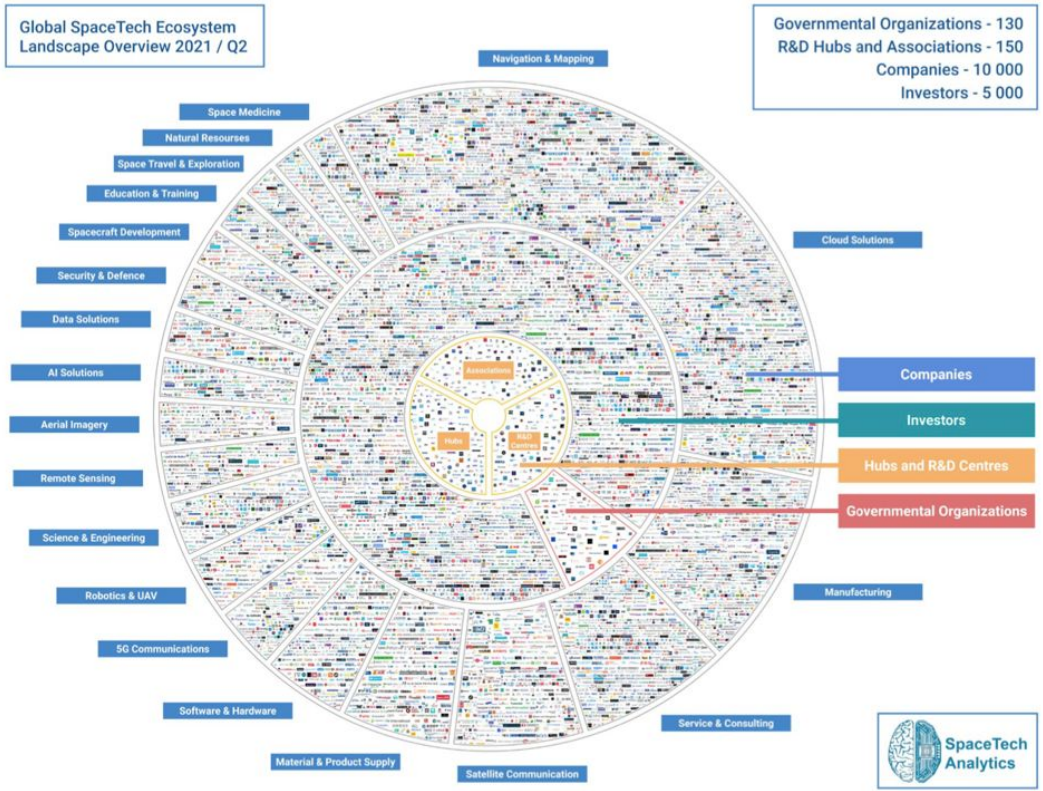
Companies in an Era of Competition

Leah Walker
Executive Director, Berkeley Risk and Security Lab

BERKELEY RISK & SECURITY LAB

Witnessing a Boom in the Commercial Space Industry



And it’s not just the U.S.….

Eastern Stars Rising: The Rise of China’s Commercial Space Industry

RYAN NELSON, TAYLOR RHOTEN, AND BRIAN MACCARTHY

July 29, 2025

But commercial space companies operate in a dual use space…

A REUTERS SPECIAL REPORT

Musk ordered shutdown of Starlink satellite service as Ukraine retook territory from Russia

Soldiers panicked and drones surveilling Russian forces went dark.

By **Joey Roulette**, **Cassell Bryan-Low** and **Tom Balmforth**

July 25, 2025 4:00 AM PDT · Updated July 27, 2025

Ukraine relies on Starlink for its drone war. Russia appears to be bypassing sanctions to use the devices too

And it’s not just Satellites…

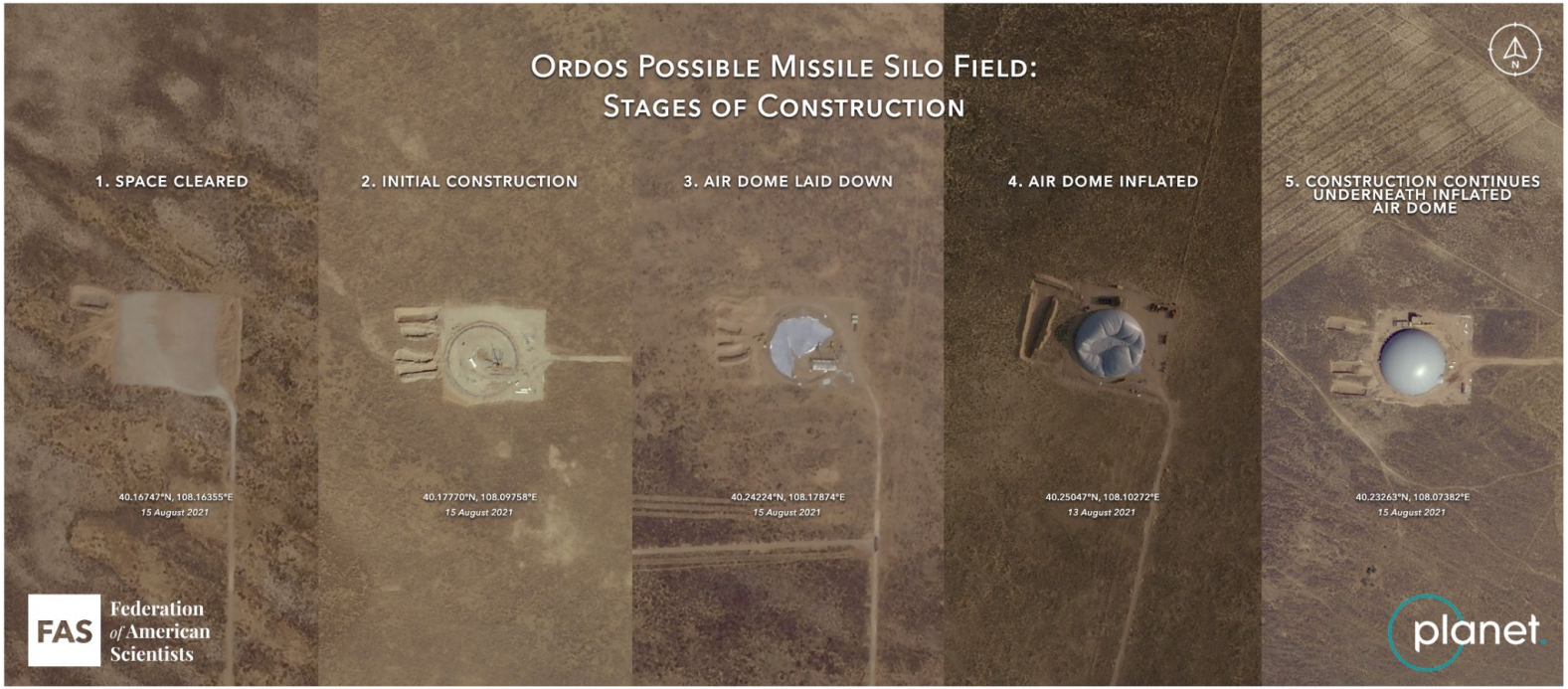


Fig. 1. Images from the *Zhousidun* dataset, which feature various military vessels with overlaid bou

Fig. 2. Additional examples of images from the *Zhousidun* dataset.

the
in s
data
data
mod

Bri

Due
tech
dee
avai
the
not

of a

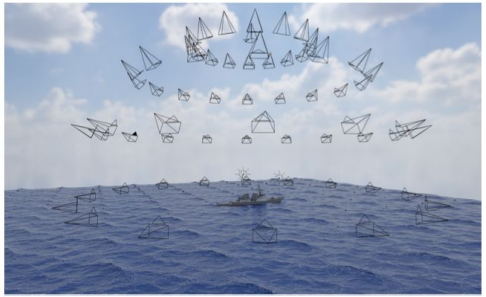


Fig. 4. A synthetic scene of the USS *Arleigh Burke* with positions of captured images.

