



C4ADS
innovation for peace

TRADE SECRETS:

**Exposing China-Russia Defense Trade
in Global Supply Chains**

ABOUT C4ADS

C4ADS (www.c4ads.org) is a 501(c)(3) nonprofit organization dedicated to data-driven analysis and evidence-based reporting of conflict and security issues worldwide. Our approach leverages nontraditional investigative techniques and emerging analytical technologies. We recognize the value of working on the ground in the field, capturing local knowledge, and collecting original data to inform our analysis. At the same time, we employ cutting edge technology to manage and analyze that data. The result is an innovative analytical approach to conflict prevention and mitigation.

© C4ADS 2022

ABOUT THE AUTHOR

Naomi Garcia is an Analyst at C4ADS on the State-Sponsored Threats Cell. She holds an MA in International Economics, China Studies, and Korea Studies from the Johns Hopkins University School of Advanced International Studies (SAIS). Naomi speaks Mandarin, Spanish, French, and Korean.

LEGAL DISCLAIMER

The mention of any individual, company, organization, or other entity in this report does not imply the violation of any law or international agreement, and should not be construed to so imply.

ACKNOWLEDGEMENTS

C4ADS would like to thank all those who provided guidance and support during this project. The authors would like to particularly thank the C4ADS analysts who supported one or more aspects of the creation of this report: Jason Arterburn and Sara Thelen for shaping and editing the writing, Nicholas Carpenter for his assistant research, and Anna Wheeler for improving the report layout and design.

C4ADS would also like to thank its technology partners whose software and systems were integral to the project's success.



EXECUTIVE SUMMARY

Chinese state-owned conglomerates trade in sensitive technologies with Russia's defense sector, including to companies involved in Russia's ongoing war in Ukraine. At a time when the People's Republic of China (PRC) has become the subject of heightened vigilance and new trade sanctions, evidence suggests that patterns of data censorship and convoluted corporate networks serve to obscure trade in defense-applicable technology. Whether or not the PRC's trade data environment is opaque by design, it ultimately conceals the networks of people and companies involved in the trade of military equipment and undermines global nonproliferation efforts.

C4ADS developed reproducible methods for detecting PRC weapons trade that overcome these challenges in China's poor data environment. In the past year, these methods have supported more than 10 U.S. and international law enforcement actions against PRC entities involved in illicit trade of defense technologies. To demonstrate our methodologies in this report, we highlight three examples of previously undetected trade in defense products between a major Chinese state-owned conglomerate and Russia's state defense sector. In doing so, we find the following:

- **PRC state-owned conglomerates proliferate to companies supporting Russia's invasion of Ukraine.** We identified 281 previously unreported shipments of sensitive goods by China Poly Group Corporation (hereafter Poly Group) subsidiaries to Russian defense organizations between 2014 to 2022. For example, in January 2022, Poly Group's subsidiary Poly Technologies Inc. reportedly exported one shipment containing anti-aircraft missile radar parts to the sanctioned Russian state-owned defense company Almaz Antey, which reportedly supports Russia's war in Ukraine.¹
- **International import records provide actionable information about PRC defense shipments that is missing from China's domestic trade data sources.** Chinese trade data is expensive, unreliable, and incomplete, lacking details about both the products in any given shipment and the importing company overseas. We demonstrate how to overcome these limitations using other countries' reported imports from China, which can enable law enforcement and civil regulators to detect and target illicit PRC defense networks.
- **Corporate network analysis exposes proliferation activity by companies that may go undetected within the PRC's complex commercial system.** For example, corporate records indicate that Poly Group consists of more than 2,900 companies operating in more than 100 sectors with convoluted ownership structures across many layers of subsidiaries. By

¹ Pop, V. (2022a, March 4). Russia sanctions list: What the west imposed over the Ukraine invasion. Financial Times. <https://www.ft.com/content/6f3ce193-ab7d-4449-ac1b-751d49b1aaf8>; Adam Bychawski, S. M. (2022). Exclusive: UK firms bankroll arms fair where Russia shows off weapons. OpenDemocracy. <https://www.opendemocracy.net/en/exclusive-uk-firms-bankroll-arms-fair-where-russia-shows-off-weapons/>; Mann, S., König, O., Smith, B., Rose, A., & Ericsson, F. (2022, February 27). EU agrees on second wave of significant sanctions against Russia. Sanctions & Export Controls Update. <https://sanctionsnews.bakermckenzie.com/eu-agrees-on-second-wave-of-significant-sanctions-against-russia/>; The Council of the European Union. (2022). Council Decision (CFSP) 2022/430 of 15 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. <https://eur-lex.europa.eu/eli/dec/2022/430/oj>

investigating companies connected via shared corporate officers, C4ADS identified unsanctioned companies that trade in the same defense products with the same overseas partners as sanctioned entities in the conglomerate. Our findings indicate that network analysis focused on corporate leadership enables the detection of previously unknown defense proliferators within massive PRC conglomerates.

TABLE OF CONTENTS

The Challenge: PRC Companies Proliferate, but Detection is Difficult.....	6
In Focus: Poly Technologies and Its U.S. Sanctions Exposure.....	8
U.S. Department of State Sanctions on Poly Technologies and Subsidiaries.....	10
U.S. Department of Commerce Sanctions on Poly Technologies.....	10
U.S. Department of Treasury Sanctions Associated with Transferring U.S. Goods to Poly Technologies.....	11
Our Approach: Mirror Export Records and Complex Corporate Network Analysis.....	12
Step 1: Prepare PRC “Mirror” Export Data.....	12
Step 2: Identify Possible Proliferators.....	12
Step 3: Expose Proliferation.....	13
Limitations.....	15
In Action: Mapping Poly Group Defense Shipments to Russia.....	16
Case Study 1: Directly Sanctioned—Poly Technologies.....	16
Case Study 2: Subsidiary of a Sanctioned Entity—Poly Aviation Technologies.....	18
Case Study 3: More Distant Connections—Surpass Commercial.....	20
Conclusion.....	22
Appendix I: Poly Technologies’ Majority Owned Subsidiaries.....	23

THE CHALLENGE

PRC COMPANIES PROLIFERATE, BUT DETECTION IS DIFFICULT

PRC state-owned conglomerates proliferate weapons- and missile-related products internationally. While the international community has advanced a number of policies intended to limit Russia's access to defense technologies from abroad, PRC conglomerates continue to support Russia's military. As Russia continues to invade Ukraine, policymakers have become increasingly concerned about the extent to which Chinese firms might undermine global efforts to sanction Russia's defense sector. However, China's complex commercial system and its restricted trade data environment have made assessments difficult.

