



## Karl Lee Network Procures Controlled Materials for Iran's Ballistic Missile Program

By Victoria Cheng

October 24, 2024

### Key Takeaways

- Xiangjiang Qiao (Joe Hansen), an associate of Karl Lee (Lee Fangwei), was indicted in 2023 for evading U.S. sanctions on Iran and violating money laundering laws to procure isostatic graphite and other advanced materials for Iran's ballistic missile program.
- While the end users are unspecified in the indictment, the Iranian entities involved are undoubtedly the Islamic Revolutionary Guard Corps (IRGC) and/or the Aerospace Industries Organization (AIO), which lead Iran's ballistic missile program.
- Iranian missile development is of particular concern considering their potential to be used as nuclear warhead delivery vehicles and more immediately to strike targets in the Middle East.
- Qiao used front companies and exploited the U.S. financial system to bypass sanctions against Sinotech Dalian, a company where Qiao was an employee, to acquire the materials as part of Iranian missile procurement efforts.
- This scheme is part of a larger procurement network, led by Karl Lee, involved in obtaining equipment and technology for Iran's missile program.
- Recommendations include more routine audits of entities linked to sanctioned individuals and companies and enhanced monitoring of international wire transfers by financial institutions to prevent future sanctions evasion.

### Overview

In 2023, Xiangjiang Qiao, also known as Joe Hansen, was indicted by the U.S. Southern District of New York on multiple charges, including sanctions evasion and money laundering. The defendant is charged with his involvement in an illicit procurement scheme to supply advanced materials to Iran's ballistic missile program. While the specific end users are not explicitly stated in the indictment, the Iranian entities involved are undoubtedly the Islamic Revolutionary Guard Corps (IRGC) and/or the Aerospace Industries Organization (AIO), which lead Iran's ballistic missile program. Qiao, an employee of the Chinese company Sinotech

Dalian Carbon and Graphite Manufacturing Corporation (hereafter, Sinotech Dalian), exploited the U.S. financial system to procure isostatic graphite for use in Iran. This material is an ultra-fine grain that is used in the “manufacture of rocket nozzles and reentry vehicle nose tips in intercontinental ballistic missiles.”<sup>1</sup> Given these potential uses of isostatic graphite, “certain graphites and isostatic presses are controlled under Category II of the Missile Technology Control Regime (MTCR).”<sup>2</sup>

In 2014, Sinotech Dalian was sanctioned by the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC) for its involvement in aiding Iran in procuring materials for its ballistic missile program, and the company was added to OFAC’s Specially Designated Nationals and Blocked Persons (SDN) list.<sup>3</sup> Being on the SDN list barred Sinotech Dalian from using the U.S. financial system to conduct transactions without OFAC’s explicit authorization. Additionally, Sinotech Dalian was identified as part of a network of Chinese companies managed by Li Fangwei, also known as Karl Lee, who is recognized as an associate of Qiao. Fangwei himself was charged in 2014 for violating U.S. sanctions by procuring materials such as “gyroscopes, accelerometers, graphite cylinders, ultra-high strength steel and high-grade aluminum alloy” for Iran’s missile program.<sup>4</sup>

Qiao’s activities are believed to be part of a broader network involved in procuring materials for Iran’s ballistic missile program. Iranian development of ballistic missiles is of particular concern considering their potential as nuclear warhead delivery vehicles as well as their potential use against American allies in the Middle East. Iranian missiles, such as the Shahab-3 medium-range ballistic missile, based on North Korea’s Nodong-1, and the Khorramshahr medium-range ballistic missile, are recognized as being capable of carrying nuclear payloads. The Shahab-3 and the Khorramshahr have operational ranges between 1,000 to 2,000 kilometers, placing Israel well within their striking distance. The international community has long recognized Iran’s growing missile capabilities, and the threat of their use as nuclear delivery systems. United Nations Security Council Resolution 2231 called on Iran to “not undertake any activity related to ballistic missiles designed to be capable of delivering nuclear weapons” for a period of 8 years.<sup>5</sup> Despite these restrictions, Iran continued to develop nuclear-weapons-capable missiles during the embargo. Those UN restrictions expired in 2023. Qiao, Fangwei, and the Chinese network involved in procuring materials for Iran’s ballistic missile program demonstrate that Iran is likely to continue developing its nuclear-capable missiles.