In computer vision research, the mmdetection[9] framework is commonly used due to the extensibility it provides. In industry, one of the most adopted frameworks for object detection is the Ultralytics[10] object detection framework. For example, the YOLO family of models in the Ultralytics library is used broadly. YOLO is a single-stage CNN for object detection that is fast, memory efficient, and accurate, all highly desirable characteristics for deployment on edge devices such as small unmanned aerial vehicles (sUAS).

Recently, vision transformers have beat models such as YOLO for object detection on almost all popular object detection benchmarks, such as COCO [48], by at least 17% on mAP (a metric described in depth later in this report).[11] However, these other methods are more difficult to

Evaluated simply on the test set of *Zhousidun*, the trained model achieves a mAP (at 0.50 intersection over union (IoU)) of 0.926. In many targeting workflows, this mAP is considered to be quite good. These results are visualized in Figure 5.

Fig. 5. Predictions on the *Zhousidun* test set

Which opens them up to targeting

Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault

The satellite hack that took the world by storm was more complex than initially thought, according to a Viasat executive.

BY CHRISTIAN VASQUEZ AND ELIAS GROLL • AUGUST 10, 2023

Securing Taiwan's Satellite Infrastructure Against China's Reach

Gil Baram | Tuesday, November 14, 2023, 10:14 AM

Share On:

As Taiwan faces the looming threat of a Chinese invasion, the need to fortify its satellite infrastructure from cyberattacks becomes ever more urgent.

But targeting doesn't just happen in the skies…

GOV·UK Menu

Home > Government > Cyber security > Cyber risks of cloud computing in the ground segment of the space sector

Department for Science, Innovation & Technology

Research and analysis

Cyber risks of cloud computing in the ground segment of the space sector

Published 8 August 2025

Security challenges when space merges with cyberspace

Vijay Varadharajan [a], Neeraj Suri [b]

Defense Supply Chain Vulnerabilities Under Scrutiny

The U.S. Department of Defense's industrial base strategy aims to mitigate critical vulnerabilities in supply chains supporting military space operations. Supply constraints in the space sector struggle to keep up with the increasing demands of military satellite manufacturing. Reliance on single sources or "fragile" sources of supply of critical components is a significant weakness in the supply chain. The new National Defense Industrial Strategy Implementation Plan addresses this issue in its remediation strategy. Key measures include strengthening domestic manufacturing and leveraging the Defense Production Act to fortify supply chain resilience for national defense. The Pentagon is weary of supply risks as the Space Development Agency begins to develop and deploy a military LEO satellite constellation. The increasing demand on the sector is straining suppliers who face limited development capacity. The Office of Strategic Capital has begun offering loans to companies that aim to develop critical space technologies as a method of improving supply chain resilience and removing the risk of single and fragile sources. This plan will ideally boost both the commercial space economy and national security by encouraging more partners to invest in critical space technology.

How military technology reaches Russia in breach of U.S. export controls

By **David Gauthier-Villars**, **Steve Stecklow** and **John Shiffman**

April 29, 2022 1:43 PM PDT · Updated April 29, 2022

April 29 (Reuters) - By his own account, Ilias Sabirov, a Moscow businessman, had supplied Russia's military with high-performance computer chips made in the United States for years.

Then, in 2014, Russia seized the Ukrainian peninsula of Crimea, and the U.S. government began imposing a series of new sanctions and export controls on Russia, including severely restricting sales of such chips.

Bureau of Industry & Security
Office of Congressional and Public Affairs

FOR IMMEDIATE RELEASE | December 18, 2020 | Media Contact: OCPA@bis.doc.gov

International Trio Indicted in Austin for Illegal Exports to Russia

Levers of Economic Competition

Sanctions and Export Control

Limiting the goods and services that a country or entity can receive (sanctions) or that entities can export to non-domestic markets (export control).

Regulation

Government laws and regulations applied to critical technology fields, directing their use, development, and potential restriction.

Government Contracts and Acquisitions

Government signals of technology priority, as well as efforts to grow “critical” technologies.

Targeting Competitor Sectors

Targeting the sectors and capabilities of adversaries and competitors….

Threat Vectors for the Technology Sector

Cyberattacks and Espionage

Cyber intrusions with the aim of collecting information, disrupting operations, and otherwise harming business operations.

IP and Trade Secrets Theft

Theft of intellectual property and or trade secrets, usually with the intent of replicating the capability to gain market advantage.

Illegal Export and Sanctions

Illegal export of technologies or their components, with the intent of illegal use (often in the context of violating sanctions and export control).

Supply Chain Security

Targeting supply chains for disruptions, seizure of goods and components, or as a mean to reach an upstream entity (like SolarWinds).

Capital Security and Adversarial Capital

The Threats

- **Loss of Intelligence (Espionage):** Certain FOCI activities aim to support corporate and state-based espionage, insider threats, unintended or illegal tech transfer of critical technologies (IP, trade secrets, state secrets), and cyber exploits or intrusions into critical infrastructure.
- **Loss of Control (Supply Chain):** FOCI risks include those of sole-source dependence on adversary-controlled suppliers (where supply could be shut off or defects introduced during a conflict), as well as the establishment of infiltration points where systems could be hijacked or shut down directly.
- **Loss of Economic Assets:** An inadequate response to FOCI will result in the continued loss of jobs (over-dependence on offshoring), loss of investment money and time partnering with compromised partners, and loss of engagement from critical technology partners.

Emerging Tech and Threat Vectors for the Technology Sector

Data Poisoning

AI systems are dependent on datasets. By poisoning datasets, adversaries can manipulate the way models behave and react, disrupting their ability to function and potentially causing them to make incorrect decisions or unexpected actions.

Vulnerability Detection

Adversaries can use pattern recognition algorithms to detect vulnerabilities in firewalls and software, finding the easiest way to target a digital system.

Employee Targeting

Artificial intelligence models can be used to track employee profiles, finding patterns in behaviors that can be exploited. Generative AI models can be used to generate false content, like voice samples and videos, to trick employees into providing access or information.

Data Liabilities

Datasets with sensitive material, such as personal identifying information (PII), classified materials, and trade secrets can be a liability for overseeing companies. Models can inadvertently reproduce materials in the dataset, exposing companies to legal actions.

