



SHIELD
by SOURCEREE



What's Inside

21st century defense industrial strategy for America - OSD A&S Industrial Policy

Risks and considerations for businesses using data services and equipment from firms linked to the People's Republic of China

Rare Earth Elements (REE), an essential component in key consumer and defense technologies, come from China

National Security Newsletter

January 2021



Authors: Adam Murphy & John Lash

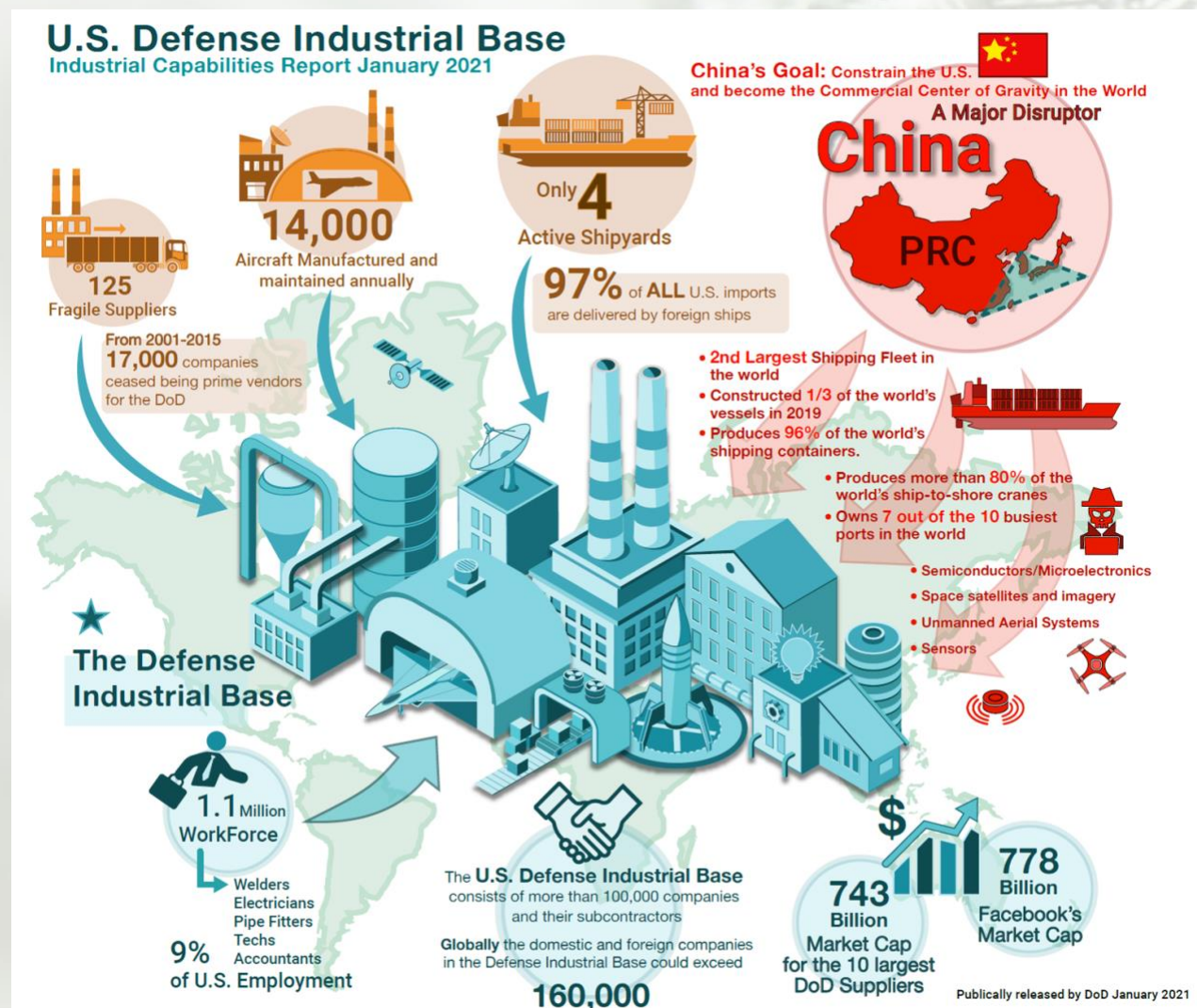
Fiscal Year 2020 Industrial Capabilities Report to Congress: OSD A&S Industrial Policy

This report describes a 21st century defense industrial strategy for America.

