LIBERTY BELL PROJECT

Counter-Intelligence Risks in the IoT Module Supply Chain

The Latent Software Threat of an "Adversary Affiliate-Designed, American-Made" Approach

by Clete Johnson[1]
July 2026

Note on Analytical Scope and Basis: *This paper's analysis focuses narrowly on one specific issue in technology security, namely the capabilities of an adversary government's intelligence services to use commercial technology companies as an operational avenue for future human and technical espionage, sabotage, and "battlefield preparation" for military operations. It examines the scenario of IoT modules, drawing illustrative parallels from two similar scenarios regarding Huawei and Kaspersky Labs. This paper explicitly does not address the numerous other issues that the IoT module supply chain may raise, including U.S.-China policy in general or economic, trade, employment, or industrial policy in particular.*

For this analysis, the paper accepts the U.S. government's public assessment under law, described herein, that China is an adversary government and that the China-based IoT manufacturer Quectel is affiliated with China's military. The analytical opinions in this paper derive from publicly available materials and the author's decades of experience with these issues in the U.S. Army, the Senate Select Committee on Intelligence, the Federal Communications Commission, the Department of Commerce, and in the private sector telecommunications industry.

The paper stipulates that all technology suppliers — whether based in the United States, allied countries, or adversary countries — are vulnerable to sophisticated intelligence operations. It also bases its analysis on the obvious operational reality that adversary intelligence operations are simpler and more likely to succeed if the adversary can leverage a commercial entity with human and technical infrastructure that is familiar to the adversary intelligence service or susceptible to its influence (or both). In simple terms, for an adversary intelligence operation to succeed against a trusted technology supplier, the adversary would have to "break in" to the trusted supplier via multiple clandestine and undiscovered human and/or technical means. In contrast, with a supplier susceptible to adversary government influence, the adversary's intelligence operations can begin, and continue, at a lower level of operational risk and with more active or latent operational avenues available.

Executive Summary of Analytical Findings

- Untrusted IoT modules present a unique risk for U.S. security given China-based manufacturers' market dominance and modules' ubiquity in the connected economy.
- There is severe counter-intelligence risk – the possibility that an intelligence service can steal, influence, manipulate, or otherwise exploit an entity's technology for malicious purposes – in relying on an "adversary affiliate-designed, American-made" approach.
- Manufacturing location is irrelevant to this risk, which comes not from geography but from design authority, firmware control, and post-deployment update pathways – all of which are simpler for a sophisticated adversary intelligence service to influence if it can leverage a commercial entity with familiar human and technical infrastructure.
- The primary risk is espionage, sabotage, and "battlefield preparation" at scale, such as aggregate telemetry espionage, mass remote-disable "kill switches," and coercion.

[1] The Liberty Bell Project is a 501(c)(3) non-profit education and training organization that aims to strengthen the infrastructure of our free society; the organization does not conduct advocacy of any kind.

- Standard mitigations cannot remediate this threat, as code review, signing, and anomaly detection all assume a trustworthy vendor rather than a sophisticated, well-resourced nation-state intelligence service adversary that can conduct a malicious firmware operation years after a device deploys. The U.S. ban on Kaspersky and the United Kingdom's failed evaluation of Huawei confirm this operational reality.

- Mitigations for the "adversary affiliate-designed, American-made" software risk are not effective. Genuine security would require total separation (human and technical) from the adversary design entity or a constant quasi-government counter-intelligence operation.

- The U.S. government has recognized this risk in two distinct regulatory proposals in recent months that seek to define the term "produced by" for purposes of U.S. supply chain restrictions on U.S. government listed entities.