BRSL

Cyberattacks and Espionage

LockBit claims cyberattack on India's national aerospace lab

Japan aerospace agency provides details of October data breach

Boeing confirms 2023 $200m ransomware demand

Pro-Russian hackers claim responsibility for knocking U.S. airport websites offline

Intellectual Property and Trade Secrets

Engineer Arrested for Allegedly Stealing Trade Secret Technology Designed to Detect Nuclear Missile Launches and Track Missiles

Former Engineer Sentenced for Possessing Stolen Semiconductor Trade Secret

Chinese spy convicted of trying to steal U.S. aircraft trade secrets given 20-year sentence

Illegal Export and Sanction Violations

South Bay Resident Charged With Smuggling And Exporting American Aviation Technology To Beijing University

Kansas businessman pleads guilty in case over illegal export of aviation tech to Russia

California Man Indicted for Illegally Exporting Aircraft Parts to Iran

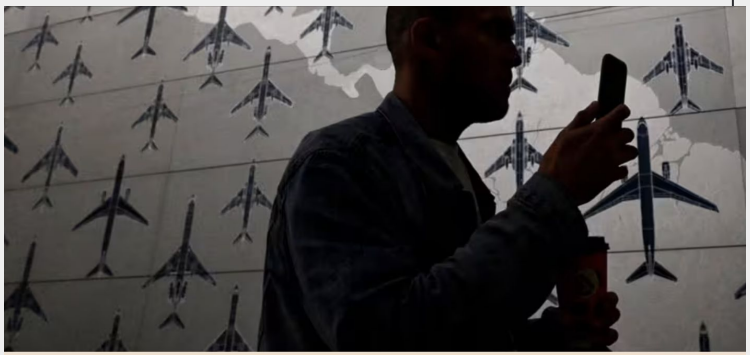
Russian Nationals Admit to Illegally Sending Controlled Aviation Technology to Russia

BRSL

Geopolitical Crises

Russo-Ukrainian War: The sanctions placed on Russia have dramatically crippled the Russian technology sector, which was highly dependent on technology and industrial imports like aircraft components and microelectronics.

Crisis and Supply Chain Disruptions: As Covid demonstrated, the global supply chain for microelectronics is delicate, and crisis, both manmade and natural, could dramatically affect access to critical components like semiconductors.



The Big Read Airlines + Add to myFT

The smuggling trail keeping Russian passenger jets in the air

Sanctions have caused imports of spare parts to collapse. But airlines have found new ways to get components into the country

BRSL

Case Study: Lattice Semiconductor

From Chips War: “Then, in spring 2016, Tsinghua quietly bought 6 percent of the shares in Lattice semiconductor, another U.S. chip firm. “This is purely a financial investment,” Zhao told the *Wall Street Journal*. “We don’t have any intention at all to try and acquire Lattice.” Scarcely weeks after the investment was publicized, Tsinghua Unigroup began to sell its shares in Lattice. Shortly thereafter, Lattice received a buyout offer from a California-based investment firm called Canyon Bridge, which journalists from Reuters revealed had been discreetly funded by the Chinese government. The U.S. government firmly rejected the deal.”

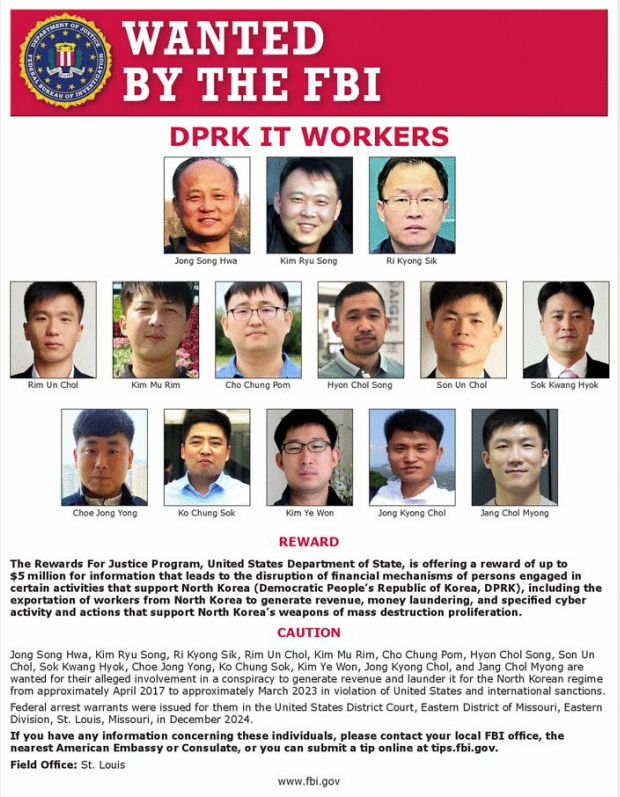
“The problem wasn’t simply that Chinese government-linked funds were buying up foreign chip firms. They were doing so in ways that violated laws about market manipulation and insider trading. While Canyon Bridge was maneuvering to purchase Lattice Semiconductor, for example, one of Canyon Bridge’s cofounders tipped off a colleague in Beijing, passing along details about the transaction via WeChat and at meetings in a Starbucks in Beijing. His colleague bought stock based on this knowledge; the Canyon Bridge executive was convicted of insider trading” pp. 268

BRSL

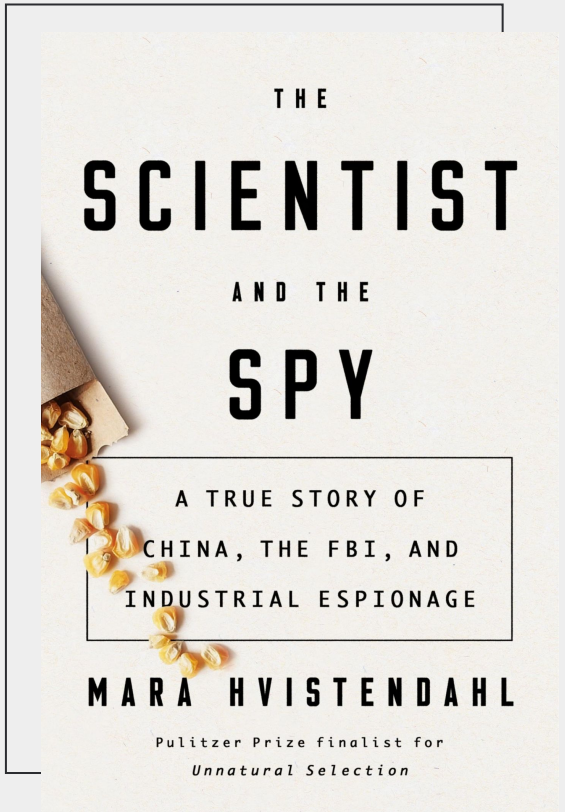
Case Study: North Korean IT Employees

From Recorded Future: “In an era in which remote work has become the norm, North Korea has seized the opportunity to manipulate hiring processes, using fraudulent information technology (IT) employment to generate revenue for the regime. North Korean IT workers infiltrate international companies and secure remote positions under false identities. These operatives not only violate international sanctions but also pose severe cybersecurity threats, engaging in fraud and data theft and potentially disrupting business operations.”

Financial Fraud & Cyber Espionage



Case Study: Targeting GMO Crops



Case Study: Even Google Can Be Targeted

Google employee exfiltrated files associated with Google cloud computing by copying data to Notes Application ->

Employee receives emails from CEO of an early-stage technology company in Beijing, offering salary and CTO position ->

Employee started acting as CTO while retaining Google position ->

Employee then founded Shanghai Zhisuan Technology Co., serving as its CEO, pitching and building the company while still employed by Google. ->

Employee transfers Google files to personal file while in China, Google notices activity but employee reassures investigator. ->

Employee books ticket to leave the country and resigns from Google by email.