China's sprawling commercial networks create daunting challenges for law enforcement and civil regulators who wish to understand the PRC's illicit defense trade. China's State-owned Assets Supervision and Administration Commission of the State Council (国务院国有资产监督管理委员会; hereafter SASAC), which operates the central government's state-owned enterprises, controls 97 companies that together operate more than 80,000 total group companies in virtually all industry sectors, which exhibit complex ownership structures across many layers of subsidiaries.² Additionally, the thousands of companies within a conglomerate group may or may not operate in sectors that are related to the stated operations of the conglomerate's leading company, which complicates efforts to understand commercial risks from one company to the next across a conglomerate.

For example, the state-owned defense company NORINCO (中国北方工业集团有限公司) lists its business sector in Chinese corporate records as "wholesale," while its website describes its role as the "main platform responsible for developing [...] equipment for the PLA [People's Liberation Army]."³ While NORINCO is well known internationally as a major defense contractor, observers would be misled if they were to rely solely on corporate records to determine the company's primary industry, as is also evidenced when investigating lesser known conglomerates. The nondescript nature of business descriptions on corporate records makes it difficult to identify the companies involved in defense trade from corporate registration documents alone, which may not provide any indication of connections to military technology.

² Qichacha (2022, April). SASAC. <https://www.qcc.com/firm/g4bdd6c24056bb434978acfc5f40d168.html>

³ Norinco Group. (2015). Brief of NORINCO GROUP. <http://En.Norincogroup.Com.Cn/>
<http://en.norincogroup.com.cn/col/col432/index.html>

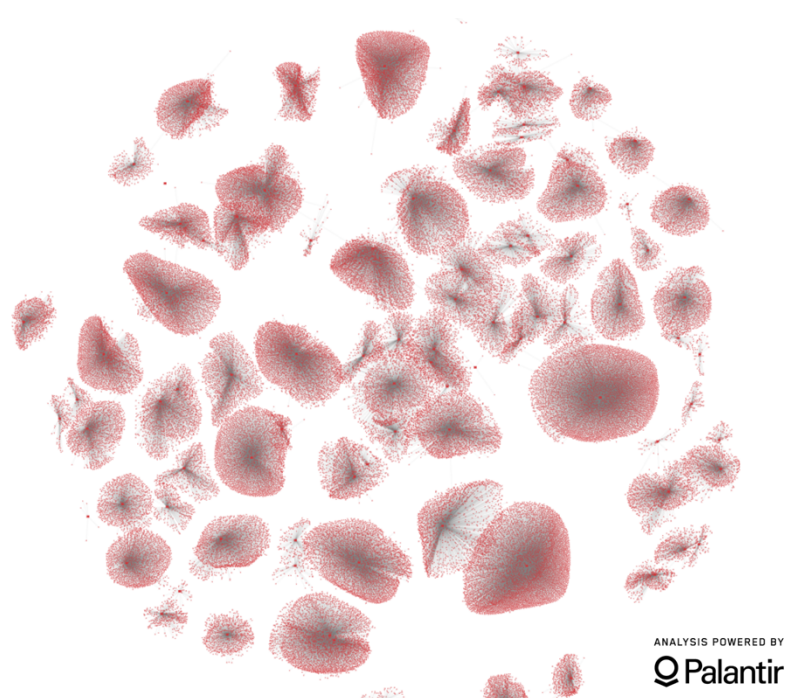


Figure 1: SASAC's 97 Conglomerates and their 80,000+ Group Companies

In addition to the complexity of China's commercial system, China's restricted trade data environment also complicates nonproliferation efforts. In particular, Chinese trade data often lacks the information required to conduct straightforward supply chain investigations. As shown in **Figure 2**, available PRC trade data omits the names of international business partners, which prevents analysts from gathering the information about the specific people and companies that would be necessary to take action against weapons proliferation activities. Moreover, China restricts the publication of its export records to international providers, unlike the United States, Russia, India, and other large economic powers that still publish their global trade data.⁴ Incomplete, censored trade records frustrate multilateral sanctions compliance efforts and allow PRC state defense companies to proliferate with little to no detection, which puts businesses around the world at risk of unwitting sanctions exposure.

⁴ S&P Global Market Intelligence. (n.d.). Panjiva - Global Trade Insights. Panjiva.Com. Retrieved April 26, 2022, from <https://panjiva.com/>

Shipment Date	Exporter	Importer
2013-01-01	Urumqi Akedili Imp. & Exp. Co., Ltd.	
2013-01-01	Shaanxi Xian Yi Electronics Co., Ltd.	
2013-01-01	Shaanxi Haojing Micro Electronics Technology Co., Ltd.	
2013-01-01	Core Ray Electronics Co., Ltd.	
2013-01-01	Complete Tech Trade & Industry Co., Ltd.	
2013-01-01	Xian State Imp. Exp. Corp.	
2013-01-01	China Guang Yun (Cgy)	
2013-01-01	China Shaanxi Haihui Imp.& Exp.Co. Ltd.	
2013-01-01	Shaanxi Shinhom Enterprise Co., Ltd.	
2013-01-01	Shaanxi Shinhom Enterprise Co., Ltd.	