Introduction

IoT modules are the hardware components that allow connected devices to communicate over cellular, Wi-Fi, and other wireless networks. Every connected vehicle, smart meter, medical device, drone, police body camera, and industrial sensor — in fact most IoT devices in the world — depends on a module, and all data flowing into or out of a device passes through it. Without a functioning module, the device is a "brick." As prior papers explained, the United States is playing defense in a cyber war against an aggressive People's Republic of China that is building operational advantage through aggressive global buildout of technology infrastructure, and the central role of IoT modules makes them a high-value target for malicious cyber-supply chain operations by sophisticated adversary intelligence services.[2]

This paper builds on that previous analysis to address a specific arrangement now emerging as a response to U.S. government restrictions: modules that are designed by a U.S.-government-restricted company based in China but manufactured in the United States. Two U.S. government proposed rulemaking processes are examining this complex issue and attempting to draw lines to allow commerce to continue to flow while addressing national security risks from prohibited or restricted entities.[3] The paper argues that this "adversary affiliate[4]-designed, American-made" model does not reduce counter-intelligence concerns, because the risk lies in original design authority, firmware control, and long-term software update pathways available to adversary intelligence operations, not in the physical site of manufacturing and assembly.

---

[2] *See* Clete Johnson and Diane Rinaldo, *Dynamic Competition vs. Predatory Mercantilism: Leveraging Superpower Scale to Build a Trusted Technology Stack*, Liberty Bell Project (November 19, 2025), https://libertybellproject.us/reports/dynamic-competition-vs-predatory-mercantilism/; Clete Johnson, *Spies, Saboteurs, and Access to U.S. Connected Devices: Options to Address the Market Dominance of China-Made IoT Modules*, Liberty Bell Project (July 14, 2025), https://libertybellproject.us/reports/spies-saboteurs-and-access-to-u-s-connected-devices/.

[3] *See* Federal Acquisition Regulatory Council (FAR Council) and Federal Communications Commission (FCC) proposals discussed below, page 11.

[4] For brevity, this paper uses the term "adversary affiliate" as shorthand description of the U.S. government's determination, described herein, that China is an adversary government and that Quectel is an affiliate of China's military.

The cyber-supply chain threat for modules is well established and obvious. A compromised module can conceivably be updated to permit remote access to its host device, enable data exfiltration, allow firmware manipulation, or disable equipment outright.[5] Sophisticated adversary intelligence operations can introduce vulnerabilities at any point in the lifecycle: during design, manufacturing, distribution, or, most importantly, through post-sale, post-deployment firmware updates pushed months or years after the device begins operating. Because modules are the gatekeeper at the boundary between a device and the wireless network, they are in a uniquely privileged position for espionage or sabotage.

At the most elite end of intelligence, sophisticated actors can pursue narrowly targeted operations. Adversary intelligence operators could embed malicious firmware in a specific shipment of devices destined for a particular customer, push tailored updates to a single endpoint, or conduct human-enabled technical operations — "HUMINT-enabled SIGINT" — in which a trained operative places malware on a specific device or set of devices belonging to a person of interest. These operations are real, albeit extremely complex and operationally difficult to conduct successfully; they are not just the subject of Hollywood productions, and they matter for the protection of senior officials, sensitive facilities, and high-value individuals.

However, individualized targeting that would provide thrilling scenes in an action movie is not the most significant counter-intelligence risk; the greatest risk is espionage, sabotage, and "battlefield preparation" at scale.

The Large-Scale Counter-Intelligence Risk

IoT modules from a small number of China-based vendors are now embedded across consumer devices, industrial systems, energy infrastructure, transportation networks, and defense-adjacent supply chains such as drones, body cameras, and fleet vehicles. Two China-based firms — Quectel and Fibocom — account for nearly half of the global IoT module market.[6] The U.S. government has formally determined and stated publicly that the largest of these two companies, Quectel, is affiliated with China's military and therefore, in the U.S. government's view, constitutes a security risk that necessitates a ban on U.S. military reliance on Quectel modules.[7] (Again, for analytical purposes, this paper accepts the U.S. government's assessment of Quectel's relationship with China's military.)

---

[5] *See* Letter from Reps. Mike Gallagher and Raja Krishnamoorthi to FCC Chairwoman Jessica Rosenworcel (Aug. 7, 2023), https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2023-08-07-cellular-iot-modules.pdf.