An Old Case Study: Tech Transfer and Submarine Capabilities

Toshiba Details Trail of Crime In Sale of Machinery to Soviet

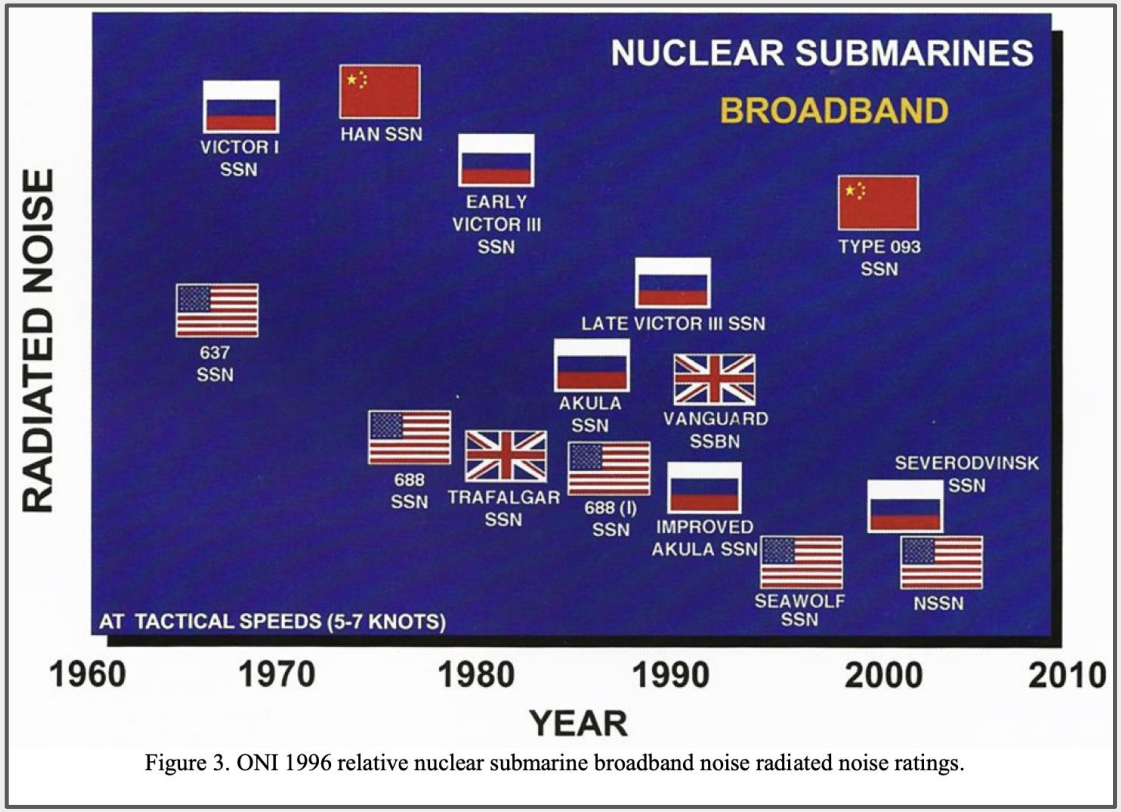


Figure 3. ONI 1996 relative nuclear submarine broadband noise radiated noise ratings.

Retrospective on AI Export Controls

Leah Walker
Executive Director, Berkeley Risk and Security Lab

BERKELEY RISK & SECURITY LAB

The Platonic Ideal of Export Controls

1. **Clear idea of what event, capability, or occurrence that must be prevented.** Example: the development of a nuclear weapon.
2. **Clear idea of what technologies and capabilities enable that capability.** Example: gas centrifuges
3. **Clear idea of current state of play.** Example: Iranian uranium stockpiles, processing and storage facilities, and seeming lack of plutonium pathway.
4. **Clear idea of what is below and above that threshold:** Example: plutonium processing

From there, need to consistently and widely implement controls.

An Example from NOAA

Instead of limiting the export of all GPUs that meet a performance threshold, forever, the U.S. government might take inspiration from the National Oceanic and Atmospheric Agency and Department of Commerce's approach to licensing satellite. This approach stipulates that U.S. commercial satellite imaging companies can only export imagery of the quality that matches the best foreign provider.

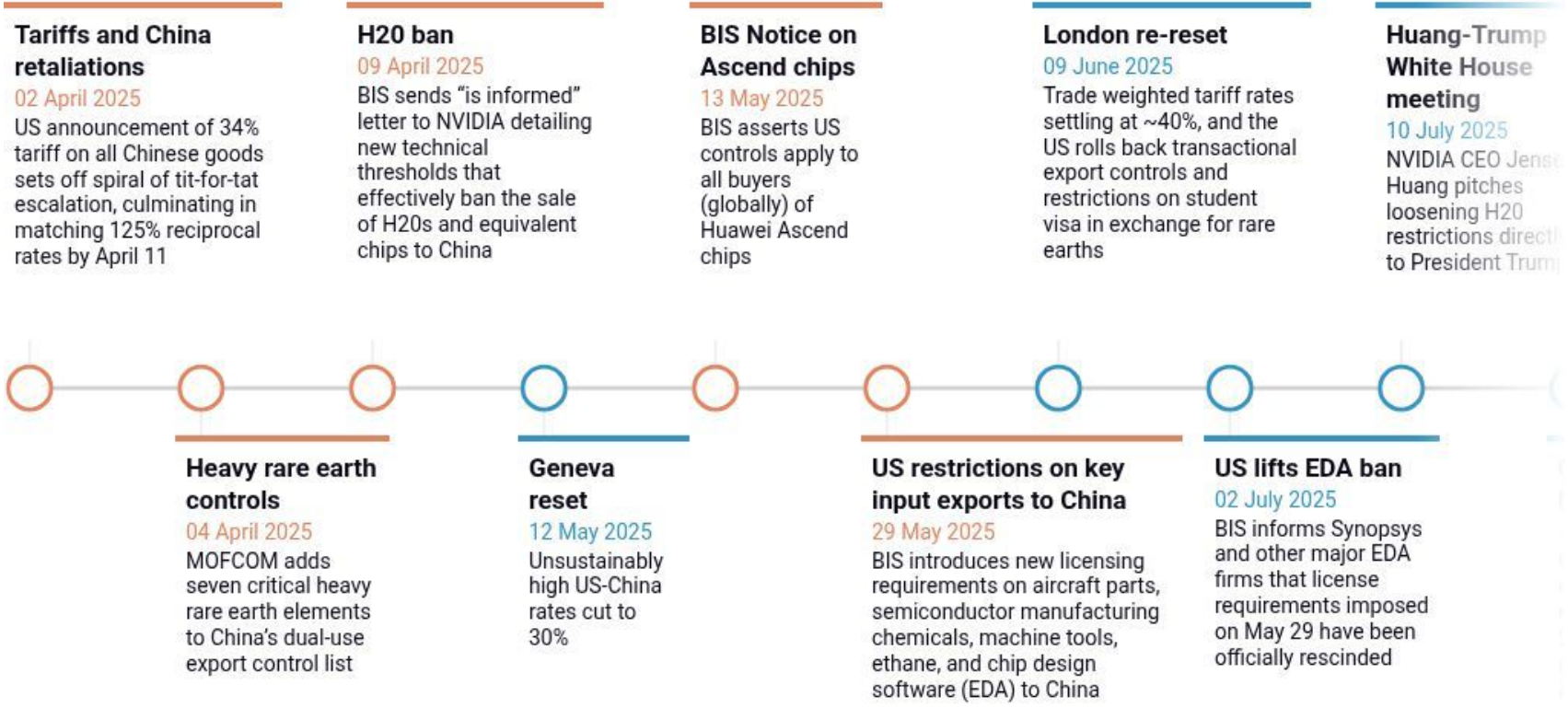
1. Clear objective of what to prevent: High quality satellite imagery (dual-use)
2. Clear idea of enabling technology: Commercial satellite imagery
3. Clear threshold to tie control to: Best resolution in domestic market
4. Clear understanding of what is above and below that threshold: Resolution in domestic market, which is not difficult to measure

FIGURE 1

Crisis-reset loop: Timeline of escalatory and de-escalatory actions in US-China tech and trade policy

April to July 2025

Escalation De-escalation



Source: Rhodium Group

Restrictions work….