Figure 2: Snapshot of Censored Chinese Trade Data

In Focus: Poly Technologies and Its U.S. Sanctions Exposure

Poly Technologies is a PRC company that has repeatedly engaged in proliferation activities with states of concern. Poly Technologies operates within Poly Group, a state-owned defense conglomerate with more than 2,900 member companies, according to Chinese corporate records.⁵ Poly Group's significant size and industry breadth comingles international weapons trade with consumer electronics, art, and antiquities, and more, which complicates efforts to isolate the companies involved in defense trade and limits the effectiveness of sanctions targeted at only one company within the broader group.⁶

⁵ Qichacha (2022, April). China Poly Group Corporation Limited. <https://www.qcc.com/firm/e049cdd6736d9ab1f3ceb84f7370b2f4.html>

⁶ Arterburn, J. (n.d.). Party Capital: A blueprint for national security due diligence on China. Retrieved April 26, 2022, from <https://c4ads.org/party-capital>

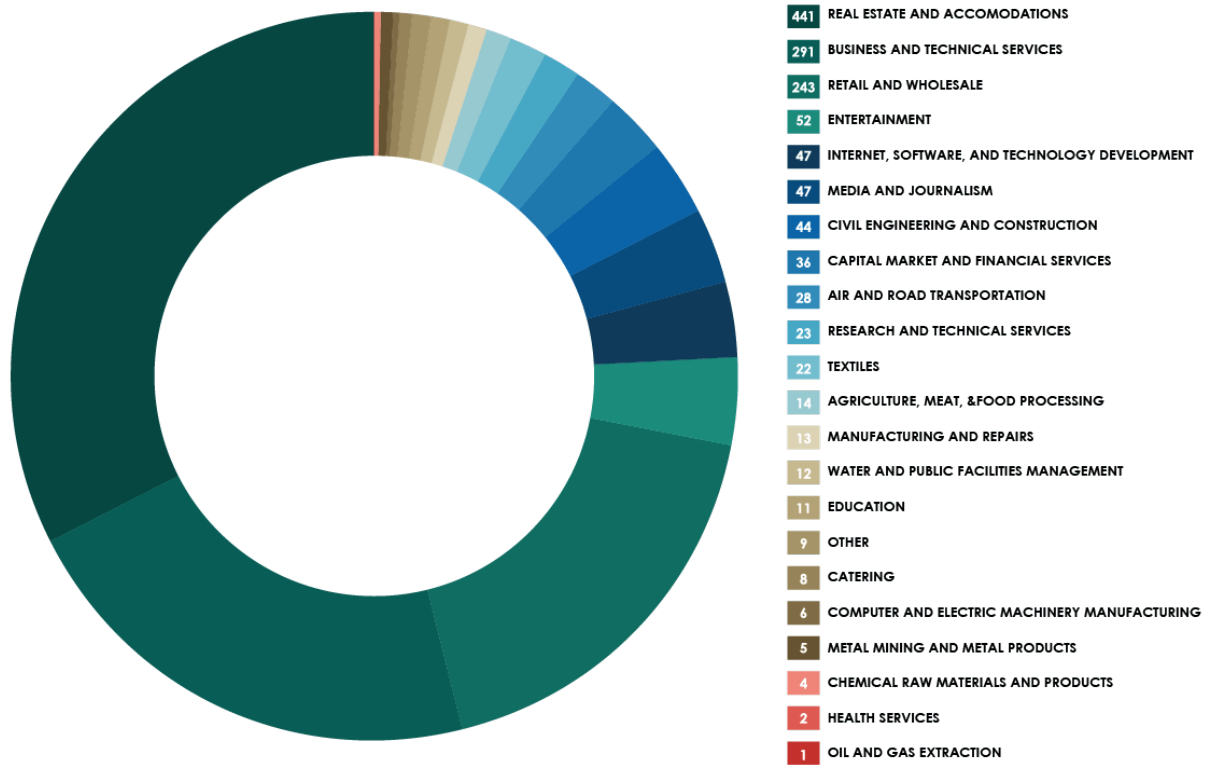


Figure 3: Poly Group Snapshot—Poly Group and PTI 20% or Greater Owned Entities by Industry Spread

U.S. regulators have imposed sanctions on Poly Technologies since 2013 for its proliferation of defense technology to states of concern. Those sanctions are summarized in the subsections below.

U.S. Department of State Sanctions on Poly Technologies and Subsidiaries

In 2013, the U.S. Department of State first sanctioned Poly Technologies under the Iran, North Korea, and Syria Nonproliferation Act (INKSNA) for transferring “equipment and technology... [that] could materially contribute to a weapons of mass destruction or cruise or ballistic missile program” to or from Iran, North Korea, or Syria.⁷ INKSNA sanctions automatically remain in effect for two years after their imposition date, and were not renewed on Poly Technologies in 2015.

On January 21, 2022, the U.S. Department of State again sanctioned Poly Technologies pursuant to the Arms Export Control Act because the company “substantially contributed to the design, development, or production of missiles” in a controlled country.⁸ These sanctions currently prohibit all imports to the U.S. from Poly Technologies, including imports of products that it manufactures. These sanctions remain in effect for at least two years from their listing date in January 2022, and may be renewed when the period of two years ends.⁹

Pursuant to Arms Export Control Act regulations, U.S. companies that import goods from Poly Technologies or its subsidiaries may be subject to penalties that include criminal fines up to \$1 million per violation and up to 20 years of imprisonment.¹⁰ In addition, administrative monetary fines can total up to \$300,000 per violation or twice the value of the transaction, whichever is greater.¹¹

U.S. Department of Commerce Sanctions on Poly Technologies

On June 26, 2014, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) included Poly Technologies on its Entity List for “acting contrary to the national security or foreign policy interests of the United States” for having “attempted to supply items to the People's Liberation Army.”¹² These regulations prohibit the export of any U.S. goods subject to Export Administration Regulations (EAR) to Poly Technologies. There are no license exceptions.^{13 14}

U.S. persons that export EAR goods to Poly Technologies may be subject to penalties including a fine of up to USD \$1 million per violation and up to 20 years imprisonment.¹⁵