[6] Numerous other China-based or China-controlled manufacturers make up a large percentage of the half of the global market that Quectel and Fibocom do not occupy. *See, e,g.,* Mark Montgomery & Jack Burnham, *The Risks of Chinese-Produced Cellular Modules*, Foundation for Defense of Democracies (Apr. 15, 2026), https://www.fdd.org/analysis/2026/04/15/the-risks-of-chinese-produced-cellular-modules/.

[7] Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189 (June 10, 2026) (designating, among others, Quectel Wireless Solutions Co., Ltd. as a "Chinese military company" under Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283), https://www.federalregister.gov/documents/2026/06/10/2026-11571/notice-of-availability-of-designation-of-chinese-military-companies.

There are dozens of module manufacturers in the global market that are based outside of China and are not subject to China's government, military, or intelligence influence, but the extraordinary market reach of the U.S. government-listed supplier creates three systemic risks.

First, "big data" espionage and aggregation. Sophisticated adversary intelligence operations could conduct operations to use compromised modules to aggregate module-level visibility into device telemetry — locations, usage patterns, sensor readings, communications metadata — across entire sectors over time, generating strategic intelligence insights even without targeted collection against any particular individual. Because IoT modules maintain persistent remote access for the purpose of routine firmware and software updates, manufacturers are positioned to channel that telemetry to their home jurisdictions; the Foundation for Defense of Democracies (FDD) has warned that this design feature may already mean that ordinary U.S. smart devices are quietly transmitting data to China.[8] The Australian Strategic Policy Institute has separately documented how China-based technology firms use commercial partnerships to channel downstream data back to China-based entities for processing and exploitation.[9]

The intelligence product of such espionage would not be intercepted communications; instead, it would be a big-picture map of how the U.S. economy, infrastructure, and population behave. That map of aggregated data can become a strategic intelligence database — who moves where, when systems run at what level, which facilities depend on which suppliers, etc. — that adversary intelligence services can analyze to identify chokepoints for sabotage, to time economic or military coercion for maximum effect, to target influence and disinformation campaigns to a population's assessed behavior, and in some cases even to track the patterns-of-life and travel of government or corporate personnel. Such metadata need not contain substantive content to be damaging to U.S. national security; the pattern of activity can illuminate U.S. vulnerabilities or adversary opportunities that even intercepted communications cannot.

Second, sabotage at scale. Control over firmware updates means control over device behavior. A manufacturer — or a state actor able to compel a manufacturer — could develop the operational capability of degrading performance, disabling specific functions, or "bricking" devices across thousands or millions of endpoints simultaneously. This is not a speculative scenario: in 2022, agricultural equipment looted from a Ukrainian dealership was remotely disabled by its manufacturer once the machines crossed into Russian-held territory, demonstrating that mass remote-disable capability is a routine feature of modern connected devices.[10] FDD analysts describe adversary-made modules in U.S. infrastructure as potential "time bombs" that could be triggered to disrupt American military mobilization or hold critical economic systems hostage during a crisis.[11]

---

[8] *Supra* note 6, Montgomery and Burnham.

[9] Australian Strategic Policy Institute, *Mapping China's Tech Giants: Supply Chains and the Global Data Collection Ecosystem*, https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem.

[10] Oleksandr Fylyppov & Tim Lister, *Russians plunder $5M farm vehicles from Ukraine — to find they've been remotely disabled*, CNN (May 1, 2022), https://www.cnn.com/2022/05/01/europe/russia-farm-vehicles-ukraine-disabled-melitopol-intl/index.html.

[11] *Supra* note 6, Montgomery and Burnham.

The same capability that makes connected devices serviceable makes them, in adversary hands, the functional equivalent of a "kill switch." Consider, as just one example, modules embedded in emergency-services infrastructure: 911 dispatch systems, ambulance and fire telematics, and the commercial cellular networks on which first-responder communications increasingly depend. An adversary compromise of software update authority could degrade, disrupt, or even disable those devices at the moment a crisis demands their functioning, converting a routine firmware update into a paralyzing attack on public safety response during an emergency. Mobile payment terminals provide similar exposure across the economy: a coordinated firmware update could "brick" point-of-sale modules across a region or an entire retail sector, halting card transactions, fuel sales, and cash access, thereby inflicting broad disruption and public alarm via quiet software updates to largely unknown little widgets — devastating impact without a single physical attack. The threat is similar with almost every type of connected device, including medical devices, energy infrastructure, drones, industrial systems, and others.

