USINDOPACOM Legal Vigilance Update

Issue #46, 7 September 2025

PREVAIL

Teammates,

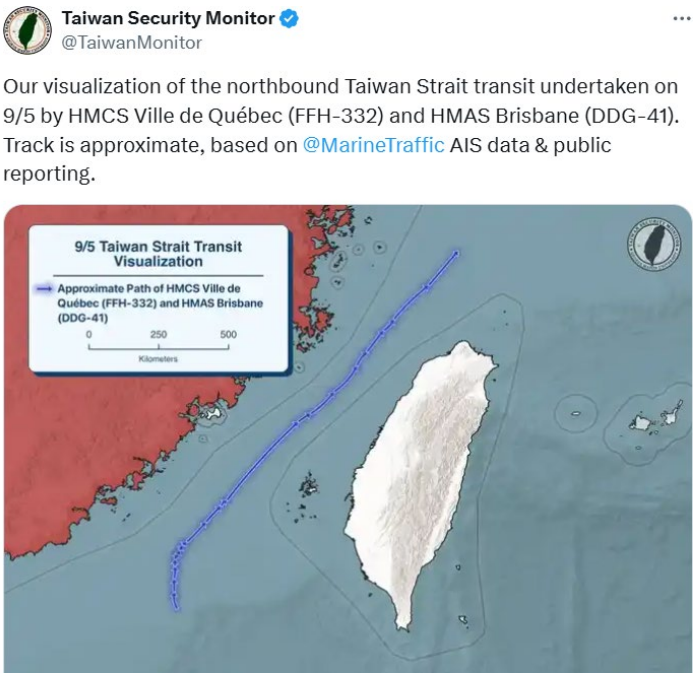
Below please find the 46th edition of U.S. Indo-Pacific Command's (USINDOPACOM) Legal Vigilance Update (LVU). To access previous LVUs, please visit https://www.pacom.mil/Contact/Directory/Jo/Jo6-Staff-Judge-Advocate/.

Quote of the Week:

"Overdoses from synthetic opioids like fentanyl is the leading killer of young Americans from 18-45. ***China plays a central role in this crisis, not merely by failing to stem the ultimate source of many illicit drugs distributed in the United States, but by actively sustaining and expanding the business of poisoning our citizens****."*

Thomas Pigott, Principal Deputy Spokesperson
U.S. Department of State
Press Statement, *Sanctioning China-Based Synthetic Opioid and Chemical Suppliers*

- 6-7 September 2025: Australia and Canada exercise freedom of navigation and uphold the rule of law in transit of Taiwan Strait.
  - **Bottom-line:** Royal Australian Navy Hobart Class destroyer HMAS Brisbane and Royal Canadian Navy frigate HMCS Ville de Québec conducted a routine transit through the Taiwan Strait from September 6 to 7 in accordance with international law.
    - References:
      - *China criticizes Canadian, Australian warships transiting Taiwan Strait* (Reuters, Sep. 6, 2025)
    - Key Points:
      - An Australian Defense Department spokesperson said: "Australian vessels and aircraft will continue to exercise freedom of navigation and uphold International Law, particularly United Nations Convention on the Law of the Sea."
      - The Taiwan Strait encompasses a corridor of waters and airspace beyond the territorial sea and sovereign airspace of any coastal state – in this corridor, all nations enjoy high-seas freedoms of navigation, overflight, and other internationally lawful uses of the sea.



- ***The United States rejects any assertion by China of sovereignty over the entirety of the Strait or beyond its 12-nm TTS, and rejects any assertion of excessive jurisdiction or control, i.e. exceeding the limited contiguous and exclusive economic zone jurisdiction or rights provided for by international law of the sea as reflected in UNCLOS.***

- 25 August 2025: new report exposes China's coercive influence operations targeting U.S. elections.
  - **Bottom-line:** a New York Times investigation reveals how the Chinese Communist Party (CCP) deploys covert, coercive, and deceptive tactics to influence elections in the United States—methods that mirror Beijing's influence playbook across the Indo-Pacific, from Taiwan to the Pacific Islands.
    - References:
      - *How China Influences Elections in America's Biggest City* (New York Times, Aug. 25, 2025)
      - *Inside Our Investigation of China's Influence Campaigns* (New York Times, Aug. 25, 2025)

    - Key Points:
      - The investigation (which was also the subject of a NY Times' The Daily podcast) describes a ***CCP strategy to sway political outcomes in the U.S. by exploiting diaspora communities, leveraging business ties, and covertly backing candidates perceived as favorable to Beijing***.
      - These activities include intimidation of dissidents, disinformation in Mandarin-language outlets, and cyber-enabled propaganda aimed at shaping narratives on Taiwan, Hong Kong, and U.S.-China relations.
      - Analysts warned that these efforts are not isolated but part of a long-term CCP campaign to erode trust in democratic institutions abroad and normalize Beijing's narratives—consistent with broader Chinese lawfare and political warfare tactics.
      - The ***tactics closely mirror CCP influence campaigns targeting other Indo-Pacific states***, including:
        - Taiwan, where CCP disinformation and economic leverage seeks to erode democratic resilience;
        - Australia, where CCP covert funding and academic influence operations have prompted new counter-interference laws; and
        - Pacific Island countries, where Beijing mixes development aid with political pressure to shape domestic decision-making.
      - Common across these campaigns is a reliance on hybrid instruments—lawfare, front groups, disinformation, and diaspora intimidation—that blur the line between diplomacy and coercion.
      - The findings highlight that safeguarding democracy and the freedom, security, and prosperity of the Indo-Pacific requires coordinated vigilance—not only against Beijing's maritime gray-zone coercion, but also its political and legal warfare aimed at democratic processes themselves.