The American military is still the most powerful in the world. U.S. defense industry companies are global leaders in weapons innovation and production. Likewise, the Department of Defense is the colossus of the federal system, i.e., the single biggest buyer of goods in the U.S. government. But unless the industrial and manufacturing base that develops and builds those goods modernizes, adjusting to the world's new geopolitical and economic realities, America will face a growing and likely permanent national security deficit.

Four efforts to improve the defense-industrial base, preserving U.S. military dominance and keeping Americans safe:

1. Re-shore the U.S. defense industrial base and supply chains to the United States and to allies, starting with microelectronics, and restore our shipbuilding base.
2. Build a modern manufacturing and engineering workforce and research and development base.
3. Continue to modernize the defense acquisition process to fit 21st century realities.
4. Find new ways to partner private sector innovation with public sector resources and demand.



Select excerpts from the report (specific to Navy):

There has been a rise of The People's Republic of China (PRC) as a dual threat, both military (the Chinese Navy is now the largest in the world with 350 vessels) and economic, which threatens critical supply chains, and also challenges our export control, foreign investment, and technology transfer policies.

The buildup of China's navy, including aircraft carriers, has been one of the most remarkable and strategically disruptive global defense spending trends in the past two decades. By commissioning fourteen warships a year, Beijing has made clear that it intends to be a world-class maritime power in addition to having the world's largest military on land. While China's naval buildup has been able to piggyback on its rapidly expanding commercial shipbuilding industry, U.S. shipbuilding, by contrast, has become a key vulnerability in the U.S. defense manufacturing base, as we will see.

The Office of Industrial Policy assessed America's shipbuilding woes, both defense and commercial, which began more than five decades ago. Fourteen defense-related new ship-construction yards have shuttered, and three have exited the defense industry. Only one new-ship-construction yard has opened. Today, the Navy contracts primarily with seven private new-construction shipyards, owned by four prime contractors, to build its future Battle Force, representing significantly less capacity than the leading shipbuilding nations.

The Future Naval Force Study (FNFS), developed by the Department of Defense to ensure American naval supremacy, sets forth a multi-year program divided into five-year increments with careful attention to meeting base budgetary limitations to achieve the goal of a 355-ship navy. Yet that plan has to rely on a maritime industry, both naval and commercial, that has significantly less capacity than the world's other leading shipbuilding nations – South Korea, Japan, and, ominously, China. So while today, the United States Navy's Battle Force consists of 297 ships, China has managed to build the world's biggest navy with 350 vessels.

China's shipbuilders also enjoy the advantage of being part of the world's biggest national steel producer and user. The United States meanwhile is fourth, after China, India, and Japan. How do we fill the shipbuilding gap? Start by building more ships. Not only will that expand the fleet, but it will also drive the analysis and decisions required to ensure a shipbuilding base that can produce and sustain an expanded Navy. That our shipbuilders delivered in 2020 no fewer than ten ships (two Virginia-class submarines, one America class amphibious assault ship, three littoral combat ships, two Spearhead-class expeditionary fast transports, one Arleigh Burke-class destroyer, and one Lewis B Puller-class expeditionary sea base) is a remarkable achievement. It is a harbinger of what can be done with even a modest expansion of that capacity.




Given current macroeconomic conditions, China is expected to continue to out-build the United States in terms of ship quantities. The U.S. Navy will continue to use its technological advantages to maintain superiority in the maritime domain.

Industry Changes: The U.S. Navy continually monitors its industrial base, focusing on critical suppliers to ensure the supply of material and components for shipbuilding programs. There are constant changes in an industrial base with thousands of suppliers, but the health of the industrial base remained steady in 2020. The Navy is closely monitoring the purchase of AK Steel Corporation and ArcelorMittal USA by Cleveland-Cliffs Inc., which has traditionally been a mining company; and the purchase of Fairbanks

Morse Engines, a critical supplier of medium speed diesel engines for the Navy, by Arcline Investments, a private equity firm.

Foreign Investment Review: Within Industrial Policy, the *Protect* function is predominately carried out by the Office's Foreign Investment Review (FIR) team. FIR leads the Committee on Foreign Investment in the United States (CFIUS) reviews for DoD and acts as the principal advisor to the USD(A&S) on foreign investment in the U.S. This involves coordination across more than 30 DoD component organizations to identify, review, investigate, mitigate, and monitor foreign direct investment in the United States. FIR relies on DoD stakeholders for the technical expertise needed to analyze the threats, vulnerabilities, and consequences associated with foreign investment. Predatory and adversarial investments can result in diminishing U.S. sources and expertise, and increasing foreign dependence and illegitimate technology transfer, thereby threatening U.S. military superiority.

