Impacts of the BIOSECURE Act on the Global BioTech Industry

TLP:WHITE This report may be shared without restriction. For Health-ISAC Members be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Health-ISAC™ Collaborating for Resilience in Healthcare | CyberCX | RANE Risk Assistance Network + Exchange

health-isac.org

Key Judgements

- If the BIOSECURE Act is signed into law, it will make Western biotech R&D particularly inaccessible to Chinese companies, placing biotech R&D organizations at higher risk of espionage in the years following BIOSECUE Act adoption.
- BioTech research and multiomic data are strategic assets for multiple adversarial nations, placing the biotech industry in the crosshairs of state-sponsored espionage groups from all around the world after the BIOSECURE Act bill is passed.
- The BIOSECURE Act will force many US companies to shift their supply chains away from both blacklisted Chinese suppliers, as well as unlisted Chinese suppliers that are at risk of being blacklisted in the future.
- While pharmaceutical companies in Western nations are positioned to take advantage of new market opportunities created from the BIOSECURE Act, but the change in supply chains will likely disrupt contract manufacturing in the short term.
- China is likely to retaliate against the BIOSECURE Act with potential export restrictions.

Biotechnology, Research and Multiomic Data as a Target

In September 2024, the BIOSECURE Act was passed by the US House of Representatives and passed to the Senate, where it was deferred to the Committee on Homeland Security and Governmental Affairs. If passed, the BIOSECURE Act will prohibit federal funded entities from using biotechnology from a company associated with a foreign adversary where there are risks to national security stemming from research or multiomic data collection. Biotechnology is a high value target for strategically, economically and commercially motivated threat actors. The Health-ISAC Threat Operations Center and CyberCX Intelligence assess there are three key angles to understanding biotechnology as a target.

1 | Capabilities

While there are many positive applications of biotechnology, many of these technologies are dual use and could be used for hostile and/or military purposes by foreign adversaries.

Case Snippet 1

In August 2024, the US House China committee submitted a letter to the Food and Drug Administration (FDA) claiming that US biopharmaceutical companies conducted clinical trials with China's military organizations, specifically with medical centers and hospitals affiliated with the People's Liberation Army (PLA), for over a decade. The US House China Committee also raised concerns about US pharmaceutical organizations conducting clinical trials with hospital infrastructure located in Xinjiang, where the Chinese Communist Party (CCP) is alleged to have engaged in significant human rights abuses.[1]

2 | Research & Intellectual Property (IP)

Research, development and IP related to emerging and innovative biotechnology is of high interest to foreign adversaries seeking to establish market dominance, like China. China is dominant in biotechnology supply chains, with some studies indicating that up to 79% of biopharmaceutical and biotechnology organizations are engaged with a Chinese contract manufacturing organization or contract development and manufacturing organization.

As seen through the COVID-19 vaccine "IP war", foreign adversaries, including China, Russia, North Korea and Iran conducted cyber-enabled espionage to steal vaccine research, with the overall view of extending geopolitical power by being the first to present a solution to the pandemic.

1. https://www.documentcloud.org/documents/25052080-81924-fda-letter-on-pla-trials?responsive=1&title=1

The risk to research and development (R&D) elements of biotech companies in the event that the BIOSECURE Act becomes law may be compounded by its synergy with existing regulatory measures that distance Western and Chinese technological innovation. In 2022, the United States banned the exports of certain advanced semiconductors to China.[2] Then, in 2023, the US signed the CHIPS and Science Act, incentivizing US companies to manufacture advanced semiconductors in the US, away from China which further separated the two R&D markets.[3] The BIOSECURE Act would make Western R&D in biotech especially inaccessible to Chinese companies, potentially resulting in increased espionage activity.

Case Snippet 2

In July 2020, the US Department of Justice indicted two Chinese nationals for a 10-year cyber-enabled espionage campaign targeting high tech industries in the US, Australia, Belgium, Germany, Japan, Lithuania, the Netherlands, Spain, South Korea, Sweden and the UK. The Chinese nationals were allegedly working with the Guangdong State Security Department and the Ministry of State Security. The Chinese nationals had been identified probing for vulnerabilities in computer networks of companies developing Covid-19 vaccines, testing technology, and treatments.

