip and replace” existing Huawei and ZTE products with trusted equipment. This saga generated two key lessons. First, a strong association with the Chinese government or military gives a company both the motive and means to sell untrustworthy equipment. Second, Beijing coordinated with these companies to distort the market to China’s strategic advantage. With Chinese government–subsidized prices, Huawei and ZTE unfairly influenced the marketplace against numerous Western communications equipment manufacturers. Meanwhile, Chinese equipment’s vulnerability to data abuse and cyber interference raised national security concerns.
**Current Tools**

Congress has put tools in place to protect the country from compromised telecoms equipment. The most pointed tool is the Secure and Trusted Communications Networks Act of 2019, which authorizes executive branch agencies to designate communications equipment or services that are deemed a threat to US national security or the American people. This includes equipment that routes or redirects user traffic or causes the provider networks to be remotely controlled. Once an entity is designated, the Federal Communications Commission is prohibited under the Secure Equipment Act of 2019 from providing review or authorization for such equipment, effectively eliminating the untrusted equipment from the market. Though most nationwide and midsized service providers did not use such equipment, providers who did are obligated to rip and replace it. The US government will provide subsidies to these smaller providers to compensate for their economic hardship. Since this is a significant burden and expense, the government should reserve this option for extraordinary circumstances such as serious national security threats.

While the 2019 law is a valuable tool, it is not sufficient. The US still needs to develop a fine-tuned, cohesive, logical, and transparent approach for reviewing other threats, such as foreign-backed vendors that benefit from subsidies and other anticompetitive measures. While Washington has so far emphasized service provider networks, many other aspects of communications service equipment are worth reviewing through a similar lens.

**Are Routers Creating Vulnerabilities?**

Hundreds of millions of mini-wireless networks in our country—namely, consumer wireless network devices—are effectively administered by consumers and enterprises. Wireless routers are an integral part of internet connectivity for homes and small businesses, eliminating wired connections and easing internet access. Should Americans be concerned about these networks?

Yes. Routers are vital to the overall chain of internet security.

Don’t just take my word for it: the subject was raised as part of a recent hearing in the House Energy and Commerce Committee.

Bad actors can misuse wireless routers to infect millions of home networks to obtain consumer information and documents, proliferate misinformation, disrupt functionality, or cause other harm. While the underlying internet infrastructure is protected by layers of encryption and other security features in its embedded standards, routers can give malicious actors entry to these systems, potentially affecting service providers, wider networks, and the global internet. Policymakers need to examine whether wireless routers could be China-sponsored hackers’ next entry point into US networks.

While there is nothing inherently insecure about home networking devices, the US should investigate whether Chinese routing vendors have questionable relationships with the Chinese government. A cautious inquiry into the entire Chinese consumer networking device industry by the right entities is appropriate. But the US government should avoid two pitfalls. First, Washington should not needlessly restrict wireless service providers that provide competition to the market and benefits to consumers. Second, the government should not conduct an overbroad review of the totality of the networking community.

Small software and firmware vulnerabilities in consumer and enterprise wireless routers can enable larger abuses, including cybercrime. Cybercrime goes beyond financial theft. It includes exploits like ransomware: taking critical information within an organization hostage and demanding compensation for its return. Cybercriminals can also disrupt personal computers, perpetrate identity theft, commit software piracy to steal corporate or national secrets, derail passenger and freight transportation, cut off energy supplies, and initiate targeted...
bombings. The Federal Bureau of Investigation’s latest Internet Crime Report indicates that complainants filed over 900,000 cyberattack reports worth an estimated $10.3 billion.7 Suffice it to say, in an everything-connected world, minor disruptions have the potential to cause cataclysmic damage.

The Director of National Intelligence (DNI)’s 2023 Annual Threat Assessment of the US Intelligence Community states that “transnational organized ransomware actors continue to improve and execute high-impact ransomware attacks, extorting funds, disrupting critical services, and exposing sensitive data.”8 In few places is this activity more prevalent than in China. The DNI’s report further explains that “China probably currently represents the broadest, most active, and persistent cyber espionage threat to US Government and private-sector networks.”9 Elsewhere in the federal government, in February the US Department of Justice revealed the results of an investigation uncovering more threats from China. It found that China-sponsored hackers used trojan horse malware to infect older-model home routers and attack numerous critical layers of American infrastructure, including electrical grids and water supplies.10 That’s damning stuff.

Most companies that produce wireless network devices have clear reputational—and, therefore, financial—incentives to produce equipment that is less vulnerable. Voluntary cyber-housekeeping practices include disclosure of vulnerabilities, availability of software updates to remedy issues, participation in standards bodies to address security issues, and responsiveness to those who flag vulnerabilities, including government agencies. But that clear picture of good cyber-citizenship should not lull consumers into complacency.