Third, supply-chain coercion. Even setting aside cyber operations, dependence on a small set of China-based module suppliers creates a coercive lever analogous to those China has exercised in other strategic sectors, most prominently rare-earth minerals.[12] The ability to throttle, delay, or condition the supply of a critical component becomes a geopolitical instrument. As trusted suppliers exit the market — Switzerland-based u-blox announced its exit in January 2025 — market alternatives narrow and coercive leverage grows. China's recently released 2026–2028 IoT Action Plan sets explicit targets of ten billion terminal connections and more than fifty new standards, and pushes from device proliferation toward control of the underlying networks, platforms, and standards on which the cyber-physical layer will run.[13] China's strategic ambition is not merely to sell modules for commercial purposes; it is to establish technical presence in the architecture in which all modules operate, for strategic purposes.

Adversary Intelligence Capabilities and the Limits of Remediation and Mitigation

According to public reports and statements of its executives, Quectel has sought various ways to maintain its market share in the United States,[14] most recently indicating that it was seeking to leverage a licensing arrangement with a U.S.-based manufacturer in which Quectel modules would be made in the United States under a different name.[15] The U.S.-based company, now led

---

[12] *See, e.g.*, David J. Lynch, *U.S.-China rare earths fight shows risk of economic coercion*, Wash. Post (Oct. 14, 2025), https://www.washingtonpost.com/world/2025/10/14/us-china-rare-earths-economic-coercion.

[13] Matthew Johnson, *New Internet of Things Plan Targets Global Infrastructure*, China Brief, Jamestown Foundation (Apr. 10, 2026), https://jamestown.org/new-internet-of-things-plan-targets-global-infrastructure/.

[14] *See* Quectel Responds to US Select Committee on China, IoT M2M Council (Jan. 9, 2024), https://iotm2mcouncil.org/iot-library/news/iot-newsdesk/quectel-responds-to-us-select-committee-on-china/ (describing Quectel's compliance representations, third-party penetration testing by Finite State, and publication of software bills of materials); *see also* Quectel's Jan. 7, 2025 statement that it would take action to protect its stakeholders and was confident it would be removed from the 1260H List, quoted in Cellular IoT Market Q1 2025: Module Shipments Up 23%, IoT Analytics (July 8, 2025), https://iot-analytics.com/cellular-iot-market-q1-2025-module-shipments-23-percent-us-china-tensions-vendor-impact/.

[15] Quectel, *"PARTNER RELEASE: Eagle Electronics Announces Formation of State-of-the-Art Electronics Manufacturing Facility, $14mm of Funding, and Customer Commitments,"* December 4, 2024, https://www.quectel.com/news-and-pr/partner-release-eagle-electronics-electronics-manufacturing-facility/ (quoting Quectel President and Chief Strategy Officer, Norbert Muhrer: "Some customers need access to cellular modules that are made in the United States. We are excited to partner with

by a former senior Quectel executive,[16] has taken measures to insulate its operations from Quectel influence and secure its Quectel-licensed products, including through the services of a highly respected U.S.-based cybersecurity company.[17] However, this paper argues that it would be extraordinarily difficult —and, as a practical matter, altogether impossible — for an "adversary affiliate-designed, American-made" approach to mitigate the counter-intelligence risks identified by the U.S. government in the relationship between Quectel and China's military.

To be explicitly clear, this assessment does not question the integrity or intent of any individual employed by either Quectel or the U.S. manufacturer; instead, it rests on three factors: (1) the nature of China's aggressive and sophisticated intelligence capabilities, (2) the laws that can compel companies subject to China's jurisdiction,[18] and (3) the U.S. government's assessment of Quectel's relationship with China's military. Beneficent intent of personnel and sophisticated security measures employed to address the threat are necessary for security in any connected device scenario, including among trusted suppliers, but not nearly sufficient to secure future software in the context of an acknowledged adversary affiliated entity.