3 | Multiomic data

Multiomics combines unique, highly sensitive data, such as genomic data, to identify associations between biological entities and discover novel treatments. While providing significant benefits, multiomics can also present significant risks and be abused for malicious purposes. Multiomic data could be targeted by threat actors seeking to gain a competitive advantage, including nation-states seeking market dominance and establish itself as a global leader in the field. Additionally, multiomic data can be used to conduct intelligence operations abroad, particularly to target perceived "diaspora" communities living in other countries. Finally, it is plausible that malicious actors could use multiomic data to create pathogens and toxins intended to cause harm.

Spotlight on: China

Biotechnology and pharmaceuticals is a highly strategic industry for China. China's 14th Five Year Plan (145YP)—a key driver of Chinese nation-state espionage activity—explicitly calls out innovation in health and biomedicine as a key priority. Since at least 2012, biotech and pharmaceuticals have been a major part of its Five Year Plans. Biotechnology and pharmaceuticals are also key parts of Made in China 2025 and Health China 2030. Made in China 2025 aims to increase the domestic development and production of biopharmaceuticals to 25 percent in 2020 and to 45 per cent by 2025. Further, China's unique regulatory environment can compel organizations in China, including those not owned by the state, to share data with the CCP under its National Intelligence Law. This law states that Chinese citizens must act in the interest of active national intelligence objectives when called on. Health-ISAC explored the national security implications of the Chinese National Intelligence Law and other covert tools of pressure in a joint public-private sector analysis on obscure tools of Chinese economic competition, available here.

China views multiomic data as a strategic commodity needed to inform its security and economic priorities. For over a decade, China has collected large healthcare data sets, including multiomic data, from organizations globally through both legitimate arrangements and illegal operations. Due to the uniqueness of multiomic data, it can significantly enhance Chinese intelligence's ability to precisely conduct surveillance, blackmail or interference against intelligence targets in government and strategic industries globally. The CCP has also gradually increased surveillance of citizens through biometric technologies, attracting significant ethical and human rights concerns. Chinese nation-state actors have targeted healthcare organizations globally in cyber-enabled espionage.

2. https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/
3. https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/
4. https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

Case Snippet 3

In September 2022, the US Department of Health and Human Services reported on a Chinese nation-state actor, APT41, targeting sectors including healthcare since at least 2014. This included an incident in May 2015, in which APT41 targeted a biotechnology company undergoing acquisition, exfiltrating clinical trials data of developed drugs, academic data, and R&D funding-related documents.

However, the threats are not just external. China has demonstrated intent and capability to implant malicious hardware and backdoors in technology supply chains to facilitate espionage for over a decade, enabled by extrajudicial legislation and a lack of separation between industry and government. Chinese intelligence is known to adopt the use of front companies to obfuscate their activities, demonstrating the importance of effective due diligence and risk management across biotechnology supply chains.

Case Snippet 4

In September 2024, the New Zealand Security Threat Environment 2024 report provided insights into how Chinese intelligence uses complex and deceptive front organizations to connect with community groups in New Zealand, as well as to steal IP or covertly purchase it without disclosing the real end user.[5]

Spotlight on: Disruption

Some nation-state actors have demonstrated intent and capability to embed disruptive and/or destructive functions in multi-use technologies, including those used in healthcare settings globally. Like Chinese nation-state actors, other foreign intelligence apparatuses are known to use front companies and highly obfuscated supply chains to conduct covert operations.

Case Snippet 5

In September 2024, pagers and radios exploded in Lebanon and Syria, killing at least 37 people and injuring thousands of civilians, Hezbollah members and the Iranian Ambassador to Lebanon. Former Israel and Western security officials disclosed the attacks were part of an elaborate, decade-long effort to penetrate Hezbollah. Components of the exploded devices have been linked through Taiwanese manufacturer, Gold Apollo, to suspected Hungarian shell company, BAC Consulting KFT. Preliminary investigations indicated that Gold Apollo had sent 254 pagers to Hungary and earned $15 for each pager sold by BAC.

Other forms of disruption, like economic coercion, are common retaliatory measures used by foreign adversaries. For instance, China is known to apply economic coercion, like tariffs, in response to adverse economic and geopolitical decisions made by Western governments.

