THE PEOPLE’S REPUBLIC OF CHINA USES DIVERSE TOOLS TO ACCESS FOREIGN TECHNOLOGY AND CRITICAL INFRASTRUCTURE

THE PRC USES LEGAL AND ILLEGAL METHODS TO OBTAIN UNSANCTIONED ACCESS TO TARGETED TECHNOLOGY AND CRITICAL INFRASTRUCTURE.

- The PRC has a large “toolkit” it can use—often employing several tools at once.
- PRC methods continually evolve to evade or bypass other countries’ legal and regulatory measures.
- When one method of technology acquisition fails, PRC actors will pursue another.
- The PRC can use these methods to impede supply chains by limiting exports from PRC manufacturers, taking control of overseas manufacturers, or hampering business operations.

WHAT TOOLS DOES THE PRC EMPLOY TO ACCESS FOREIGN TECHNOLOGY AND INFRASTRUCTURE?

China’s activities can be categorized into 5 B’s.

BUYING TECHNOLOGY:
PRC firms purchase weapons, equipment, parts, or technology from foreign sellers.

BOOSTING TALENT:
PRC programs encourage foreign talent acquisition and joint research collaboration.

BARGAINING FOR MARKET ACCESS:
The PRC makes legal and regulatory demands on foreign companies operating in China, including handing over their technology. PRC actors may access other countries’ infrastructure by offering funding through international institutions.

BURGLARIZING TECHNOLOGY:
The PRC uses cyber-actors or traditional intelligence collection methods to steal technology or illegally access infrastructure.

BETTING ON INVESTMENTS:
PRC actors invest in foreign firms, create joint ventures, take over foreign firms, and leverage investment funds or venture capital to access emerging technology.
PRC ACTIONS TO ACCESS FOREIGN TECHNOLOGY AND INFRASTRUCTURE FOLLOW A COMMON PATTERN

PRC national guidance provides insights into the types of technologies and infrastructure that the PRC is likely to target. This guidance is then turned into action by government organizations, companies, and individuals through a series of observable steps. Case studies below illustrate this process.

SONOBUOYS

Hydrophones and sonobuoys are key technologies that could help the PLA improve its antisubmarine warfare (ASW) capabilities. In 2014, a PRC national created an intermediary front company, LinkOcean Technologies, to acquire underwater technologies. LinkOcean exported hydrophones from the United States to the PRC without obtaining the required export licenses. End-users were concealed from the US manufacturer and illegally exported products were provided to two PRC universities that are closely associated with the PLA. In 2021, this individual was convicted of money laundering, making false statements, smuggling, and conspiracy to violate US export control laws.

UNDERSEA CABLES

Pacific Island nations have substantial unmet needs for internet connectivity. In 2018 the World Bank and Asian Development Bank agreed to fund the East Micronesia Cable project to connect the Federated States of Micronesia (FSM), Kiribati, and Nauru. The cable would have joined to the HANTRU-1 trunk, which links Guam and the Marshall Islands and may carry sensitive US military communications. Huawei Marine Networks, a PRC firm now on the US Entity List, won the project with a very low bid. World Bank projects may not disqualify bids on criteria other than price unless they have been specified in advance. In 2021 the three recipient nations withdrew from the World Bank project.

FROM NATIONAL GUIDANCE TO TARGETED TECHNOLOGY

<table>
<thead>
<tr>
<th>PRC government issues Five-Year Plans calling for deep sea mapping, maritime monitoring, and related capabilities.</th>
<th>PRC National Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRC incentivizes individuals to buy, invest in, or steal technologies to improve ASW capabilities.</td>
<td>PRC Tools &amp; Incentives</td>
</tr>
<tr>
<td>PRC actors seek access to US-made military hydrophones and sonobuoys that monitor underwater acoustics.</td>
<td>Foreign Targets (technology, companies, individuals, governments)</td>
</tr>
<tr>
<td>PRC national creates front company to circumvent US export control laws.</td>
<td>Target Nation Response</td>
</tr>
<tr>
<td>US DOJ arrests PRC national for illegally exporting US goods to PLA-affiliated universities. At least $100,000 worth of tech had already been transported to the PRC.</td>
<td>Outcome</td>
</tr>
</tbody>
</table>

Many of China’s Activities Occur in Plain Sight.
PROTECT YOUR TECH BY KNOWING WHAT TO LOOK FOR!

For additional information, please contact: chinastudies@cna.org
For additional CNA work on this topic, see: https://www.cna.org/centers/cna/cip/economic-statecraft

This work was performed under Federal Government Contract No. N00014-16-D-5003. This document contains the best opinion of CNA at the time of issue. The views, opinions, and findings contained in this report should not be construed as representing the official position of the Department of the Navy.