- 3 September 2025: United States targets China-linked synthetic drug trafficking networks.
  - **Bottom-line:** in a coordinated effort, the Departments of Justice, State, and Treasury announced indictments and sanctions against China-based chemical companies, executives, and brokers fueling the U.S. synthetic opioid crisis through precursor exports and laundering operations.
    - References:
      - *Grand Jury Indicts Three U.S. Citizens, 22 Chinese Nationals, Four Chinese Pharmaceutical Companies in International Drug Trafficking, Money Laundering Conspiracies* (U.S. Dep't of Justice, Sep. 3, 2025)
      - *Sanctioning China-Based Synthetic Opioid and Chemical Suppliers* (U.S. Dep't of State, Sep. 3, 2025)
      - *Treasury Sanctions China-Based Chemical Company to Combat Synthetic Opioid Trafficking* (U.S. Treasury Dep't, Sep. 3, 2025)
    - Key Points:
      - Federal prosecutors announced that a federal grand jury in Dayton, Ohio, returned charges against dozens of defendants, including Chinese nationals and companies, in narcotics and money laundering conspiracies involving illegal cutting agents.
      - Concurrent with the charges brought against this network, the U.S. Department of the Treasury sanctioned Chinese chemical company Guangzhou Tengyue Chemical Co., Ltd. (Guangzhou Tengyue) and two of the company's representatives, Huang Xiaojun and Huang Zhanpeng, for manufacturing and coordinating shipments of illicit opioids and chemical agents to the United States.
      - The indictment alleges that ***Chinese companies and affiliated foreign nationals intentionally and openly marketed, delivered, and exported to the United States controlled substances and other compounds that they knew would be used by domestic drug dealers to increase the yield and potency of fentanyl distributed in the U.S.***
      - China-based chemical manufacturing companies remain the primary source of fentanyl precursor chemicals and other illicit opioids entering the United States.

- September 2025: multinational advisory warns of China state-sponsored cyber campaigns targeting global networks.
  - **Bottom-line:** a joint advisory issued by the U.S. and partner cyber agencies details how China state-sponsored advanced persistent threat (APT) actors have targeted telecommunications, government, and military networks worldwide to fuel a global espionage system.
    - References:
      - Joint Cybersecurity Advisory, *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System* (Sep. 2025)
    - Key Points:
      - The advisory confirms that Chinese APT actors have conducted persistent operations since at least 2021, targeting backbone routers and edge devices in telecommunications, transportation, lodging, government, and military networks to enable long-term espionage access.
      - APT operations have been linked to multiple China-based entities, including at least: Sichuan Juxinhe Network Technology Co. Ltd.; Beijing Huanyu Tianqiong Information Technology Co., Ltd.; and Sichuan Zhixin Ruijie Network Technology Co., Ltd.
      - These companies provide cyber-related products and services to China's intelligence services, including multiple units in the People's Liberation Army and Ministry of State Security.
      - ***The data stolen through this activity against foreign telecommunications and internet service providers, as well as intrusions in the lodging and transportation sectors, ultimately can***

provide Chinese intelligence services with the capability to identify and track their targets' communications and movements around the world.

- The report highlights coordinated multinational attribution and response—demonstrating broad consensus among the U.S., Five Eyes, and other allies/partners that China's cyber operations are systemic, state-backed, and a direct threat to security and prosperity.

- 29 August 2025: United States, Japan, and Republic of Korea convene trilateral diplomatic working group meeting on Democratic People's Republic of Korea (DPRK) cyber activities.
  - **Bottom-line:** on August 27 and 28, the United States, Japan, and the Republic of Korea (ROK) convened in Tokyo for the fourth meeting of the Trilateral Diplomatic Working Group to counter cyber threats posed by the DPRK.
    - References:
      - *Fourth United States-Japan-Republic of Korea Trilateral Diplomatic Working Group Meeting on Democratic People's Republic of Korea Cyber Activities* (U.S. Department of State, Aug. 29, 2025)
    - Key Points:
      - The meeting deepened trilateral collaboration to disrupt the DPRK's ability to generate and launder revenue through malicious cyber activity, IT workers, and third-party facilitators, which it uses to fund its unlawful WMD and ballistic missile programs.
      - Through the working group, the United States, Japan, and the ROK continue to coordinate on a wide range of trilateral actions, including efforts to restrict DPRK actors' access to key jurisdictions in which they generate revenue and prevent private sector companies from being exploited by DPRK targeting.
      - The three sides also discussed future engagement with the AI industry, autonomous sanctions, and law enforcement cooperation.
      - By some estimates, ***DPRK-backed hackers stole at least $1.34 billion worth of cryptocurrency last year***.
      - UN officials monitoring sanctions imposed on the DPRK believe that the ***proceeds from dozens of suspected cyber-attacks the regime carried out between 2017 and 2023 were used to improve its nuclear weapons program.***