Domestic U.S. assembly of adversary affiliated connected devices is not a security solution; instead, it is the modern equivalent of accepting an acknowledged Trojan horse, in the hopes that known and unknown security threats can be addressed both presently and in perpetuity. The author is not aware of any certification or testing regime capable of resolving this threat, because it does not necessarily derive from a defect present in the module today. Instead, the threat is latent and derives from the future prospect of a firmware update, configuration change, or selectively delivered operation, via human or technical actions that may not even be presently planned and may not begin until years after deployment. Modules that pass every security test on the day they ship can be influenced through future software activity.

In this context, consider that the engineers, firmware teams, update managers, and corporate leadership on both the China-based and U.S.-based sides of the operation would actually be the witting or unwitting practical delivery mechanism through which state pressure or intelligence objectives can be exercised. Again, under Chinese law, Chinese entities and personnel are obligated to cooperate with state intelligence requests, and moreover China's intelligence services are elite, highly skilled, and aggressive. Their U.S.-based commercial counterparts, however expertly vigilant and well-intentioned, cannot possibly detect all types of nefarious,

---

Eagle Electronics to be able to offer customers the option to procure U.S.-made and cyber-secure modules and we're thrilled to be part of bringing production jobs back to the U.S."). Mr. Muhrer has since left his senior executive position at Quectel and is now the CEO of the U.S.-based manufacturer.

[16] Eagle Wireless, Leadership, https://www.eaglewireless.com/leadership/.

[17] *See* Press Release, *Eagle Electronics Announces Formation of State-of-the-Art Electronics Manufacturing Facility, $14mm of Funding, and Customer Commitments,* Eagle Electronics (Dec. 4, 2024), https://www.prnewswire.com/news-releases/eagle-electronics-announces-formation-of-state-of-the-art-electronics-manufacturing-facility-14mm-of-funding-and-customer-commitments-302321711.html (describing the company's partnership with Finite State to build, compile, and audit all device firmware domestically, and the appointment to its board of the former head of the CIA's Directorate of Science & Technology).

[18] *See, e.g.,* China Mobile International (USA) Inc., Memorandum Opinion and Order, 34 F.C.C. Rcd. 3361, ¶ 17 (2019) (stating that "Chinese law requires citizens and organizations, including state-owned enterprises, to cooperate, assist, and support Chinese intelligence efforts wherever they are in the world," and quoting China's National Intelligence Law: "An organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law…").

clandestine intelligence cooperation that takes the form of ostensibly ordinary communication or collaboration about code or a routine firmware push. This risk is of course present for any device manufacturer; the difference in this scenario, with a U.S. government-listed company, is the assessed nature of that company's close relationship with China's government. As illustrated by the United Kingdom's failed attempt to achieve this goal for deployment of Huawei discussed below, the depth and sophistication of security measures ultimately do not matter. Instead, the human and technical infrastructure of the untrusted software apparatus is the decisive factor.

Indeed, one might argue that this risk can be managed through a robust portfolio of standard mitigations such as hardware and software bills of materials, independent third-party code review, cryptographic firmware signing, network-level anomaly detection, vendor security attestations, and contractual restrictions on the source of personnel and code. Each of these is valuable, and each is part of any serious cyber-supply chain hygiene program. But none of them alone, nor all of them together, addresses the central problem of a future sophisticated intelligence operation directed by China's government. Bills of materials describe what is in a module today, not what will be pushed to it in years to come. Code review can examine the firmware shipping with the device, but a module under active vendor support may receive dozens of firmware updates over its operational life. Each of those updates would itself need to be independently reviewed — line by line, by analysts cleared to evaluate adversary tradecraft — before being permitted onto a fielded device, all with no mistakes.

Regardless of the intent, dedication, or security expertise of the U.S. manufacturer and the cybersecurity services vetting the adversary module, the operational mismatch between offensive adversary nation-state intelligence services and commercial counter-intelligence defense in such a scenario is simply overwhelming. Put bluntly, no commercial vendor, and few if any government programs, could perform the depth of review on every routine update necessary to address the ever-present risk inherent in a company whose engineers operate under legal compulsion from a deeply resourced and sophisticated adversary intelligence service.