⁷ 9768 Federal Register. (2013). Vol. 78, No. 28 / Monday, February 11, 2013 / Notices. Govinfo.Gov. <https://www.govinfo.gov/content/pkg/FR-2013-02-11/pdf/2013-03030.pdf>

⁸ State Department. (2022). Imposition of Missile Proliferation Sanctions on Three Entities in the People's Republic of China (PRC). In Federal Register (Vol. 87). <https://www.federalregister.gov/d/2022-01117>

⁹ Foreign Relations and Intercourse, 22 U.S.C. § 2797b. <https://www.govinfo.gov/content/pkg/USCODE-2020-title22/pdf/USCODE-2020-title22-chap39-subchapVII-sec2797b.pdf>

¹⁰ Bureau of Industry Security, U.S. Department of Commerce. (2020). Penalties. <https://www.bis.doc.gov/index.php/enforcement/oe/enforcement/penalties>

¹¹ Ibid.

¹² Bureau of Industry and Security. (2014). Addition of certain persons to the Entity List; And removal of person from the Entity List based on removal request. In Federal Register (Vol. 79, pp. 36199–36203). <https://www.federalregister.gov/d/2014-14935>

¹³ Ibid.

¹⁴ The EAR includes most goods from the U.S. with the exception of certain cultural and educational items such as books, newspapers, photo and video film; certain educational/information software; and items such as patents regulated by other U.S. agencies. For a complete list of exceptions to this export ban, check 734.3(b) of the EAR. [https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.3#p-734.3\(b\)](https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.3#p-734.3(b))

¹⁵ Foreign Relations and Intercourse, 22 U.S.C. § 2778. <https://www.govinfo.gov/content/pkg/USCODE-2020-title22/pdf/USCODE-2020-title22-chap39-subchapIII-sec2778.pdf>

U.S. Department of Treasury Sanctions Associated with Transferring U.S. Goods to Poly Technologies

In addition to penalties from violating the above U.S. State and Commerce sanctions programs by trading with Poly Technologies, U.S. companies that export to Poly Technologies may also be at risk of U.S. Department of Treasury Office of Foreign Assets Control (OFAC) sanctions if any of their exports—whether knowingly or unknowingly—are later diverted to an OFAC-sanctioned end-user.

Previous OFAC sanctions penalties have specifically penalized U.S. businesses for indirectly transferring goods to entities listed as Specially Designated Nationals. For example, in November 2018, U.S.-based technology company Cobham Holdings, Inc. paid USD \$87,507 to settle a civil liability investigation into its subsidiary's transfer of dual-use goods to OFAC-sanctioned Russian company Almaz Antey through Canadian and Russia distribution companies in violation of OFAC sanctions.¹⁶ Consequently, it is essential for businesses to conduct rigorous due diligence on trading partners—particularly those subject to any U.S. sanctions programs that may be proliferating more broadly than currently detected.

While Poly Technologies is explicitly subject to broad sanctions by multiple agencies across the U.S. government, private industry participants may still have a difficult time avoiding all potential risks of exposure to U.S. sanctions penalties due to the complexity of Chinese corporate networks and the lack of reliable Chinese trade data. We present the following methodologies both to assist international businesses in complying with sanctions protocols as well as to enhance civil regulatory detection and enforcement efforts.

¹⁶ Enforcement Information for November 27, 2018. (2018). Department of Treasury. https://home.treasury.gov/system/files/126/20181127_metelics.pdf

OUR APPROACH

MIRROR EXPORT RECORDS AND COMPLEX CORPORATE NETWORK ANALYSIS

PRC proliferation operations not only contribute to global insecurity, but also put unknowing business partners at risk of U.S. sanctions penalties for directly or indirectly transferring goods to sanctioned end-users, whether knowingly or unknowingly. In this report, we demonstrate how using new approaches to trade and corporate data analysis can assist law enforcement, civil regulators, and compliant businesses to overcome these challenges and advance global nonproliferation efforts.

Step 1: Prepare PRC “Mirror” Export Data

We first collected and integrated import records and transshipment records from countries that trade with China, which created a “mirror” of PRC exports abroad. We combined these sets of global imports into one larger Chinese export database and merged the records with C4ADS’ in-house international trade data. In total, we integrated more than 500 million unique global trade data records from international reporting jurisdictions.

This dataset is not a complete representation of PRC trade. Additionally, since the dataset constitutes reported trade from many different countries, it may be variable in its veracity and/or completeness as reporting standards may vary from country to country. Because of these limitations, this report does not aim to represent a comprehensive view of PRC exports globally, but instead uses the dataset as a baseline from which to investigate discrete companies and shipments that can be corroborated with other sources of data.

Step 2: Identify Possible Proliferators

We then identified companies associated with China’s military-industrial complex from government lists including but not limited to the U.S. Department of Treasury’s Office of Foreign Assets Control, the U.S. Department of Commerce Bureau of Industry and Security Entity List, and other sources. Next, we used official corporate registry documentation to identify additional corporate affiliates, which included not only a company’s majority owned subsidiaries but also sister companies with which it shares current or former leadership, as shown below in **Figure 4**. Where possible, we collected each company’s Mandarin- and English-language names from corporate records and translated them into local languages present in the import data, including Russian. Additionally, we included common nicknames and variations of group subsidiaries identified in public reporting, such as Poly Technologies’ “PTI” nickname in English or “Поли” in Russian, in order to enable searches in trade data collected in Step 1.