Investment Priority Areas

	Long Range Precision Fires; Next Generation Combat Vehicle; Future Vertical Lift; Network; Assured Positioning, Navigation, and Timing; Air and Missile Defense; Soldier Lethality; Synthetic Training Environment
	Metals Processing and Fabrication; Electronics Processing and Fabrication; Composites Processing and Fabrication; Manufacturing Enterprise; Energetics Manufacturing
	Advanced Concepts; Future Factory; Digital Enterprise; Additive Manufacturing; Low-Cost Attributable Systems; Networked Command, Control, & Communications (C3) Systems; Hypersonic Strike
	Advanced Microcircuit Emulation; Battery Network; Castings/Forgings; Military Unique Sustainment Technology; Subsistence Network; Defense Logistics Information Research; Additive Manufacturing
	High Temperature; Refractory Alloys; Thermal Protection Systems; Advanced Ceramic Composites; Printed Sensor Microsystems; Next Generation Electronics; Flexible Hybrid; Electronics; Biocarbon-based Supercapacitors; Additive Manufacturing
	Metals; Electronics; Composites; Advanced Manufacturing Enterprise; Energetic Materials; USD(R&E) Modernization Priorities: 5G, Artificial Intelligence and Machine Learning, Autonomy, Biotechnology, Cyber, Directed Energy, FNC3, Hypersonics, Microelectronics, Quantum Science, Space

2020 Economic Security Assessment: DHS - Office of Strategy, Policy, and Plans (PLCY)

In 2020, DHS established the Trade and Economic Security (TES) sub-office within PLCY

TES is comprised of four teams: Economic Security Policy, Analysis and Assessments, Trade Policy, and Foreign Investment Risk Management (CFIUS).

TES identified the following key trends that shaped the global economic landscape in 2020:

- **The People's Republic of China is rising using a combination of hostile economic practices and an industrial policy** that, if left unchecked, will threaten the future of U.S. economic security. These practices give China a disproportionate advantage in global influence over competitors who seek to uphold both the text and spirit of the rules-based international economic order.
- **The integration of high-tech systems into traditional infrastructure shows transformational economic promise, but also introduces cyber vulnerabilities** to those same systems increasing risks of stolen intellectual property, illicitly acquired data, and disruption of national critical functions. These risks endanger the future of U.S. economic prosperity if proper steps are not taken to secure the systems.
- **Supply chain dependences on single, sometimes adversarial nations create access chokepoints and vectors for inflicting non-economic actions with a geopolitical agenda**, posing significant risk to the integrity of systems and the long-term availability of goods if access is disrupted.

Select excerpts from the report:

Data Practices of the People's Republic of China: China has a storied history of leveraging cyber-enabled means of intrusion for intellectual property and technology theft, resulting in the loss of billions of dollars to U.S. businesses. Now, it seeks to codify potentially malicious data practices to give its companies greater competitive advantages when harnessing that data. Currently in effect, its Cybersecurity Law requires companies operating in China to store their data within the geographical borders of China; and its National Intelligence Law requires companies to submit relevant information and data to the Chinese security apparatus without allowing those companies to inform their customers.

Electronic Vehicle (EV) Battery Manufacturing: China dominates production of battery-grade raw materials, accounting for 80% of total global output in 2019. China leads in other segments of the EV battery supply chain producing 66% of anodes and cathodes (the two critical pieces for EV battery functionality) and controls 73% of global output of lithium-ion battery cell manufacturing in 2019.

Position, Navigation, and Timing (PNT) Infrastructure: Position, navigation and timing services is an enabling domain that includes the creation, placement, and uninterrupted use of satellites and other internationally placed sensors that are necessary to ensure the ability to navigate international and domestic airspace and waters. The principal technology in the PNT domain is the Global Positioning System (GPS) in the United States. Other satellite navigation systems in the world include GALILEO (European Union), GLONASS (Russia), and BeiDou (China). PNT services can also be used to track users, measure and monitor weather and nature-related events (e.g., hurricanes, volcano eruptions), and collect data on the Earth in general. Several civil, military, and commercial technologies, services, and critical infrastructure are heavily reliant on the integrity of PNT systems. PNT enables other critical

economic domains as it powers communications, information technology, transportation, emergency services, energy, and financial services.