Standard risk mitigation assumes that the vendor is trying to be trustworthy and that the question is whether some defect or malicious operation has slipped through. It does not address the case in which an adversary intelligence service could at some future moment undertake a clandestine operation to influence the vendor, or the engineers writing the vendor's firmware, to ship code that compromises the device. Against that adversary threat model, vetting future firmware updates is not just difficult; it is fundamentally impossible.

"Sleeper Software" Risk and the Kaspersky and Huawei Examples

The U.S. government has already reached this conclusion in an analogous context. In June 2024, the Commerce Department's Bureau of Industry and Security issued a Final Determination prohibiting Kaspersky Lab from providing antivirus and cybersecurity software to U.S. persons. The Determination did not rest on a finding that any specific Kaspersky product contained a backdoor today. It was based on the reality that Kaspersky was subject to the jurisdiction of the Russian government, that its software maintained privileged administrative access to U.S.

systems, that it possessed the ability to push updates capable of installing malicious code or selectively withholding protections, and that this combination of factors could not be mitigated.[19]

This logic pertains directly to adversary modules. Like Kaspersky software, modules sit at a privileged position inside the host system; like Kaspersky software, they are designed to receive routine updates that could be influenced by operatives in a foreign adversary jurisdiction; like Kaspersky software, commercial personnel subject to influence or legal compulsion by the adversary government have multiple avenues to influence the software. That combination justified a categorical prohibition for Russian antivirus software, and it justifies the same scrutiny for adversary affiliate modules — regardless of where the physical module is manufactured.

Consider also the case of Huawei in the United Kingdom, the most extensive real-world test ever for a sophisticated intelligence service trying to vet an adversary affiliate's software well enough to make its deployment secure. In 2010, the UK government and Huawei jointly established the Huawei Cyber Security Evaluation Centre (HCSEC), an extraordinary and unprecedented venture in which Huawei funded a facility with staff of UK nationals holding national security clearances, under the operational oversight of the UK's Government Communications Headquarters (GCHQ), the UK's signals intelligence agency that is the equivalent of the U.S. National Security Agency. HCSEC had source-code access to the Huawei equipment proposed for deployment in UK communications networks, and an oversight board chaired by the head of GCHQ's public arm reported annually to the UK government's National Security Adviser on whether the risks of Huawei's continued presence could be adequately managed.

In short, the answer was no. This effort failed. The Oversight Board's 2018 annual report concluded that it could provide only limited assurance that long-term national security risks from Huawei equipment in UK networks could be sufficiently mitigated, citing serious technical and supply chain process defects in Huawei's software engineering processes.[20] The 2019 report went further, identifying "further significant technical issues" in Huawei's engineering processes and finding that Huawei had made no material progress in remediating the problems identified in 2018 and the assessment was that HCSEC's work had revealed systematic defects in Huawei's software engineering and cyber security competence.[21] In July 2020, the UK government concluded that the risk could not be managed and, in the context of U.S. action against Huawei, ordered Huawei equipment removed from UK 5G networks by the end of 2027.[22]

---

[19] Final Determination Prohibiting AO Kaspersky Lab's Provision of Cybersecurity and Anti-Virus Software in the United States, 89 Fed. Reg. 52424 (June 24, 2024); *see also* U.S. Dep't of Commerce, Bureau of Industry and Security, *Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers* (June 20, 2024), https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-us-customers.

[20] Huawei Cyber Sec. Evaluation Ctr. (HCSEC) Oversight Bd., Annual Report 2018: A Report to the National Security Adviser of the United Kingdom (July 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf.

[21] 2019 HCSEC Report, *supra* note 20.

[22] *See* Press Release, Dep't for Digit., Culture, Media & Sport & Nat'l Cyber Sec. Ctr., *Huawei to Be Removed from UK 5G Networks by 2027* (July 14, 2020); *Telecommunications Infrastructure*, HC Deb (July 14, 2020) (statement of Oliver Dowden, Sec'y of State for Digit., Culture, Media & Sport).