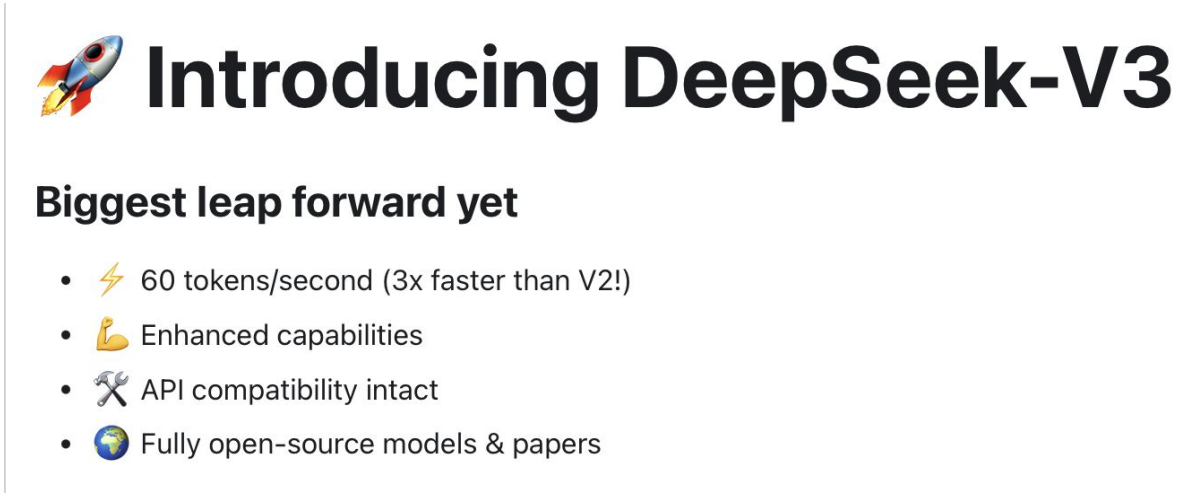
America's Chip Restrictions Are Biting in China

Shortages of advanced AI chips are so acute that Beijing is intervening and tech companies are resorting to workarounds

China's Tech Still Constrained by Export Controls, ASML's CEO Says

Christophe Fouquet says tech companies will always look for ways to advance despite restrictions that have limited their access to cutting-edge chips and the equipment needed to make them

… but also breed ingenuity



DeepSeek-V3, ultra-large open-source AI, outperforms Llama and Qwen on launch

Shubham Sharma

December 26, 2024

TEVV is critical to detecting efficiency gains

Whack-a-Chip: The Futility of Hardware-Centric Export Controls

Ritwik Gupta,[1,2,*] Leah Walker[1] and Andrew W. Reddie[1]

[1]Berkeley Risk and Security Lab, University of California, Berkeley and [2]Berkeley AI Research Lab, University of California, Berkeley
*Corresponding author: ritwikgupta@berkeley.edu

U.S. export controls on semiconductors are widely known to be permeable, with the People's Republic of China (PRC) steadily creating state-of-the-art artificial intelligence (AI) models with exfiltrated chips. This paper presents the first concrete, public evidence of how leading PRC AI labs evade and circumvent U.S. export controls. We examine how Chinese companies, notably Tencent, are not only using chips that are restricted under U.S. export controls but are also finding ways to circumvent these regulations by using software and modeling techniques that maximize less capable hardware. Specifically, we argue that Tencent's ability to power its Hunyuan-Large model with non-export controlled NVIDIA H20s exemplifies broader gains in efficiency in machine learning that have eroded the moat that the United States initially built via its existing export controls. Finally, we examine the implications of this finding for the future of the United States' export control strategy.

Dynamic Export Controls and High Speed Innovation

“Notably, NVIDIA limits GPUDirect RDMA to only its data center GPU offerings, excluding clusters built using consumer GPUs. Thus consumer GPUs, including the NVIDIA RTX 4090—common in academic labs—are left to suffer communication overhead that GPUDirect RDMA alleviates in data center GPUs. The limiting of direct peer-to-peer communications is not done in hardware—it is “soft locked” through proprietary NVIDIA drivers. Tiny Corp., a startup developing AI “supercomputers,” reverse-engineered and publicly released custom drivers for the RTX 4090 which enabled peer-to-peer communications in June 2024—opening this soft lock.7 Reporting has shown that China is using RTX 3090 and 4090 GPUs for AI workloads; drivers such as the one released by Tiny Corp. could increase the effectiveness of these bootleg data centers.”

From “Whack-A-Chip”

Skirting Export Controls

1. Stockpiling chips in advance of restrictions.

2. Illegally exporting and acquiring physical chips, including forging documents, diverting shipments, acquiring through third parties or subsidiaries, and otherwise accessing.

3. Renting access or otherwise remotely accessing chips.

Diffusion Rule: A Lesson in Compliance Challenges

In its final weeks, the Biden administration introduced the AI Diffusion rule, an export control regime which placed countries into three tiers of chip access. A country's place in the tiering system was based not just on alliance status, but also on a country's perceived ability and willingness to prevent further diffusion (through re-export or smuggling). This rule proved deeply unpopular. The administration faced backlash from the U.S. tech sector and U.S. allies who saw it as overly burdensome, diplomatically risky, and detrimental to the U.S's advantageous position in the advanced chip marketplace.

Trump Administration AI Governance Activity

Rescission of Biden Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO 14110)

Executive Order Establishing the United States Investment Accelerator (EO 14255), promoting exports of U.S. AI and investment in the U.S.

Executive Order on Advancing United States Leadership in Artificial Intelligence Infrastructure (EO 14141), “The United States can and should lead the world in operation the next generation of AI data centers with clean power”

Launch of “Stargate” AI Infrastructure Initiative with OpenAI, Oracle, and SoftBank

M-25-21: Accelerative Federal Use of AI through Innovation, Governance, and Public Trust

M-25-22: Driving Efficient Acquisition of AI

Three EOs Released Alongside the Action Plan

Promoting the Export of the American AI Technology Stack

Accelerating Federal Permitting of Data Center Infrastructure

Preventing Woke AI in the Federal Government

"The Secretary of Commerce shall issue a public call for proposals from industry-led consortia for inclusion in the Program. The public call shall require that each proposal must:

(i) include a full-stack AI technology package, which encompasses:

(ii) identify specific target countries or regional blocs for export engagement;

(iii) describe a business and operational model to explain, at a high level, which entities will build, own, and operate data centers and associated infrastructure;

(iv) detail requested Federal incentives and support mechanisms; and

(v) comply with all relevant United States export control regimes, outbound investment regulations, and end-user policies, including chapter 58 of title 50, United States Code, and relevant guidance from the Bureau of Industry and Security within the Department of Commerce."

