



| Flash |

U.S.-Led Trade Restrictions Likely to Increase Espionage Threat

F-2024-07-18a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Malware, Vulnerability, Geopolitical & Physical, Threat Actor Targeting

July 18, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on July 18, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | U.S.-Led Trade Restrictions Likely to Increase Cyber Espionage Threat

> Key Findings

- Some of the world's largest technology companies and global stock markets plummeted in value on July 18, likely because the United States is seeking to enforce a rarely-used rule allowing it to prohibit sales of any foreign-made product with at least some U.S.-made materials to China.
- Restricting access to advanced technologies will likely put China at a competitive disadvantage when it comes to producing emerging technologies vital to its trade-based economy, as well as weapons systems needed for national security.
- China is very likely to retaliate with its own trade restrictions against companies and states that comply with the U.S. restrictions.
- Chinese-backed cyber threat actors are very likely to increase cyber espionage against entities that produce the withheld technology with the goal of creating its own endogenous industries.

| Background

U.S.-Led Trade Restrictions

In September 2022, President Biden announced new export control rules known as the CHIPS and Science Act (CHIPS Act) that limit China's access to advanced computer chips.¹

- The consequential legislation prohibits not only U.S. companies but also major U.S. allies that produce advanced semiconductor technology and count China as one of their main customers—like Taiwan, South Korea, Japan, and the Netherlands—from selling the most sophisticated forms of the technology and the equipment used to make it to China.²
- China likely does not possess the advanced semiconductor technology that goes into the state-of-the-art computer and weapons systems, and it could take years for China to develop its own endogenous systems.³

Since its passage, the United States has announced new measures that aim to close loopholes in the original law. In mid-July 2024, media reports emerged that the United States was considering enacting new measures, including enforcing the foreign direct product rule (FDPR) on companies that continue to sell semiconductor chip-making equipment to China.⁴ The FDPR allows the United States to impose restrictions on foreign-made products that use even small amounts of U.S. technology. The United States is considering enforcing FDPR on Japanese and Dutch companies in particular, which continue to sell prohibited technology to China, but this could impact a wide swath of some of the world's largest companies.

¹

[hXXps://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file](https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file)

² [hXXps://ajot.com/news/us-chip-gear-makers-told-to-wait-for-relief-from-china-curbs](https://ajot.com/news/us-chip-gear-makers-told-to-wait-for-relief-from-china-curbs)

³

[hXXps://www.project-syndicate.org/commentary/us-semiconductor-sanctions-china-technology-war-by-carl-bildt-2022-10](https://www.project-syndicate.org/commentary/us-semiconductor-sanctions-china-technology-war-by-carl-bildt-2022-10)

⁴

[hXXps://www.bloomberg.com/news/articles/2024-07-17/us-considers-tougher-trade-rules-against-companies-in-chip-crackdown-on-china](https://www.bloomberg.com/news/articles/2024-07-17/us-considers-tougher-trade-rules-against-companies-in-chip-crackdown-on-china)

| Details

Valuations of some of the world's largest technology companies and global stock markets plummeted following the reports.

- The Netherlands' ASML and Japan's Electron had the biggest valuation drops (by 10 percent) following reports that their continued sales to China are behind the possible FDPR enforcement.⁵
- There were also major slumps for U.S. companies like NVIDIA (-6.6 percent),⁶ which at times in 2024 was the world's most valuable company, and other technology companies that rely on or sell semiconductor chips, which is a USD 530 billion annual business.⁷ Taiwan Semiconductor Manufacturing Company (TSMC), which produces 90 percent of the world's most sophisticated chips, was also impacted.⁸

Companies impacted by the new restrictions have complained that they will limit the availability of semiconductor supplies by reducing revenue, which hinders semiconductor research and development.