Assessment of Impacts of the BIOSECURE Act on Commercial BioTech Entities

Global Trade Landscape

The BIOSECURE Act will drive a wedge in global pharmaceutical supply chains as US companies will need to reduce their ties with Chinese counterparts, disrupting supply chains and forcing companies to begin implementing mitigation strategies as soon as possible. On September 9, the US House of Representatives passed the BIOSECURE Act, which aims to restrict US businesses from working with Chinese biotechnology companies due to national security concerns, sending the legislation to the Senate, which has already been working on its own version of the legislation.

5. https://www.nzsis.govt.nz/assets/NZSIS-Documents/New-Zealands-Security-Threat-Environment-2024.pdf

While the bill easily passed in the House with bipartisan support in a 306-81 vote, there is more significant opposition to the bill due to its impact on innovation and the pharmaceutical industry in the Senate. While some version of the BIOSECURE Act is likely to eventually become law, the current House version will face difficulty in passing as a standalone bill before the end of the current legislative session that ends on Jan. 3, 2025. Instead, if the bill is passed this year, it is likely to be done so by being attached to the annual must-pass National Defense Authorization Act. Still, the House version of the bill is likely to be the version closest to the final version of the bill passed through Congress.

BioTech Companies Are Heavily Incentivized to Cut Ties with the Chinese Market

The BIOSECURE Act leverages the US federal government's contracting and research granting roles to effectively force companies to choose between working with the US government or targeted Chinese biotechnology companies. The act prohibits the US government from entering a contract with any entity, regardless of whether it is a US or foreign company, that (a) uses biotechnology equipment or services provided by a biotechnology company of concern or (b) has entered a contract that uses such equipment or services with a biotechnology company of concern. The BIOSECURE Act defines a "biotechnology company of concern" as an entity that is subject to control or operates on behalf of a US foreign adversary (such as China, Russia, North Korea and Iran), is involved in the biotechnology equipment or service industry and carries out research or services with a foreign adversary's military, internal security or intelligence agencies. Furthermore, the House version BIOSECURE Act explicitly says that five Chinese companies – BGI (formerly Beijing Genomics Institute), Complete Genomics, MGI, WuXi AppTec and WuXi Biologics – are biotechnology companies of concern. The bill requires the Office of Management and Budget to publish a list of additional companies of concern and annually update the list. The Senate version of the bill excludes WuXi Biologics, but its association with WuXi AppTec makes it a likely candidate to be affected nonetheless and/or included in the additional list of companies if the final version of the bill still excludes it. Finally, the bill broadly defines biotechnology equipment or services.

A Lengthy Amnesty Period

Once the BIOSECURE Act is signed into law there will be a long phase-in period and the House's version does provide a safe harbor and limited waiver process. The BIOSECURE Act tries to limit immediate impact to pharmaceutical and biotechnology supply chains. The House version of the bill includes a grandfather clause for existing contracts signed before the act's effective date to remain in place until Jan. 1, 2032. The Senate version includes a grandfather clause that does not expire. The House's version also includes a safe harbor mechanism that excludes equipment or services that were formerly but no longer provided by a blacklisted biotechnology company. There is also a waiver process that allows the prohibitions to be waived when providing overseas services (such as in China).

The BIOSECURE Act Will Transform Supply Chains Across the World

Changes in Upstream Supply Chain Entities

The BIOSECURE Act is already forcing US companies to make changes to their long-term supply chain strategies, but China's competitors in the United States, Europe, India and South Korea are all likely to benefit from the BIOSECURE Act as alternative suppliers. China and the five listed companies play a key role in the global biotechnology industry. Estimates vary widely, but Chinese active pharmaceutical ingredients (APIs) are believed to account for 15 to 20% of total US imports of APIs; even though India is also a major alternative, and likely beneficiary of the bill, about 75% of the intermediates used to make APIs in India come from China.

A survey earlier this year by the Biotechnology Innovation Organization, which opposes the BIOSECURE Act, found that 79% of biopharmaceutical and biotechnology companies have a product or contract with a Chinese contract manufacturing organization (CMO) or contract development and manufacturing organization (CDMOs). WuXi AppTec and WuXi Biotech in particular commonly partner with US biotechnology companies and would cause the most significant impact if they are included in the final list. Even prior to the bill's passage, many companies across the globe are already looking to adjust their supply chains. A July survey by life sciences consulting firm LEK found that 26% of life science companies were looking to shift away from their Chinese partners and that 16% would only consider non-Chinese partners going forward.