To be clear, HCSEC was not an ordinary commercial code review; indeed, it was not simply an extraordinarily rigorous code review. It was a singularly unique initiative; it was purposeful, government-organized, elite intelligence agency-supervised, with cleared government personnel, source-code access, and a decade of accumulated tradecraft directed at one single adversary affiliate. It is the most significant effort ever attempted to prove the proposition that a U.S.-allied country can deploy an adversary affiliate's equipment securely so long as it builds a rigorous evaluation regime around it. The judgment of the intelligence service running that regime was that the approach could not work, but not because Huawei's engineers had been caught planting "backdoors" — instead, the initiative failed because the combination of opaque software practices, vendor-controlled update pathways, and the impossibility of inspecting every future software update simply rendered assurance unattainable.

If GCHQ-supervised source-code review of Huawei's equipment cannot produce sufficient security assurance, it should be manifestly clear that no level of commercial vetting of firmware updates from an adversary affiliate module manufacturer can do so.

Conclusion: Irremediable Risks and Considerations for the U.S. Government

This paper argues that standard mitigation is inadequate to address the counter-intelligence risk of adversary affiliate modules, and there are only two paths to genuine security with the "adversary affiliate-designed, American-made" arrangement. Neither is conceivably realistic.

The first possible security solution is total, hermetic human and technical separation from the adversary affiliate design entity. This would require far more than relocating assembly. It would require severing all human and technical design collaboration, firmware development authority, source-code access, update infrastructure, and technical support pathways; establishing independent control over firmware signing keys, update servers, and lifecycle management; and permanently insulating U.S. operations from shared engineering teams, vendor maintenance channels, and remote diagnostic capabilities. Each of these types of human and technical relationships constitutes a path for an offensive adversary intelligence operation. In practice, creating this total separation would mean altogether rebuilding the entire software and governance stack and replacing the adversary affiliate design authority. A firm that genuinely accomplished this would no longer be operating under the adversary affiliate design model at all; it would be a completely different company with no human or technical ties to the U.S. government-listed China-based company.

The second possible security solution is to accept the counter-intelligence risks of the human and technical connections and compensate for them by operating as a de facto counter-intelligence organization. That posture would entail continuous monitoring of firmware behavior, independent code review of every update, anomaly detection at scale across deployed devices, personnel vetting on both sides of the relationship, supply-chain auditing, and ongoing threat modeling against state-level adversaries. It would require anticipating not only technical exploits but also clandestine operations or legal compulsion of foreign personnel, insider risk, and the slow accumulation of geopolitical leverage. This is the work of a nation-state intelligence service, not a module manufacturer. For commercial companies competing on thin margins and rapid production cycles, it is not conceivably feasible.

In short, the "adversary affiliate-designed, American-made" arrangement offers the appearance of security — a domestic supplier and a U.S. address on the box — without addressing the substance of the threat identified by the U.S. government. It may be possible that the significant technical advances underway through AI and cloud innovation will ultimately provide security solutions via well-resourced, independent, trusted intermediaries focused on the variable that matters: the malleability of software.[23] However, at present the author is not aware of realistic solutions that could meaningfully address the counter-intelligence risks articulated by the U.S. government as posed by Quectel's "adversary affiliate-designed, American-made" manufacturing approach.

What can the U.S. government do to protect against this risk? There are numerous tools, both longstanding and newer, that the government can bring to bear to address these challenges specific to listed adversary affiliate entities. Through interagency efforts such as the Committee on Foreign Investment in the United States (CFIUS), Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (also known as "Team Telecom"), the Department of Commerce's Office of Information and Communications Technology and Services (OICTS) in the Bureau of Industry and Security, and the FCC's administration of Covered List authorities under the Secure Networks Act and Secure Equipment Act, government agencies have long-established processes, significant resources, and fundamental governance responsibilities to investigate, condition, or prohibit suppliers that are subject to the ownership or control of a foreign adversary such as China, Russia, or Iran.[24]

To use these tools effectively and reduce unnecessary burdens on supply chains, these efforts should be (1) tied to specific threats posed by an adversary's ability to exploit a technology or its components, (2) grounded in formal processes with transparent criteria and rules; and (3) provide practical paths for compliance and durable predictability to market stakeholders.