---

<sup>1</sup> “Chinese National Charged For Conspiring to Provide Materials for the Production of Ballistic Missiles To Iran In Violation of U.S. Sanctions,” U.S. Attorney’s Office, Southern District of New York, May 16, 2023, <https://www.justice.gov/usao-sdny/pr/chinese-national-charged-conspiring-provide-materials-production-ballistic-missiles#:~:text=Isostatic%20graphite%20is%20a%20type,tips%20in%20intercontinental%20ballistic%20missiles.>

<sup>2</sup> “Karl Lee’s Network Lives On,” Iran Watch, July 25, 2023, <https://www.iranwatch.org/our-publications/international-enforcement-actions/karl-lees-network-lives.>

<sup>3</sup> Specially Designated Nationals and Blocked Persons List, <https://sanctionssearch.ofac.treas.gov/Details.aspx?id=16852.>

<sup>4</sup> “Karl Lee’s Network Lives On.”

<sup>5</sup> “Table of Iran’s Missile Arsenal,” Iran Watch, February 22, 2024, <https://www.iranwatch.org/our-publications/weapon-program-background-report/table-irans-missile-arsenal.>

China also is complicit in aiding and abetting Iran's illicit procurement of materials for its ballistic missile program. China has repeatedly illustrated its willingness to violate U.S. law in its role in helping other nations to procure illicit materials that could be used for weapons of mass destruction. This is evident in the case of Qiao and the broader Karl Lee network; China's response to this issue has been slow, both in prosecuting or extraditing Karl Lee and his associates, as well as in curbing the network's ability to operate within China.

In his role in the scheme to procure isostatic graphite for Iran's missile program, Qiao is charged with violating U.S. sanctions, conspiring to commit bank fraud, and money laundering. These charges stem from Qiao's violation of the International Emergency Economic Powers Act (IEEPA), Executive Orders 12957, 12959 and 13059, and the WMD Proliferators Sanctions Regulations. Under the IEEPA and the Executive Orders, a comprehensive trade and financial embargo was imposed on Iran, and the Iranian Transactions and Sanctions Regulations (ITSR) were created to prohibit "the exportation, reexportation, sale, or supply, directly or indirectly, of any goods, technology, or services from the United States" to Iran.<sup>6</sup> The WMD Proliferations Sanctions Regulations prohibit "transactions or dealings by any U.S. person or within the United States with individuals and entities that have been placed on the SDN list, except as authorized or licensed by OFAC."<sup>7</sup> By conducting transactions through the U.S. financial system for Sinotech Dalian, a sanctioned company, without OFAC's approval, Qiao violated these regulations, leading to his indictment.

## The Scheme

Between March 2019 and September 2022, Xiangjiang Qiao exploited the U.S. financial system to facilitate transactions for Sinotech Dalian, an OFAC sanctioned company on the SDN list, as part of an effort to procure isostatic graphite for Iran's ballistic missile program. Due to Sinotech Dalian's restricted status, Qiao took steps to obscure the company's involvement by establishing a bank account under the name of a front company, Lexing International Trade Co. This was done to bypass OFAC sanctions, as Sinotech Dalian was prohibited from conducting any transactions using the United States financial system without prior authorization.

On September 1, 2020, Qiao initiated a wire transfer of approximately \$6,255 from a bank account in the Southern District of New York to an account in China held by Lexing International Trade Co. Another transfer occurred on September 23, 2021, when Qiao wired \$8,840 from the same New York based account to Lexing International Trade Co. It was later discovered that Lexing International Trade Co. was a front company created to mask Sinotech Dalian's procurement activities, allowing the sanctioned company to circumvent OFAC regulations and secretly acquire materials for Iran's missile procurement.