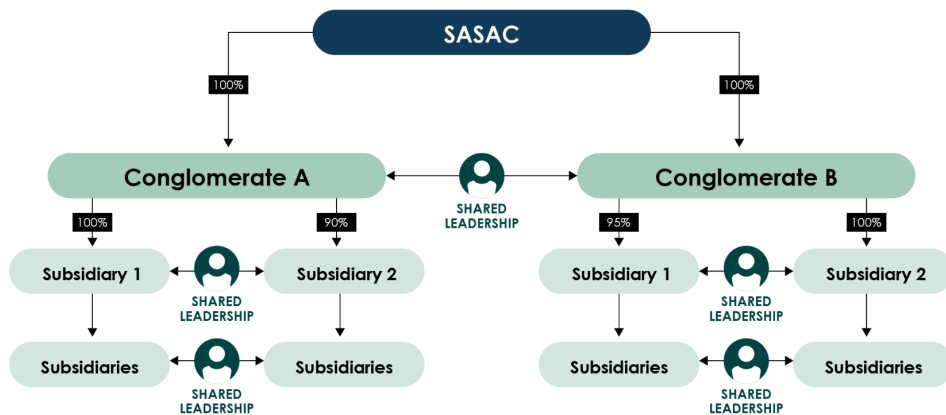


Figure 4: Structure of shared leadership across sister companies

Step 3: Expose Proliferation

As a final step, we searched for shipments associated with PRC companies of interest in our integrated trade dataset. To find various company names in these “messy” international records, we used a computational linguistic tool called a Levenshtein distance calculation that measures how similar two words or phrases are, which allowed us to identify shipments associated with companies of interest even when their names were misspelled from one source dataset to another. Once shipments were identified, we expanded our findings using social media, websites, news articles, and other primary source documentation in Mandarin, Russian, and other languages as relevant.

What is Levenshtein Distance?

Search Term	Name in Data	Characters Mismatched	Levenshtein Distance Ratio	Match?
Q POLY TECHNOLOGIES INC	POLY TECHNOLOGY INC	3/17	17%	YES
Q POLY AVIATION TECHNOLOGIES INC	POLY AVIATION TECHNOLOGY INC	1/22	32%	YES
Q POLY GROUP	POLYMER GROUP CONSULTING	13/22	59%	NO

Levenshtein Distance Ratio: Below 33% or 1/3 = mismatched, Above 33% or 1/3 = matched

■ 1 Mismatched character space

Figure 5: Levenshtein Distance Ratio—Percentage of Incorrect Letters

The Levenshtein distance is the number of letters that would need to change from one phrase to another to make them exactly the same. In our case, we sought to identify where a misspelled exporter name in trade data might correspond to our official company names in Chinese corporate records. For example, “POLY TECHNOLOGY” is only a 3-character distance from “POLY TECHNOLOGIES,” while the unrelated “SCHUCO POLYMER TECHNOLOGIES” company is a 12-character distance. This calculation works well to highlight companies that are misspelled variations of search terms, which helps to account for the human errors present in international trade records. Prior to calculating the distance, we recommend removing all punctuation. Some researchers may also wish to remove white spaces before calculation.

By taking the Levenshtein distance divided by the total number of letters in our “messy” exporter name, we produce a ratio of incorrect characters to correct characters. This creates a more standardized reference point, accounting for short and long company names alike. For example, the distance between “two” and “too” is only one character, but a Levenshtein ratio of 33% (or 1/3) because the inputs are so short. Essentially, a one-character difference between three-letter words is a much bigger problem than a one-character difference between longer words. For example, the distance between “computer” and “komputer” is also just one character, but this set has a lower ratio of incorrect characters at only 12.5% (or 1/8). See **Figure 5** below for more details.

With the Levenshtein distance calculated between each search term and exporter name pair seen in the data, we selected company name matches with a ratio of less than 33%, as entities with 2/3 non-matching characters are unlikely to form a match.¹⁷ We then we removed common suffixes, trailing characters, and punctuation from these potential matches to bucket company names into 150 unique potential exporter name matches. Next we manually referenced these 150 possible matches against their respective Poly Group search terms, discarding false positives. For companies whose name matches were ambiguous—for example the search term “Poly Aviation Technologies, Inc.” matched with the messy exporter name “P Aviation Tech Inc”—we cross-referenced the exporter’s registered address with its address listed in trade records, where available, to manually confirm a match.

¹⁷ Richard Cadieux, Towers Watson, Daniel R. Bretheim. (2014). Matching Rules: Too Loose, Too Tight, or Just Right? <https://support.sas.com/resources/papers/proceedings14/1674-2014.pdf>

Limitations

The report's methodology has several limitations. First, the use of international trade records to mirror PRC exports means that the data and any findings may not be comprehensive, as sanctionable trade activity may be missing from the dataset. Secondly, there is no way to verify that trade records are accurate or consistent from one jurisdiction to another. For these reasons, C4ADS limits its analytical conclusions to those supported directly by underlying documentation within the limitations of those documents. Throughout our research, we have used only corroborated, detailed customs data aggregated from reliable international sources and verifiable documentation such as corporate registry filings for which the source and credibility can be clearly established.

Additionally, we do not aim to draw comprehensive conclusions about PRC trade, Poly Technologies, or its network affiliates. Instead, we provide case studies to demonstrate the effectiveness of the methodologies we present to identify discrete instances of proliferation.

IN ACTION

MAPPING POLY GROUP DEFENSE SHIPMENTS TO RUSSIA

With the methodologies described above, we identified 281 previously unreported exports from China Poly Group Corporation companies to Russia's defense sector between 2014 and 2022. This section highlights three companies involved in illicit defense exports to Russia:

- Poly Technologies, which has been repeatedly sanctioned by the U.S. government and sent at least 268 sensitive shipments to an OFAC-designated SDN in Russia;
- Poly Aviation Technologies, which is a direct subsidiary of Poly Technologies and sent two dual-use shipments to two companies in Russia's defense sector; and
- Surpass Commercial, which shares only commercial officers with Poly Technologies and sent 11 shipments to the same Russian defense company as Poly Technologies and Poly Aviation Technologies.

Despite these companies' varying positions in Poly Group's corporate structure, they have all shared current or former senior leadership, according to corporate records, and have all exported similar dual-use machinery and laboratory equipment to the same Russian defense company Kazan Giproniiaviaprom (Казанский Гипронииавиапром), among other Russian defense exports.¹⁸ These three case studies illustrate varying degrees of connectedness from known PRC proliferators within a large conglomerate network that nonetheless engage in very similar trade patterns with entities of concern abroad. As a result, they underscore the need for law enforcement and civil regulators to adopt more robust analysis methods for corporate network analysis and supply chain due diligence in order to successfully curtail PRC proliferation.