- *Risks: DHS identified the reliance on GPS as essentially the sole provider of PNT services in the United States and around the world as a significant risk. As with any technology, sole reliance and lack of back-ups for critical systems means disruption could prove catastrophic. GPS jamming, spoofing, cyber-enabled intrusions, physical sabotage, compromised technology within systems, and operation of U.S. data and computing services in data centers of other countries that compel access to the data all bear significant risk to PNT systems. In addition, military anti-satellite technologies will pose a significant threat to PNT services particularly in the event of a conflict.*

Future Prospectus

Limited Intervention on a Transaction Basis: Limited intervention in this way is largely transactional and fails to combine efforts in partnership with the private sector and other stakeholders to create large-scale incentives. By punishing only those companies that get caught, government intervention in this manner can disproportionately impose undue regulatory burdens, altering the competitive landscape in unintended ways. It can also make the government slow to adapt to the private sector, and chase innovation into less restrictive jurisdictions around the world. In addition, a narrow transactional approach does not provide an efficient way for the government to invest in certain industries, or research and development. It also limits private sector incentives to identify and mitigate risks from adversaries.

This model for addressing risk falls short in that it only tells industry what not to do, assumes the government can accurately identify risk in every case, and does not provide practical government-enabled solutions that directly promote innovation and competitiveness. This is especially true in areas where U.S. businesses are being pushed out of markets by foreign government assisted efforts, like mobile network infrastructure. Without increased tools to help U.S. companies compete against foreign government assisted conglomerates, the limited, transactional approach will further ossify U.S. innovation, while allowing certain economic vulnerabilities to deepen.

Public-Private Collaboration: A collaborative approach, with government and industry working together to identify and mitigate risks is the best way to preserve innovation and build the foundations for economic security. This future represents a proactive strategic approach to risk mitigation that leverages the combined input of the U.S. Government, allies and partners, and the private sector. Identifying not only areas where the United States is losing market share but also areas where the United States has significant market share, but those supply chains might be threatened by current and future adversaries is important.

If the emerging regulatory regimes are expanded, such as executive orders and focused regulatory action intended to diversify supply chains and stoke U.S. competitiveness, the result will be resilient U.S. ICT systems, improved data protection from cyber exploitation, and reduced operational risks that affect the security and resilience of users. Intellectual property theft will be minimized saving the U.S. billions each year. Supply chains for these sectors will begin to be diversified reducing the risk of dependence on and exploitation from China and leave the United States and the rest of the world with alternative sources of supply.

Data Security Business Advisory (DHS)

Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China

The PRC's data collection actions result in numerous risks to U.S. businesses and customers, including: the theft of trade secrets, intellectual property, and other confidential business information; violations of U.S. export control laws; violations of U.S. privacy laws; breaches of contractual provisions and terms of service; security and privacy risks to customers and employees; risk of PRC surveillance and tracking of regime critics; and reputational harm to U.S. businesses.

Select excerpts from the report:

Risks of Procuring Data Services From, or Partnering with PRC

Data Centers Owned or Operated by PRC Firms: PRC laws are most effective at creating compulsory data access when the data travels through a PRC firm abroad or a firm located within the PRC. PRC firms that own and operate data centers, both within China and abroad, are subject to laws which require their secret cooperation with PRC intelligence services. Under this legal framework, these firms are required to secretly share data with the PRC government or other entities upon request, even if that request is illegal under the jurisdiction in which these firms operate.

Foreign Data Centers Built with PRC Equipment: Chinese suppliers are not exempted from PRC laws which require cooperation with PRC intelligence services, even when their equipment leaves the PRC. Under the National Intelligence Law, the PRC has the ability to direct PRC firms to covertly install backdoors or "bug doors" into their equipment or software, allowing for easy access by PRC intelligence services. Additionally, the CCP subsidizes the use of PRC firm's hardware, software, telecommunications infrastructure, and other inputs for the creation and operation of data storage and processing centers.

Joint Ventures: Under the PRC legal framework, the PRC government may request secret access to any data to which a PRC firm or entity is provided access, whether as a Joint Venture (JV) partner or through other data sharing agreements. This legal requirement applies regardless of the legal jurisdiction of the JV. This is important for JVs who gather or maintain third-party data for which they have made assurances of privacy and confidentiality.