- In the second quarter of 2024, half of ASML's revenue came from sales to China.⁹ The new rules would significantly impact those sales by limiting ASML's ability to sell its most advanced chip-making equipment to China.
- South Korea's Samsung, Taiwan's TSMC, NVIDIA, and Foxconn are among the largest companies in the world, have similar revenue dependencies on China, and have been reluctant to adhere to the restrictions. NVIDIA saw its sales to China go from 22 percent to 9 percent of its business in a year.¹⁰

⁵

[hXXps://www.marketwatch\[.\]com/amp/story/asml-shares-under-pressure-as-u-s-reportedly-considers-new-export-controls-e2e63010](https://www.marketwatch.com/amp/story/asml-shares-under-pressure-as-u-s-reportedly-considers-new-export-controls-e2e63010)

⁶ [hXXps://www.bbc\[.\]com/news/articles/c7241](https://www.bbc[.]com/news/articles/c7241)

⁷

[hXXps://www.semiconductors.org/global-semiconductor-sales-decrease-8-2-in-2023-market-rebounds-late-in-year/](https://www.semiconductors.org/global-semiconductor-sales-decrease-8-2-in-2023-market-rebounds-late-in-year/)

⁸

[hXXps://www.forbes\[.\]com/sites/siladityaray/2024/07/17/major-chip-stocks-slump-after-biden-reportedly-considers-more-restrictions-on-sales-to-china/](https://www.forbes[.]com/sites/siladityaray/2024/07/17/major-chip-stocks-slump-after-biden-reportedly-considers-more-restrictions-on-sales-to-china/)

⁹ [hXXps://qz\[.\]com/biden-weighs-trade-rules-block-chipmaking-exports-china-1851596265](https://qz[.]com/biden-weighs-trade-rules-block-chipmaking-exports-china-1851596265)

¹⁰ [hXXps://s201.q4cdn\[.\]com/141608511/files/doc_financials/2025/q1/NVIDIA-10Q-20242905.pdf](https://s201.q4cdn[.]com/141608511/files/doc_financials/2025/q1/NVIDIA-10Q-20242905.pdf)

- There have been reports that the prohibited technology is still making its way to China despite the new restrictions. In early October 2023, Taiwan launched an investigation into four Taiwanese companies for cooperating with China's Huawei Technologies Co.¹¹

Enforcing FDPR could result in diplomatic tensions between the United States and its allies—in the Netherlands in particular, as ASML is the largest company in all of Europe.¹² Such tensions could lead to widespread non-compliance with the CHIPS Act. China would likely welcome this outcome and has attempted to use its close trade ties with the European Union to create divisions with the United States in other areas, like trade tariffs for Chinese-made electric vehicles (EVs).¹³

| Forward Look

China is likely to retaliate with its own trade restrictions against countries enforcing elements of the CHIPS Act. China has a similar dominance of rare-earth metals, which are used in advanced technologies like EVs, solar panels, smartphones, and even semiconductors.

- In December 2023, China announced new export controls on a range of products, including laser radars, drones, and biotechnology.¹⁴ Most importantly, the restrictions include a ban on technology used to extract, separate, and process rare-earth metals.¹⁵
- On October 20, 2023, China announced a partial export ban on some graphite products, days after updates to the CHIPS Act made by the United States restricting sales of chips used in artificial intelligence (AI). China is the world's top

¹¹

[hXXps://asia.nikkei\[.\]com/Spotlight/Huawei-crackdown/Taiwan-to-probe-4-firms-accused-of-helping-Huawei-build-chip-plants](https://asia.nikkei.com/Spotlight/Huawei-crackdown/Taiwan-to-probe-4-firms-accused-of-helping-Huawei-build-chip-plants)

¹²

[hXXps://www.euronews\[.\]com/business/2024/07/18/asml-shares-plunge-as-geopolitics-overshadow-strong-earnings](https://www.euronews.com/business/2024/07/18/asml-shares-plunge-as-geopolitics-overshadow-strong-earnings)

¹³ [hXXps://www.cnn\[.\]com/2024/07/17/eu-countries-divided-on-chinese-ev-tariffs-in-vote-reuters-reports.html](https://www.cnn.com/2024/07/17/eu-countries-divided-on-chinese-ev-tariffs-in-vote-reuters-reports.html)

¹⁴

[hXXps://www.scmp\[.\]com/news/china/diplomacy/article/3245924/china-brings-new-export-controls-hi-tech-products-amid-ongoing-rivalry-us](https://www.scmp.com/news/china/diplomacy/article/3245924/china-brings-new-export-controls-hi-tech-products-amid-ongoing-rivalry-us)

¹⁵ [hXXps://www.mining\[.\]com/web/china-bans-export-of-rare-earth-processing-tech-over-national-security/](https://www.mining[.]com/web/china-bans-export-of-rare-earth-processing-tech-over-national-security/)

graphite producer, with the United States, South Korea, and Japan among the top importers.¹⁶

- Days later, China announced a tax investigation into Foxconn operations inside China.¹⁷ Foxconn is a Taiwanese-based company and one of the world's largest electronics manufacturers; it is known for building iPhones. Foxconn also has countless ongoing partnerships with semiconductor producers, led by TSMC.
- In July 2023, China announced bans on the export of gallium and germanium—key metals needed in the production of semiconductors.¹⁸

Espionage Aimed at Semiconductor Producers

ZeroFox reporting since the first iteration of the CHIPS Act in 2022 has warned against cyber espionage campaigns as the amount of technology withheld from China grows.