Case Study 1: Directly Sanctioned—Poly Technologies

Since 2014, Poly Technologies has exported 268 shipments of dual-use aircraft, radar, and laboratory equipment parts to the Russian defense company Almaz Antey, which OFAC sanctioned in 2014 for its operations in Ukraine and Russia contrary to U.S. national security.¹⁹ Poly Technologies shipments to Almaz Antey included at least 16 shipments of klystrons, which are used to make long-range radar transmitters with dual-use applications.²⁰ Most recently, in January 2022, Poly Technologies sent Almaz Antey one shipment of radar antenna parts for Russian anti-aircraft missile systems, labeled as MRLS 92N6E antenna parts.²¹ The MRLS 92N6E is

¹⁸ Qichacha (2022, April). Surpass Commercial Corp. Ltd. <https://www.qcc.com/firm/911bcb759f7574d4058bb98229a4b7d5.html> ; Qichacha (2022, April). Poly Technologies, Inc. <https://www.qcc.com/firm/0af7bf1a55e60a1be3f5b3720b1203d2.html> ; Qichacha (2022, April). Poly Aviation Technologies Co., Ltd.. <https://www.qcc.com/firm/3ad9f858092daba14f7837411f305ca3.html>

¹⁹ Industry and Security Bureau. (2014b). Russian sanctions: Addition of persons to the Entity List and restrictions on certain military end uses and military end users. In Federal Register (Vol. 79, pp. 55608–55615). <https://www.federalregister.gov/d/2014-22207>

²⁰ Walker, W. H. (2013). Klystron transmitter (Patent No. 8559894). In US Patent (No. 8559894).

²¹ Labeled as "ЧАСТИ АНТЕНН ИЗ СОСТАВА МРАС 92Н6Е" in the data.

the radar system used in Russia's S-400 anti-aircraft missile defense systems.^{22 23} International media reports in February 2022 pictured Russia's use of these S-400s in its ongoing invasion of Ukraine.²⁴



Figure 6: Almaz Antey's S-400 Missile System Equipped with MRLS 92N6E Radar

OFAC sanctions prohibit U.S. businesses from financially or materially supporting Almaz Antey, including with goods and/or services and whether directly or indirectly. Specifically, they state that it is sanctionable for any U.S. persons to "have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of" SDNs, including Almaz Antey.²⁵ While these OFAC restrictions do not explicitly prohibit business with Poly Technologies, they reserve the right to penalize companies whose exports to Poly Technologies end up with Almaz Antey or with other SDNs.²⁶ Because of these regulations, international businesses operating even unknowingly with the affiliates of a proliferator may be at risk of U.S. OFAC sanctions. (See **Figure 7** below.)

²² Карпенко, А. В. (2014). Невский бастион, Nevsky bastion. Военно-технический сборник. История отечественного оружие, зарубежная военная техника. Nevskii-Bastion.RU. <http://nevskii-bastion.ru/s-400-tm-2014-foto/>

²³ Ansari, U. (2022, January 17). Can Pakistan counter India's new S-400 air defense system? DefenseNews. <https://www.defensenews.com/global/asia-pacific/2022/01/16/can-pakistan-counter-indias-new-s-400-air-defense-system/>

²⁴ WION. (2022). Russia-Ukraine crisis: S-400 air defence system, Iskander missiles in Belarus - see satellite images. WION. <https://www.wionews.com/photos/russia-ukraine-crisis-s-400-air-defence-system-iskander-missiles-in-belarus-see-satellite-images-451164>

²⁵ Executive Order -- Blocking Property of Additional Persons Contributing to the Situation in Ukraine. (2014, March 20). The White House - Office of the Press Secretary. <https://obamawhitehouse.archives.gov/realitycheck/the-press-office/2014/03/20/executive-order-blocking-property-additional-persons-contributing-situat>

²⁶ Pop, V. (2022, March 4). Russia sanctions list: What the west imposed over the Ukraine invasion. Financial Times. <https://www.ft.com/content/6f3ce193-ab7d-4449-ac1b-751d49b1aaf8>

Overview of US Russia Sanctions
Applies sanctions to entities that the U.S. Departments of Treasury and State determine are operating in the Russian defense sector
Applies to any business transferring U.S. products to a sanctioned entity as well as its subsidiaries and controlled entities
Stipulated Sanctionable Business Engagements
<p>“to operate in such sectors of the Russian Federation economy as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State, such as financial services, energy, metals and mining, engineering, and defense and related materiel”</p> <p>“to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order”</p> <p>“to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any person whose property and interests in property are blocked pursuant to this order”</p>

Figure 7: U.S. OFAC Russia Sanctions

Penalties for violating Russia sanctions by transferring goods to an SDN can include additional criminal penalties up to USD \$1 million as well as up to 20 years in prison. Entities unknowingly transferring to OFAC-listed Russian SDNs may be subject to fines up to USD \$250,000.²⁷

Case Study 2: Subsidiary of a Sanctioned Entity—Poly Aviation Technologies

Trade data further indicates that Poly Aviation Technologies, Inc., a 95%-owned subsidiary of Poly Technologies, has also exported dual-use laboratory and aircraft parts to state-affiliated Russian defense companies.