Legally Acquired Data Augmenting Illicitly Acquired Data: The CCP, or agents working on its behalf, can also purchase data through brokers to augment and validate illicitly acquired data. Combinations of incomplete or anonymized data, when layered on top of each other, can create a more complete data set for identification and analysis. In many cases, anonymized data sets require only a few additional "anonymized" data elements to make identification possible, even though each data set had been gathered independently under current practices for anonymization. Matching data elements across licitly and illicitly acquired data sets—especially if combined with methods to identify and link data to specific devices via media access control (MAC) address, browser fingerprinting.

Fitness Trackers and Other Wearables: Even where the identity of the wearer is kept anonymous by the device itself, the combination of location data over a certain time interval can identify where each user lives, works, or otherwise spends time. Location data of this sort would not only provide travel patterns of wearers, but—in combination with property tax records—could be further leveraged to identify names and family members.

Special Report: Rare Earth Elements (REEs)

Approximately 90 percent of all supply and processing of Rare Earth Elements, an essential component in key consumer and defense technologies, comes from China.

The United States is currently 100 percent reliant on imports of 14 critical minerals, and over 50 percent import-reliant on 15 critical minerals.

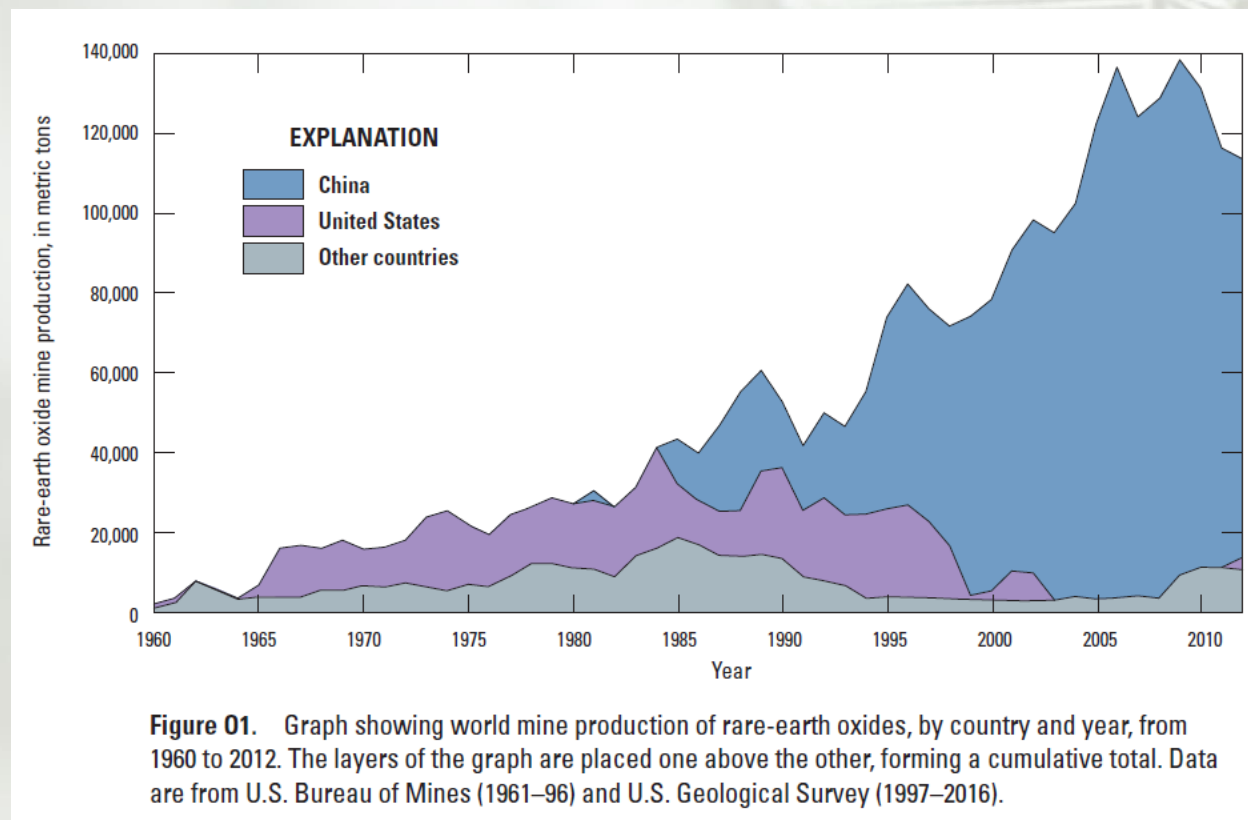
The rare-earth elements (REEs) are 15 elements that range in atomic number from 57 (lanthanum) to 71 (lutetium); they are commonly referred to as the “lanthanides.” Yttrium (atomic number 39) is also commonly regarded as an REE because it shares chemical and physical similarities and has affinities with the lanthanides. Although REEs are not rare in terms of average crustal abundance, the concentrated deposits of REEs are limited in number.