- In mid-October 2023, ZeroFox identified recent instances of possible Chinese state-sponsored threat actors conducting cyber espionage campaigns against semiconductor firms in Taiwan, Hong Kong, and Singapore. The aim of the campaigns is to provide sensitive data on semiconductor production back to the Chinese Communist Party (CCP) so that it can be replicated. This activity was attributed to Chinese advanced persistent threat (APT) group APT27 due to the overlap in tactics, techniques, and procedures (TTPs). Specifically, the use of a HyperBro malware¹⁹ variant to install Cobalt Strike beacons within a TSMC PDF in a phishing lure correlates to APT27's known TTPs.²⁰
- On October 17, 2023, intelligence officials from the United States, United Kingdom, Canada, Australia, and New Zealand (the Five Eyes) accused China of launching hacking and espionage attempts to steal trade secrets on everything from quantum technology and robotics to biotechnology and AI.²¹

¹⁶ [hXXps://asia.nikkei\[.\]com/Economy/Trade/China-to-curb-exports-of-key-EV-battery-material-from-Dec.-1](https://asia.nikkei.com/Economy/Trade/China-to-curb-exports-of-key-EV-battery-material-from-Dec.-1)

¹⁷ [hXXps://www.rfi\[.\]fr/en/international-news/20231023-taiwan-defends-foxconn-over-china-tax-probe](https://www.rfi[.]fr/en/international-news/20231023-taiwan-defends-foxconn-over-china-tax-probe)

¹⁸

[hXXps://www.reuters\[.\]com/world/china/china-exported-no-germanium-gallium-aug-due-export-curbs-2023-09-20/](https://www.reuters.com/world/china/china-exported-no-germanium-gallium-aug-due-export-curbs-2023-09-20/)

¹⁹ [hXXps://attack.mitre\[.\]org/software/S0398/](https://attack.mitre[.]org/software/S0398/)

²⁰ [hXXps://attack.mitre\[.\]org/groups/G0027/](https://attack.mitre[.]org/groups/G0027/)

²¹

[hXXps://www.reuters\[.\]com/world/five-eyes-intelligence-chiefs-warn-chinas-theft-intellectual-property-2023-10-18/](https://www.reuters.com/world/five-eyes-intelligence-chiefs-warn-chinas-theft-intellectual-property-2023-10-18/)

ZeroFox assesses that the global semiconductor industry will very likely continue to be targeted by Chinese APT groups. Cyber espionage attempts will most likely come in the form of spyware and info stealers to extract intellectual property (IP) from U.S.-based companies. The aim will be to remain undetected for as long as possible. Firms in Taiwan, South Korea, Japan, the United States, and Europe are likely to be targeted since they have the most advanced semiconductor manufacturing capabilities and a large share of IP. Verticals of the semiconductor industry—such as prominent universities and government research labs specializing in semiconductor research and development—are also likely to be targeted. In particular, these APT groups are likely to use bespoke tooling and exploit critical and widespread vulnerabilities in future cyber espionage campaigns targeting the global semiconductor industry.

| Recommendations

- Implement effective email protection solutions to mitigate phishing campaigns.
- Conduct training and awareness for employees to recognize phishing emails.
- Implement multi-factor authentication (MFA) to prevent unauthorized access to sensitive information (in the event that credentials are compromised).
- Develop and implement an effective incident response plan (IRP).
- Conduct continuous scanning and monitoring of attempted port scans, vulnerabilities, and suspicious activity on devices.
- Implement an effective anti-virus (AV) solution.

Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

Sources may use

TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

Amber

Sources may use

TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW MAY IT BE SHARED?

Recipients may NOT share

TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may ONLY share

TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP:AMBER+STRICT restricts sharing to the organization only.

Green

WHEN SHOULD IT BE USED?

Sources may use

TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Clear

Sources may use

TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW MAY IT BE SHARED?

Recipients may share

TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Recipients may share

TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%