Pillar 3: International AI Diplomacy and Security

Areas of Focus:

Export American AI to Allies and Partners

Counter Chinese Influence in International Governance Bodies

Strengthen AI Compute Export Control Enforcement

Plug Loopholes in Existing Semiconductor Manufacturing Export Controls

Align Protection Measures Globally

Ensure that the U.S. Government is at the Forefront of Evaluating National Security Risks in Frontier Models

Invest in Biosecurity

Pillar 3: International AI Diplomacy and Security

Key Recommendations:

- Department of Commerce to build a “full-stack” AI export program pairing U.S. software, hardware, models, and standards for allied adoption
- Expand export controls on semiconductor subsystems, plug loopholes, align regimes with international partners
- Lead global governance via U.S. led standard-setting and counter Chinese influence in international AI bodies
- Biosecurity measures: federated nucleic acid screening, evaluation of frontier models for CBRN risks

But then…

Nvidia's resumption of AI chips to China is part of rare earths talks, says US

By **Jarrett Renshaw** and **Karen Freifeld**

July 15, 2025 8:29 PM PDT · Updated July 15, 2025

Aa

Trump says Nvidia will hand the U.S. 15% of its H20 chip sales to China

AUGUST 11, 2025 · 1:04 PM ET

US to open up exports of Nvidia H200 chips to China, Semafor reports

By **Reuters**

December 8, 2025 10:35 AM PST · Updated 3 mins ago

Aa

China and the United States' use of export controls: legislation and restrictions, 2010–25

IISS

UNITED STATES

- Expanded export controls on semiconductor equipment, software tools and High Bandwidth Memory (HBM) chips
- 140 Chinese entities added to Entity List
- Semiconductor Manufacturing Equipment FDPR announced
- AI diffusion framework issued
- Tencent and CATL added to CMC List
- 10% tariff increase on all imports from China implemented

DECEMBER · JANUARY · DONALD TRUMP · FEBRUARY

2024 | 2025

CHINA

DECEMBER
- Export Control Law updated, introducing unified control system for dual-use goods and creating 'Watch List' for end-use and end-user verifications
- Export ban on gallium, germanium and antimony implemented with extraterritorial effects
- Anti-monopoly investigation into Nvidia launched
- Seven US companies added to UEL

JANUARY
- Licence requirements for metal exports implemented*
- Anti-trust review against Google launched
- 15% tariffs on coal and liquefied natural gas implemented
- Two US companies added to UEL

FEBRUARY

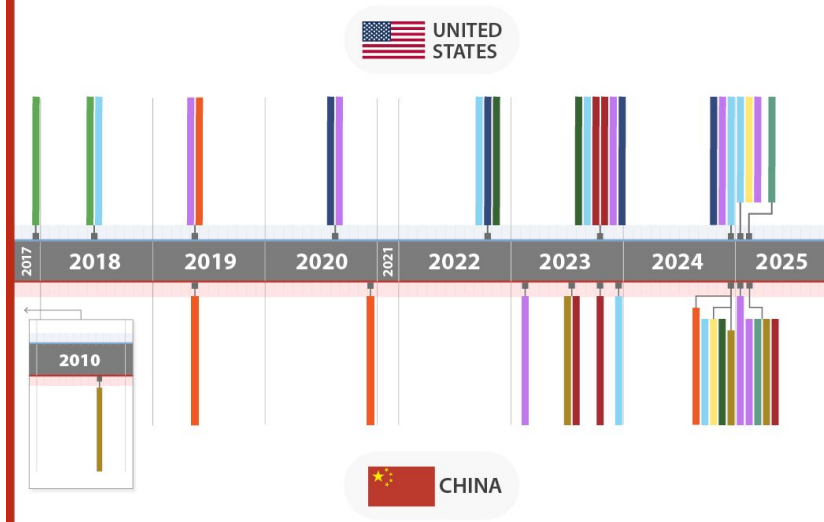
*Tungsten, tellurium, bismuth, molybdenum and indium

Elements of export controls
- Prohibitions
- Export restrictions
- Foreign Direct Product Rule (FDPR)
- Entity Lists/Chinese Military Companies (CMC) List
- Informal statecraft
- Licence requirements
- Legislation
- Extraterritorial measures
- Tariffs
- End-use export restrictions

CHARTING CHINA

Source: IISS China Programme research

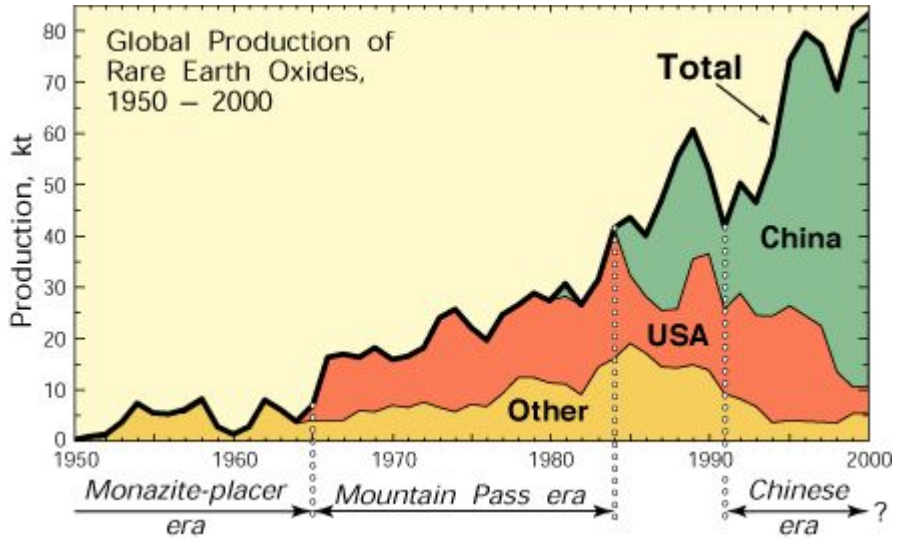
China and the United States' use of export controls: legislation and restrictions, 2010–25