When leveraging these tools to address modules specifically, two key themes should guide policymakers. First, the U.S. government should target the specific counter-intelligence risks in question. Policymakers and procurement officers evaluating module suppliers' security should treat assembly location as a near-irrelevant variable. The questions that matter pertain to the adversary intelligence service's operational reach: who designs the module, who controls or influences its firmware, who can push or influence updates to it after it is fielded, and under whose legal jurisdiction those parties operate. Until those questions can be answered in favor of trusted parties (including allies), domestic manufacturing will not address the counter-intelligence concerns.

---

[23] *See, e.g.,* Lauren Forristal & Amanda Silberling, *Here's What You Should Know About the US TikTok Deal*, TechCrunch (Jan. 23, 2026), https://techcrunch.com/2026/01/23/heres-whats-you-should-know-about-the-us-tiktok-deal/ (describing the creative approach through which Oracle is providing the U.S. government security assurance, in a non-manufacturing setting, regarding TikTok's U.S. operations).

[24] 15 C.F.R. § 791.4(a) (2026); Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909 (Jan. 19, 2021) (determining that China, Cuba, Iran, North Korea, Russia, and the Maduro Regime of Venezuela are "foreign adversaries").

The U.S. government has begun to address this reality. On June 23, 2026, the Federal Acquisition Regulatory Council (FAR Council) published in the Federal Register a proposed rule that would amend the Federal Acquisition Regulation (FAR) as part of the "Revolutionary FAR Overhaul."[25] The proposed rule would clarify an ambiguity in the definition of "covered telecommunications equipment or services." For purposes of determining whether equipment is "produced by" a listed entity, "produced" would mean manufactured, designed, developed, or based on licensed intellectual property from the listed entity. The prohibition would not be limited to equipment physically assembled or manufactured by these listed entities. Equipment could potentially be considered "produced by" a listed entity if that entity manufactured it, designed it, developed it, or licensed the intellectual property underlying it.

Similarly, on July 22, 2026, the FCC adopted a proposed rulemaking on this matter, seeking comment on whether the FCC should codify a definition of "produced by" to mean an "entity exercises substantial responsibility for, or control over, any major stage of the process by which the device comes into existence, including the design, manufacturing, assembly, or development of the device."[26] This proposed definition would also note that "[a] device may be 'produced by' more than one entity."

Taken together, these two different but parallel U.S. government proposals constitute a significant step toward addressing this counter-intelligence risk. Recognizing that a device "produced by" an adversary listed entity — and the counter-intelligence risk associated with that production — has to do with design, development, and control, rather than simply the geographic location of manufacturing, is the beginning of a sound policy to address the counter-intelligence risks of China-designed modules.

Second and perhaps most importantly, the U.S. government should build its policy approach around promoting trusted suppliers. As noted above, there are dozens of module manufacturers in the global market that are based outside of China and other U.S. adversaries, are not subject to adversaries' government, military, or intelligence influence, and have therefore not been designated on any U.S. government restriction or prohibition list. The policy possibilities for promoting these trusted suppliers are far beyond the scope of this paper, but suffice it to say that manufacturers that are not based in or subject to the influence of U.S. adversary governments should be producing the modules that connect American society and critical infrastructure.

U.S. government policy should build on that trust. American security depends on it.

---

[25] Federal Acquisition Regulation: Revolutionary Federal Acquisition Regulation Overhaul; Parts 1, 2, 4, 33, 39, 40, 52, and 53, 91 Fed. Reg. 37550 (proposed June 23, 2026) (FAR Case 2026-001), https://www.federalregister.gov/documents/2026/06/23/2026-12559/federal-acquisition-regulation-revolutionary-federal-acquisition-regulation-overhaul-parts-1-2-4-33.

[26] Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, ET Docket No. 21-232, Third Report and Order and Third Further Notice of Proposed Rulemaking, FCC 26-50, ¶ 134 (adopted July 22, 2026).