---

<sup>6</sup> United States v. Xiangjiang Qiao (United States District Court Southern District of New York, May 16, 2023), 3.

<sup>7</sup> United States v. Xiangjiang Qiao, 4.

## Lessons and Recommendations

The case of Xiangjiang Qiao and his ability to exploit the U.S. financial system to conduct transactions for the sanctioned company Sinotech Dalian highlights additional vulnerabilities in detecting and preventing illicit finance. To address these gaps, the following recommendations should be adopted to strengthen the United States’ ability to combat money laundering, bank fraud, and sanctions evasion.

The first recommendation is that companies should pay close attention to Red Flags that could indicate suspicious financial activity related to illicit procurement. Table 1 provides a list of those that are most germane.

<b>Red Flags Commonly Associated with Suspicious Financial Activity Involved in Illicit Procurement Efforts</b>		
Vague or inconsistent end user information.	Customer’s company has relationships with sanctioned entities or individuals.	Capabilities of goods do not fit the customer’s line of business or industry.
Goods being purchased fall on a watch list of items that are frequently utilized by sanctioned programs.	Company has a lack of legitimate business activity, which could signal the presence of a front company.	Customer does not seem to have technical knowledge of the items or knowledge about proper packaging and handling of them.
Inquiries about goods are highly specific, with frequent changes upon questioning.	Company has irregularities in payment flows or unusual payment structures.	Customer utilizes foreign trading or front companies as intermediaries and communicators on a transaction or as purported end users.

**Table 1.** Red flags and warning signs identified in the illicit procurement scheme.<sup>8</sup>

Another recommendation is for companies to adopt routine audits of entities connected to sanctioned individuals and companies, which could uncover front companies before they are able to facilitate financial transactions. Audits could help to proactively identify suspicious financial activities, such as irregularities in payment flows, relationships with sanctioned entities, or a lack of legitimate business activity. These audits should be focused on industries that deal with sensitive materials, such as those that are controlled via the MTCR, the Nuclear Suppliers Group, or the Wassenaar Arrangement. By performing regular audits, sanctioned entities can be prevented from evading detection, and companies like Sinotech Dalian and its

<sup>8</sup> For a more detailed list, see, David Albright, Sarah Burkhard, Spencer Faragasso, Linda Keenan, and Andrea Stricker, *Illicit Trade Networks - Connecting the Dots, Volume 1* (Washington, DC, Institute for Science and International Press, 2020), available at <https://isis-online.org/books/detail/illicit-trade-networks-connecting-the-dots-volume-1>.

front organizations can be identified early on and blocked from accessing the U.S. financial system.

A third recommendation involves the enhanced monitoring of international wire transfers by financial institutions. This would focus on strengthening financial institutions' compliance with anti-money laundering (AML) regulations through measures such as thorough due diligence and incorporating risk-based customer identification programs (CIP). Financial institutions should conduct more thorough checks to verify the identities of individuals and businesses involved in wire transfers, particularly international transfers. These checks should include comparisons against government sanctions lists, such as the SDN list maintained by OFAC. Banks should also adopt a more risk-aware approach to their CIP program, which would involve assessing individuals and assigning a risk rating to customers based on factors such as their geographic location, the industry in which they conduct business, and their transaction history. Financial institutions should employ heightened scrutiny and due diligence with customers whose monitoring and assessment raise any red flags.

The United States could also adopt a more stringent approach by imposing additional sanctions on more Chinese entities. This would serve to deter these entities from providing financial or logistical assistance to other foreign sanctioned entities and curb their abilities to acquire U.S. goods. Additionally, by expanding the scope of sanctions, the U.S. would be sending a clear message about the consequences of violating U.S. laws and regulations related to illicit finance and illicit procurement.