In February 2019, Poly Aviation Technologies sent one shipment of industrial laboratory equipment to Russian defense company Kazan Giproniaviaprom. Kazan Giproniaviaprom lists Poly Group and the Russian Government's Defense Export Organization as among its main business partners on its website. (See **Figure 8** below.)²⁸

²⁷ Office of Foreign Assets Control. (2016). Ukraine/Russia-related Sanctions Program. https://home.treasury.gov/system/files/126/ukraine_overview_of_sanctions.pdf

²⁸ Kazan Giproniaviaprom. (2022, March). www.gap-rt.ru/partners/



Figure 8: Kazan Giproniiaviaprom and Russia's Defense Export Organization

In November 2019, Poly Aviation Technologies sent one “TSV36M033” helicopter rotor collector to private Russian defense and aviation company ATC Zvezda (АТЦ ЗВЕЗДА), according to the trade data. The shipment's records also state that Poly Aviation Technologies originally imported the component parts from Russian military weapons manufacturer Sarapul Power Generating Plant (Сарапульский Электродгенераторный Завод)²⁹ at an unspecified date before reexporting them to ATC Zvezda in November 2019, demonstrating the company's multilateral financial and material support of the Russian defense sector.

ATC Zvezda reports on its website to partner with the Russian Ministry of Defense.³⁰ Russian corporate aggregators report that ATC Zvezda is wholly owned by two directors³¹ who also serve as the two chiefs of staff of a Russian government-backed scientific research organization, the Science-XXI Fund (Фонд Наука-XXI).³²



Figure 9: TSV36M033 Collector for Helicopter Rotor

²⁹ ВН. ПРИКАЗ № 2945 ОТ 29.08.2017. (2017). Minpromtorg.Gov.Ru. <https://minpromtorg.gov.ru/docs/#I20633>

³⁰ Zvezda, A. T. C. (n.d.). Aviation technology center “Zvezda” (ATC Zvezda). Atczvezda.Com. Retrieved April 26, 2022, from http://www.atczvezda.com/eng/about_company/

³¹ Timur Rafaelevich Timoshev (Тимур Рафаэльевич Тимошев) and Lian Tebin (Лянь Тебинь) own 50% each, АТЦ “Звезда”, ООО. (n.d.). СБИС. Retrieved April 26, 2022, from <https://sbis.ru/contragents/7716887072/774301001>

³² Связи ТИМОШЕВ ТИМУР РАФАЭЛЬЕВИЧ. (n.d.). List-Org.Com. Retrieved April 26, 2022, from <https://www.list-org.com/man/272050/graph;>

Case Study 3: More Distant Connections—Surpass Commercial

Trade data also indicates that Surpass Commercial (华越商业有限公司),³³ a Poly Group company with significant overlapping leadership with Poly Technologies, exported 11 shipments of dual-use goods to Kazan Giproniaviaprom, a trade partner of both Poly Technologies and Poly Aviation Technologies. This underscores how companies with similar leadership and operational structures exhibit similar trade patterns.

Surpass Commercial, like Poly Technologies, is a wholly owned subsidiary of Poly Group.³⁴ These two sister companies hold no ownership stakes in one another, but have had some of the same Poly Group executives in leadership positions:

- Surpass Commercial's former director Wang Xingye (王兴晔) is Poly Technologies' current Board Chair.³⁵
- Surpass Commercial has two executives that hold current senior leadership roles at Poly Technologies' subsidiary Poly Aviation Technologies. Surpass Commercial Director Dai Ning (戴宁) is the Board Chair of Poly Aviation Technologies,³⁶ and Surpass Commercial Supervisor Zhao Junshuang (赵君双) is a Poly Aviation Technologies supervisor.³⁷
- Surpass Commercial's current Chair of the Board Hou Hongxiang (侯鸿翔) is also the Chair of the Board at two of Poly Technologies' 100% owned subsidiaries—Xinshidai Group (保利国防科技研究中心有限公司) and Xinshidai Engineering Consulting Co., Ltd. (新时代工程咨询有限公司).³⁸ Hou Hongxiang is also Chair of the Board at PTI's 40% owned group company Shanghai Poly Defense Technology Development Co., Ltd. (上海保利防务科技发展有限公司).³⁹

Both Surpass Commercial and Poly Technologies' subsidiary Poly Aviation Technologies have exported laboratory equipment and machinery to the aforementioned Russian defense company Kazan Giproniaviaprom. Poly Technologies reportedly sent almost identical shipments of vibration system shipments to Kazan Giproniaviaprom prior to 2014, as shown below in **Figure 10**.

³³ Qichacha (2022, April). Surpass Commercial Corp. Ltd. <https://www.qcc.com/firm/911bcb759f7574d4058bb98229a4b7d5.html>

³⁴ Qichacha (2022, April). China Poly Group Corporation Limited. <https://www.qcc.com/firm/e049cdd6736d9ab1f3ceb84f7370b2f4.html>

³⁵ Qichacha (2022, April). Dai Zhu. <https://www.qcc.com/pl/p0a5d99a5bdf74399dbf2ad2b596e179.html>

³⁶ Qichacha (2022, April). Dai Zhu. <https://www.qcc.com/pl/p0a5d99a5bdf74399dbf2ad2b596e179.html>

³⁷ Qichacha (2022, April). Zhao Junshuang. <https://www.qcc.com/pl/pr2e1f410a8e4ed9c9484c987337356c.html>

³⁸ Qichacha (2022, April). Hou Hongxiang. <https://www.qcc.com/pl/p84a2e1d00420049aaaae152cee76f26.html>

³⁹ Qichacha (2022, April). Shanghai Poly Defense Technology Development Co., Ltd. <https://www.qcc.com/firm/c370a113ce4026add277ac6066752791.html>