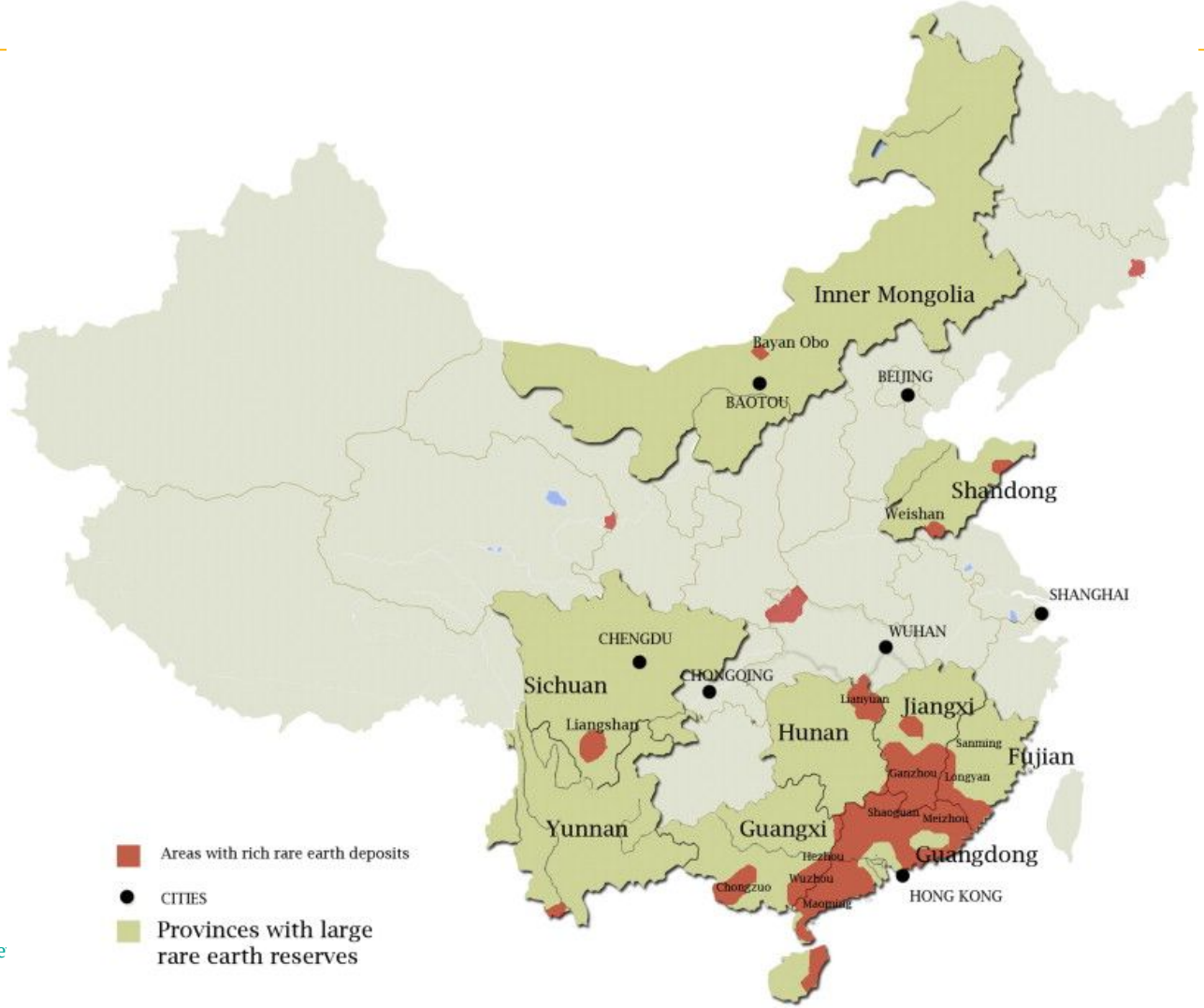


Elements of export controls
Prohibitions
Export restrictions
Foreign Direct Product Rule (FDPR)
Entity Lists/Chinese Military Companies (CMC) List
Informal statecraft
Licence requirements
Legislation
Extraterritorial measures
Tariffs
End-use export restrictions
CHARTING CHINA
Source: IISS China Programme research

China unveils sweeping rare-earth export controls to protect ‘national security’

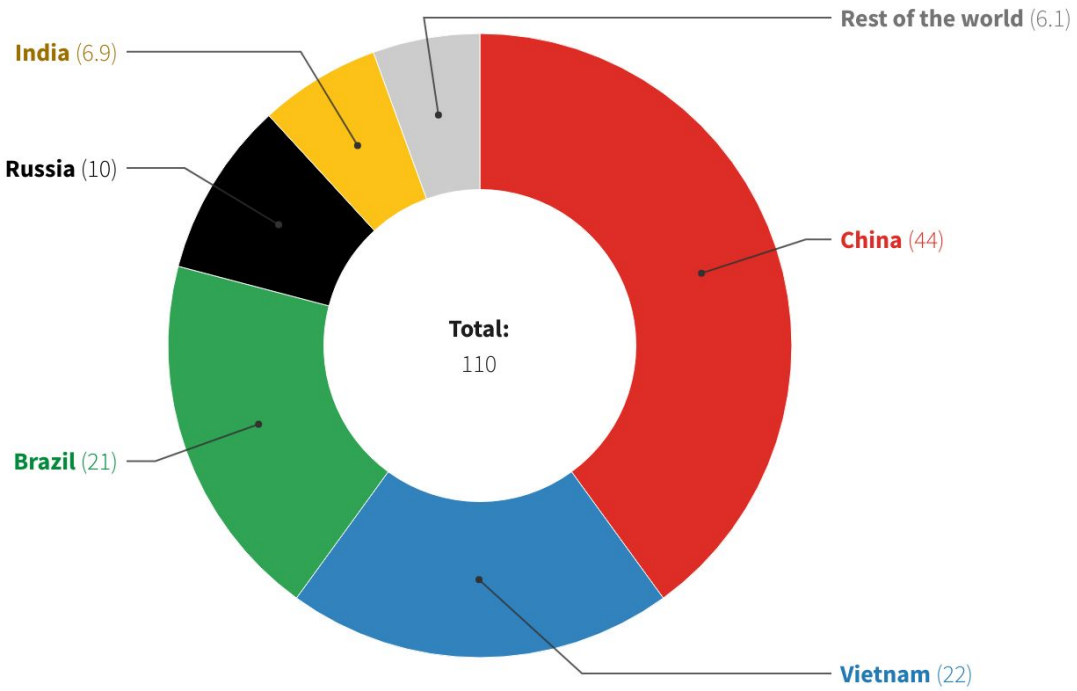
Rules come ahead of expected meeting this month between Donald Trump and Xi Jinping


Global Production of
Rare Earth Oxides,
1950 – 2000
Production, kt
0
10
20
30
40
50
60
70
80
1950
1960
1970
1980
1990
2000
Total
China
USA
Other
Monazite-placer era
Mountain Pass era
Chinese era
?


Inner Mongolia
Bayan Obo
BAOTOU
BEIJING
Shandong
Weishan
SHANGHAI
WUHAN
CHENGDU
CHONGQING
Sichuan
Liangshan
Lianyuan
Jiangxi
Hunan
Sanming
Fujian
Ganzhou
Longyan
Shaoguan
Meizhou
Yunnan
Guangxi
Guangdong
Hezhou
Wuzhou
Chongzuo
Maoming
HONG KONG
Areas with rich rare earth deposits
CITIES
Provinces with large rare earth reserves

Global rare earths deposits

Estimates, in millions of tons of rare earth oxide equivalent

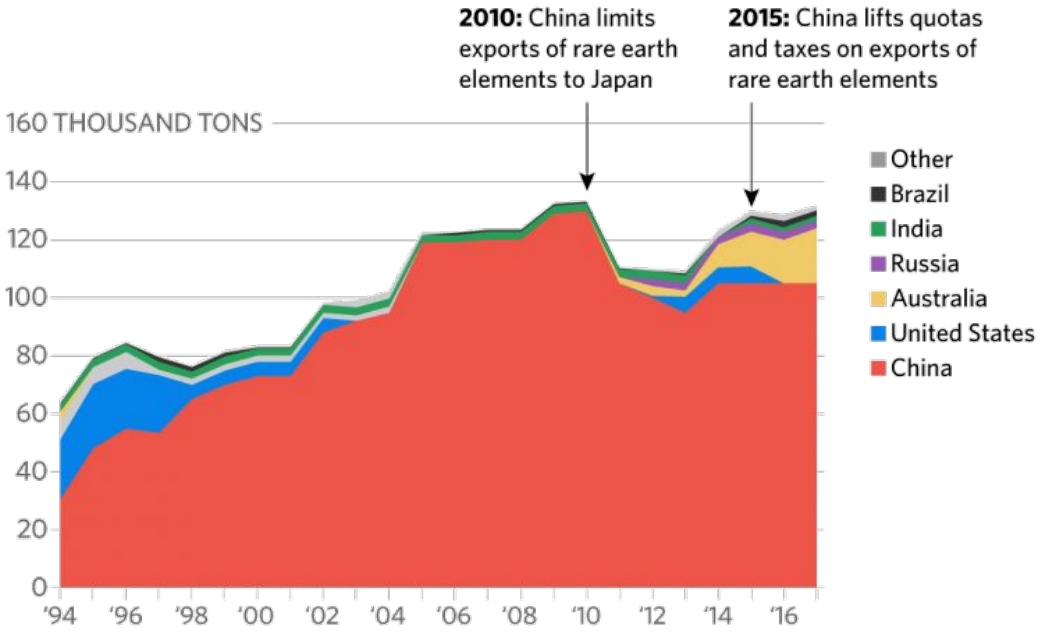


Note: Data include lanthanides and yttrium but exclude most scandium

Source: US Geological Survey, 2024 | By Francesco Guarascio | Reuters, 1 February, 2024

Rare Earth Elements Mines Production

Over the last 30 years, China has solidified its dominance over the global rare earth sector. Looking to move up the value chain and with domestic electric vehicle and renewable consumption increasing, China's domestic consumption of rare earths will only grow. This threatens to reduce China's total exports, but could also tie China more closely to the global market as it seeks more imports, slowly diversifying the market.