Operational Concerns of Restructuring Existing Supply Chains

The process of adjusting supply chains is likely to be difficult for companies despite the bill's long grandfather clause. Shifting away from WuXi AppTec is likely to be difficult as the company alone is estimated to be involved in the production of a quarter of drugs used in the United States. It is a major CDMOs and has 12 facilities in the United States that could be shuttered or sold due to the passage of the BIOSECURE Act. In the short-to-medium term, there is likely to be a decline in CDMO capacity, which could push up prices, due to companies winding down contracts with WuXi ahead of 2032 and disruptions to operations at its US plants. Replacing lost capacity cannot be done quickly given the long permitting and design process used in the pharmaceutical industry. Shifting supply chains for drugs would often trigger the US Food and Drug Administration's qualification and validation process, which takes a long time. The BIOSECURE Act also complicates R&D efforts with Chinese CDMOs and Chinese researchers. While US companies and researchers would still be allowed to work with non-listed Chinese entities, the due diligence process to ensure that the Chinese counterparty does not include a listed entity will be complex and costly.

Possible Retaliation Against the BIOSECURE Act

China is likely to retaliate against the passage of the BIOSECURE Act, likely at first with limited export controls, though the scale of pressuring Western companies' operations in China depends on how restrictive the US waiver process is. Given the significant impact the BIOSECURE Act will have on the pharmaceutical industry and Chinese pharmaceutical companies, which will lose significant market share overseas, the Chinese government will be compelled to retaliate against the US pharmaceutical industry. However, China's retaliation is likely to be measured and attempt to not accelerate the US campaign against its pharmaceutical industry and companies exiting China. This means that initial focus is likely to be on limited export controls targeting a small set of pharmaceutical products or blacklisting a US pharmaceutical company that has limited operations in China rather than one China's health care industry is dependent on. What remains to be seen is how US agencies would implement the BIOSECURE Act's waiver clause for overseas health care services in China. If the United States expansively approves such waivers, then many US companies will still look at China as a major market to sell into, even if they are building parallel supply chains to supply the US and Chinese market differently. By contrast, if the United States rarely approves such waivers, then US companies will largely exit the Chinese market and this could lead Beijing to more aggressively target companies and businesspeople in China with both formal legal tools, such as carrying out a formal product safety reviews, and irregular tools, such as raiding corporate offices and manufacturing facilities.

Recommendations to Minimize Potential BIOSECURE Act Impacts

With the BIOSECURE Act likely to pass and disrupt pharmaceutical supply chains and research and development, pharmaceutical and biotechnology companies should immediately begin preparing. Here are some recommendations for actions companies can take today:

- Develop a corporate response plan and team that includes representatives from relevant departments to oversee BIOSECURE Act compliance measures and protocols, as well as the creation of risk mitigation strategy options.
- Evaluate existing supply chains to identify where, if any, they rely on equipment or services provided by the five Chinese companies or their affiliates that would be immediately blacklisted by the BIOSECURE Act.
- Evaluate existing supply chains and carry out necessary due diligence to determine if they rely on equipment or services provided by other companies from countries of concern that are likely to be eventually listed.
- Begin the process of exploring alternative supply chain opportunities, including scoping out new potential suppliers, engaging in discussions with them and discussing timelines for potential changes.
- When assessing processes and controls for high-risk vendors, we encourage organizations to consider:
  - Regulations and laws in the vendor's country that could present confidentiality and/or integrity risks to your systems or data,
  - Past behaviour and practices of the vendor and the vendor's country in this space,
  - The nature of the vendor's ownership (such as whether it is privately or state-owned) and how transparent the vendor is about its corporate structure, shareholders and other significant influences
  - The level of influence the vendor's government could exert over the vendor,
  - Transparency around the data life cycle – including where information is initially sent, and other touchpoints it flows through or can be accessed from, and
  - The level of control your organization has over access, storage and control of data once it has left its initial collection point