DATE	EXPORTER	IMPORTER	PRODUCT DETAILS	HS CODE
2/13/19	POLY AVIATION TECHNOLOGIES CO.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	INDUSTRIAL EQUIPMENT LABORATORY TESTS FOR THE EFFECT OF EXTERNAL ENVIRONMENT	8419899890
7/19/16	SURPASS COMMERCIAL CORP.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	GALVANIC LINE DESIGNED FOR NICKEL PLATING ELECTROCHEMICAL	8543300000
5/8/15	SURPASS COMMERCIAL CORP.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	VIBRATION TESTING SYSTEM-3 PCS	9031200000
5/8/15	SURPASS COMMERCIAL CORP.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	VIBRATION TESTING SYSTEM 1pc	9031200000
5/8/15	SURPASS COMMERCIAL CORP.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	INDUSTRIAL EQUIPMENT LABORATORY TESTS FOR THE EFFECT OF EXTERNAL ENVIRONMENT	8419899890
4/20/15	SURPASS COMMERCIAL CORP.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	INDUSTRIAL EQUIPMENT LABORATORY TESTS FOR THE EFFECT OF EXTERNAL ENVIRONMENT	8419899890
4/20/15	SURPASS COMMERCIAL CORP.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	VIBRATION TESTING SYSTEM 1pc	9031200000
4/20/15	SURPASS COMMERCIAL CORP.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	VIBRATION TESTING SYSTEM 1pc	9031200000
4/20/15	SURPASS COMMERCIAL CORP.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	VIBRATION TESTING SYSTEM 1pc	9031200000
2/25/15	SURPASS COMMERCIAL CORP.LTD	ЗАО "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	VIBRATION TESTING SYSTEM 1pc	9031200000
2/24/15	SURPASS COMMERCIAL CORP.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	VIBRATION TESTING SYSTEMS.	9031200000
2/24/15	SURPASS COMMERCIAL CORP.LTD	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	VIBRATION TESTING SYSTEM 1pc	9031200000
6/9/12	POLY TECHNOLOGIES INC	ЗАО "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	ELECTRODYNAMICAL VIBRATION SYSTEM (shaker)	9031200000
6/9/12	POLY TECHNOLOGIES INC	ЗАО "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	TEMPERATURE AIR CHAMBER (heat chamber)	8419899890
6/8/12	POLY TECHNOLOGIES INC	ЗАО "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	ELECTRODYNAMICAL VIBRATION SYSTEM (shaker)	9031200000
6/8/12	POLY TECHNOLOGIES INC	ЗАО "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	TEMPERATURE AIR CHAMBER (heat chamber)	8419899890
12/29/11	POLY TECHNOLOGIES INC	ООО "ИНЖИНИРИНГОВАЯ КОМПАНИЯ "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	ELECTRODYNAMICAL VIBRATION SYSTEM (shaker)	9031200000
2/18/11	POLY TECHNOLOGIES INC	ЗАО "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	ELECTRODYNAMICAL VIBRATION SYSTEM (shaker)	9031200000
2/18/11	POLY TECHNOLOGIES INC	ЗАО "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	ELECTRODYNAMIC VIBRATING SYSTEM	9031200000
2/18/11	POLY TECHNOLOGIES INC	ЗАО "КАЗАНСКИЙ ГИПРОНИИАВИАПРОМ"	ELECTRODYNAMIC VIBRATING SYSTEM	9031200000

Figure 10: Poly Technologies' and Sister Company's Exports to Kazan Giproniaviaprom

Accounting for group companies with shared leadership that otherwise hold no ownership interests in one another can help identify new proliferation network affiliates undetectable with basic beneficial ownership investigations. With its sprawling ownership structure, a central conglomerate directly and indirectly controls operations and leadership for its majority owned group companies, and can orchestrate the movement of select officers across sister companies. With shared or similar leadership, these sister companies carry out similar business operations through non-financial mechanisms of influence and control across the corporate network.⁴⁰

⁴⁰ Arterburn, J. (n.d.). Party Capital: A blueprint for national security due diligence on China. Retrieved April 26, 2022, from <https://c4ads.org/party-capital>

CONCLUSION

PRC state-owned defense conglomerates actively export weapons technologies to Russia and other high-risk state militaries, even when U.S. and international sanctions could impose significant penalties for such activity. PRC conglomerates are able to continue making illicit shipments due in large part to China's opaque trade data environment and sprawling complex conglomerate structures that conceal their activity and blunt the impact of U.S. counterproliferation measures. These global military-related transfers contribute to the destabilization of international democracies such as Ukraine, while also putting international business partners at risk of U.S. sanctions penalties for knowingly or unknowingly transferring goods to sanctioned end users around the world.

In this report, we present methodologies that successfully identify previously undetected PRC state defense exports. Our methods for analyzing mirror export records and overlapping corporate leadership can support a wide range of law enforcement and civil regulatory efforts beyond weapons proliferation detection to include other supply chain issues including narcotics, wildlife products, natural resources, and more. We present these methods to assist researchers, businesses, and enforcement agencies in better detecting and deterring illicit trade by making it easier to recognize the offenders.

While the nature of PRC opaque trade and complex corporate data makes it difficult to confirm that any given business partner is truly complying with all international regulations, businesses can do their part to avoid financially or materially supporting the networks of entities known to be providing supplies to Russia's military and other destabilizing international forces. To that end, these methodologies may prove to be powerful tools to assist international actors and enforcement agencies that wish to contribute to global security—while also avoiding any penalties for violating U.S. nonproliferation sanctions.

APPENDIX

POLY TECHNOLOGIES' MAJORITY OWNED SUBSIDIARIES

COMPANY	CHINESE NAME	POLY TECHNOLOGIES %
Poly Technologies, Inc.	保利科技有限公司	SELF
POLY (Luannan) International Logistics Co., Ltd.	保利 (滦南) 国际物流有限公司	100
Xinshidai Group	保利国防科技研究中心有限公司	100
Poly Technologies (Tianjin) Co., Ltd.	保利科技 (天津) 有限公司	100
Poly Technologies Development Co., Ltd.	保利科技发展有限公司	100
Xinshidai Engineering Consulting Co., Ltd.	新时代工程咨询有限公司	100
Poly Aviation Technologies Co., Ltd.	保利航空科技有限公司	95
Poly Ship Technologies (Beijing) Co., Ltd.	保利 (北京) 船舶科技有限公司	51
Shaanxi Poly Special Vehicle Manufacturing Co., Ltd.	陕西保利特种车制造有限公司	51

Chart 2: Poly Technologies & Majority Owned Subsidiaries⁴¹

⁴¹ Qichacha (2022, April). Poly Technologies, Inc. <https://www.qcc.com/firm/0af7bf1a55e60a1be3f5b3720b1203d2.html>