Because of their unusual physical and chemical properties, the REEs have diverse defense, energy, industrial, and military technology applications.

As the incoming Biden administration and like-minded leaders around the world try to wean the world off fossil fuels, they are relying on a non-renewable resource: the rare earths and minerals to produce rechargeable batteries, wind turbines and solar panels.

The materials are overwhelmingly produced by one nation: China

The leading export markets for China’s REEs are Japan, the United States, and France. The supply of REEs to consumers outside of China is determined not by mine capacity but by production and export quotas set by China’s Ministry of Commerce (MOFCOM) and the Ministry of Industry and Information Technology.



United States Manufacturing Impact: Critical manufacturing also includes mining and processing of minerals that are necessary to produce certain high-tech finished products. These minerals, like cobalt, lithium, graphite, copper, and rare earth elements, not only need to be mined but also processed and refined from ore into useable material.

American Mineral Security Act (2019): Sponsor – Murkowski, Co-Sponsor – Manchin

Draft legislation that will help to fulfill the critical minerals strategy developed in response to Executive Order 13817, A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals. The bill would require the federal government to identify deposits, expedite permitting, streamline regulatory processes and invest in research and training of workers with expertise in mineral exploration, manufacturing and recycling.

Critical minerals are defined as (i) a non-fuel mineral or mineral material essential to the economic and national security of the United States, (ii) the supply chain of which is vulnerable to disruption, and (iii) that serves an essential function in the manufacturing of a product, the absence of which would have significant consequences for our economy or our national security.

Horizon Scanning:

Cobalt - China's refineries, fed in large part by feed stuff from Chinese owned mines, supply 80% of the world's battery-ready high-grade cobalt.

- *In 2019, Commodities trader and miner Glencore extended its supply agreement with Chinese battery maker GEM by another five years. Under the latest agreement, the Chinese company will receive about 150,000t of cobalt contained in hydroxide from Glencore until 2029, replacing a previous agreement to receive about 60,000t through 2024.*

Lithium - China is among the five top countries with the most lithium resources and it has been buying stakes in mining operations in Australia and South America where most of the world's lithium reserves are found. China's Tianqi Lithium owns 51 percent of the world's largest lithium reserve in Australia.

- *A major component for both electric vehicles (EVs) and large-scale battery storage for renewable energy production, lithium is set to play a key role in the renewable energy revolution. Both EVs and such energy storage rely on lithium as an absolutely essential, non-replaceable component of the battery, making the metal one of the most sought-after resources on the energy market.*
- *The U.S. contributes less than 2% of the world's lithium even though it holds 17% of global lithium reserves. U.S. lithium production has historically been hampered by the relatively low concentration of lithium in U.S. brines, and lack of new technology available to economically extract it.*
- *In December 2018, Chinese manufacturing company Tianqi bought a 23.8% share in the world's second largest lithium producer, Chilean-based SQM, for \$4.1 billion from Canadian fertilizer company Nutrien. This is the largest deal in history for a lithium asset.*
- *China has majority control of all three major components of lithium-ion batteries -- 51% of the global total of chemical lithium, 62% of chemical cobalt and 100% of spherical graphite.*

Rare Earth Salts (<http://rareearthsalts.com/>) – Located in Nebraska, with contracts with the Department of Energy. Rare Earth Salts is a privately held industrial and applications technology company focused on the separation and refining of all sixteen rare earth elements to high purity from various feedstocks worldwide. This company should remain a focus of the U.S. Government.

Lynas (Australia) <https://www.lynascorp.com/> – the only producer of scale of separated rare earths outside of China and second largest in the world.

SHIELD VISION

Software platform
for on-demand
supply chain risk
assessments and
financial intelligence

SHIELD SQUAD

Analytical Support

SHIELD INTEL

Business
intelligence reports
on critical suppliers

Protected by



SHIELD
by SOURCEREE

Sourceree's SHIELD program is a comprehensive supply chain risk management (SCRM) solution designed to help answer questions about supply chain disruptions and risks, particularly foreign investment.



downloaded from p15.wallpapers.com