Lessons from Industry Leader TP-Link’s Security Struggles
Consider TP-Link, a leading firm headquartered in Shenzhen, China.11 For the twelfth year in a row, TP-Link was the largest provider of home routers in the world according to industry

analyst reports.12 The company has been able to tap into consumer acceptance of home routers, a burgeoning market that is expected to approach $28 billion worldwide by 2028. But retaining access to the Chinese market—which comprises 60 percent of global demand—incurs certain obligations to the Chinese government.13 Therefore, although TP-Link is a private firm, unlike Huawei and ZTE, murky Chinese investment structures mean that the firm warrants further inquiry.14

US cybersecurity authorities and analysts have documented vulnerabilities from home equipment vendors across the board. But TP-Link products have had more than their fair share of citations.15 Among them:

- In May 2023, the US Cybersecurity and Infrastructure Agency (CISA) noted a known vulnerability to TP-Link’s Archer AX21 router that could be exploited to execute remote code, an exploit likely used in the Mirai botnet.16
- Also in May, US security company Check Point reported that TP-Link routers uploaded with third-party software were vulnerable to firmware attacks. This exploit affected many European foreign affairs officials.17
- Researchers for CyberNews reported in 2021 that the TP-Link’s best-selling Archer C50 router’s firmware contained 24 vulnerabilities, including some that would allow denial of service attacks or grant the attacker network privileges.18

An increased review of select consumer network equipment vendors is important because vulnerable routers—including those made by TP-Link—are in use at government agencies, schools, libraries, enterprises of all types, and private homes. American policymakers should ensure that the home router industry and government have a strong handle on the causes and ramifications of this equipment ecosystem, including TP-Link and all other available routers. It is unclear how prevalent TP-Link’s vulnerabilities are compared to other wireless routers—from China or elsewhere—as there is no definitive comparison or ranking of routers based on security. To ensure
that the US is not caught flat-footed, relevant federal agencies should keep track of TP-Link and other manufacturers’ cybersecurity practices and ownership structure, including any ties to the Chinese government. Certainly, there has been wide bipartisan support in Congress and between administrations for putting other Chinese companies under the microscope.

To be clear, this report makes no accusation that TP-Link has done anything wrong. Likewise, there is no evidence to suggest negligence or maliciousness with regard to past vulnerabilities or weaknesses in TP-Link’s security. Indeed, any suggestion that Washington should mandate US-made routers or ban Chinese-made ones is beyond premature. Moreover, additional voluntary—and especially mandatory—security standards or reporting requirements would be disastrous. And there is no suggestion of statutory changes (including prohibitions) at this time. But given TP-Link’s prime position and wide consumer adoption, it is appropriate to explore relevant questions.

Addressing and preventing network security weaknesses is a serious issue. Vetting firms that seek to sell equipment and services in the United States is in America’s collective interest.

Endnotes


4 The underlying broadband networks—be they cable, wireless, satellite, or fiber—generally employ extensive security features and are not the subject of this paper.


7 Internet Crime Report 2022 (Washington, DC: Federal Bureau of Investigation, 2022), https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. This is an exceptionally conservative figure, as it only covers reported instances, not prevented or unreported attacks.


9 2023 Annual Threat Assessment.

10 See Ken Dilanian, Summer Concepcion, and Kyla Guilfoil, “FBI Director Warns Chinese Hackers Aim to ‘Wreak Havoc’ on US

The company also maintains extensive operations in other parts of the world, including Singapore.


Similarly, wireless routers from manufacturers other than TP-Link have had incidents identified. For instance, see “National Vulnerability Database,” National Institute of Standards and Technology, April 12, 2017, CVE-2017-6884 Detail, https://nvd.nist.gov/vuln/detail/CVE-2017-6884.


About the Author

Michael O’Rielly is a visiting fellow with Hudson Institute’s Center for the Economics of the Internet.

Michael O’Rielly was nominated for a seat on the Federal Communications Commission by President Barack Obama on August 1, 2013 and was confirmed unanimously by the United States Senate on October 29, 2013. He was sworn into office on November 4, 2013. On January 29, 2015, he was sworn into office for a new term, following his re-nomination by the President and confirmation by the United States Senate and served through December 11, 2020.

© 2024 Hudson Institute, Inc. All rights reserved.

About Hudson Institute

Hudson Institute is a research organization promoting American leadership for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, energy, technology, culture, and law.

Hudson seeks to guide policymakers and global leaders in government and business through a robust program of publications, conferences, policy briefings, and recommendations.

Visit www.hudson.org for more information.

Hudson Institute
1201 Pennsylvania Avenue, NW
Fourth Floor
Washington, DC 20004

+1.202.974.2400
info@hudson.org
www.hudson.org