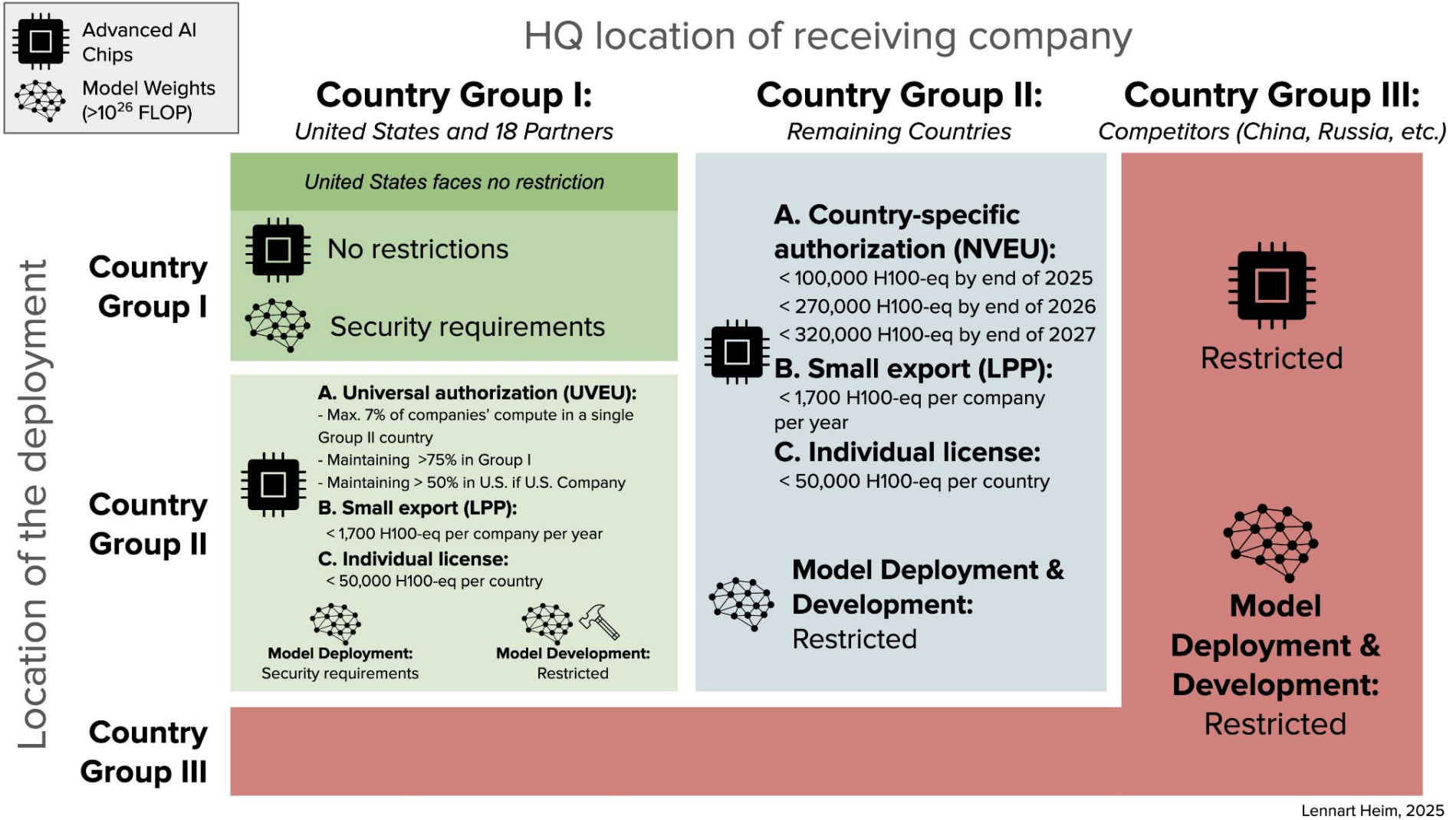
Source: USGS

Copyright Stratfor 2019

Overview of (the now suspended) 9 October 2025 REE trade restrictions

Focus Area	Main Content	Differs from Previous Rules
REE items and licensing requirements	Details export control on certain REE related items. Focus on Er, Eu, Dy, Gd, Ho, Lu, Sc, Sm, Tb, Tm, Y, Yb.	Expands the list of controlled REE elements and formalises licensing and compliance requirements.
Equipment, raw materials, and related items	Licensing for export of REE separation/refining equipment e.g. purification tanks, centrifugal extractors, specialised roasting kilns.	Adds specific equipment to the control list, as well as tighter licensing and reporting requirements tied to rare earth export licence approvals.
REE related items exported overseas	Extends controls to foreign producers using Chinese origin REEs or technologies. Introduces 0.1% de minimis and 50% affiliate thresholds.	Controls now reach across international rare earth supply chains.
REE related technologies	Controls REE extraction, separation, magnet-making, and recycling technologies. Applies to technical assistance and IP transfer.	First explicit control on REE technologies. Previous rules mainly focused on the commodities.

DATA: CRU REE Special Report 2025, Ministry of Industry and Information Technology China



Lennart Heim, 2025

Companies in the Crosshairs

Leah Walker
Executive Director, Berkeley Risk and Security Lab

BERKELEY RISK & SECURITY LAB

How the Administration is Engaging AI Companies

Deregulation to Accelerate Innovation

- Rolled back Biden-era AI requirements viewed as burdensome to industry.
- Emphasis on reducing barriers for AI development and deployment.

Public–Private Partnership Model

- Government increasingly collaborates with leading AI firms rather than relying on heavy regulation.
- AI companies are viewed as strategic partners for national security, scientific research, and economic growth.
- Federal initiatives leverage private-sector models, infrastructure, and expertise.

Building National AI Infrastructure

- Support for rapid expansion of data centers, compute capacity, and energy infrastructure.
- Policies designed to facilitate large-scale AI infrastructure investment by industry.

AI as a Geopolitical Tool

- AI policy framed as a competition with strategic rivals, especially China.
- Government seeks to export U.S. AI technology, standards, and platforms to allies.
- AI firms become instruments of broader U.S. technological and diplomatic influence.

Security Oversight for Frontier Models

- While generally pro-growth, the administration has increased scrutiny of frontier AI models with cybersecurity or national-security implications.
- Uses voluntary reviews, export controls, and security partnerships to manage high-risk capabilities.

Fin