



# SAFEGUARDING OUR MILITARY EXPERTISE

## FOREIGN COMPANIES CONTINUE TO RECRUIT CURRENT AND FORMER WESTERN SERVICE MEMBERS TO BOLSTER THE PRC'S MILITARY

### THREAT

China's (PRC) People's Liberation Army (PLA) continues to target current and former military personnel from North Atlantic Treaty Organization (NATO) nations and other Western countries to help bolster the PLA's capabilities. The PLA is using private companies in South Africa and China to hire former fighter pilots from Canada, France, Germany, the United Kingdom, Australia, the United States, and other Western nations to train PLA Air Force and Navy aviators. The PLA wants the skills and expertise of these individuals to make its own military air operations more capable while gaining insight into Western air tactics, techniques, and procedures. The insight the PLA gains from Western military talent threatens the safety of the targeted recruits, their fellow service members, and U.S. and allied security.

This threat continues to evolve in response to Western government warnings to their military personnel and public, so this notice seeks to continue highlighting this persistent, adaptive threat. The U.S. and its Western partners have also taken other actions to counter this threat, including commercial restrictions on the Test Flying Academy of South Africa (TFASA), Beijing China Aviation Technology Co. (BCAT), Stratos, and other PLA providers exploiting Western and NATO personnel; and legal and regulatory changes to prohibit former military members from engaging in post-service employment with China. This threat's scope and scale prompted more than 120 officials from U.S., NATO, and partner countries to convene a conference in January 2024 to counter this activity.

### INDICATORS

**Nefarious recruitment attempts are not always obvious**, as companies may not initially promote the PLA's role. Western service members have been the targets of both opaque and transparent recruitment.

- **Targets may be contacted directly** by personal acquaintances from the military and through headhunting emails, or indirectly via professional networking sites and online job platforms.
- **Job offers can come from privately-owned companies** around the globe whose ties with the PLA are hidden.
- **Job locations may be in China, South Africa, or elsewhere**, with lucrative contracts and the opportunity to fly exotic aircraft, with vague details on the ultimate customers.
- **The most sought-after targets to-date have been military pilots**, flight engineers, and air operations center personnel. The PRC has also targeted technical experts with insight into Western military tactics, techniques, and procedures.

### IMPACT

Insights the PLA gains from Western military talent **threaten the safety** of the targeted recruits and their fellow service members, and U.S. and allied security.

- Poaching Western military expertise enables the PLA to advance its air capabilities, improve planning for future operations, and better counter Western military strategies, **all to the detriment of the United States, its partners and allies, and their service members.**
- Western recruits who train the PLA **may increase the risk of future conflict** by reducing our deterrence capabilities and **put their military colleagues at risk** in such a conflict.
- Western recruits **may also face legal peril.** Those providing unauthorized training or expertise services to a foreign military can face **civil and criminal penalties**. In 2022, a former U.S. Marine pilot on contract with TFASA was arrested in Australia pursuant to a U.S. indictment charging him with violating the U.S. Arms Export Control Act.

## MITIGATION

Current and former service members can take several steps to thwart the PLA's efforts to exploit them.

- **Be alert to the indicators above**, including approaches via personal and professional networks, through messaging apps, veterans' reunions, conferences, and aviation community events.
- **Avoid interactions with** former Western service members involved with companies or entities affiliated with the PLA.
- **Stay engaged** with your national military, security, and law enforcement agencies for the latest threat information and mitigation steps, and to report suspicious recruitment efforts.
- **Exercise caution before posting details** about security clearances, work experience, and contacts on professional networking sites or other online job platforms, which draw PLA interest.
- **Exercise caution** before responding to emails or online invitations to connect from unknown parties. Verify these approaches and practice due diligence on the requesting party.
- **Beware of excessive flattery** in recruitment pitches, job offers with lucrative salaries and other benefits that seem too good to be true, and obfuscation about the company's customers.

References in this product to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the Intelligence Community.

For additional information on NCSC awareness materials or publications, visit our website: [www.ncsc.gov](http://www.ncsc.gov) or contact [DNI\\_NCSC\\_OUTREACH@DNI.GOV](mailto:DNI_NCSC_OUTREACH@DNI.GOV)

Find us on Twitter (X):  
[@NCSCgov](https://twitter.com/NCSCgov)

On LinkedIn:  
NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

## REPORTING INCIDENTS

If you or someone you know is being targeted for recruitment, or has already been recruited, please contact one of the agencies below:

- **U.S. Air Force/U.S. Space Force:**  
Contact the local Office of Special Investigations detachment or submit a report via [www.osi.af.mil/Submit-a-Tip/](http://www.osi.af.mil/Submit-a-Tip/).
- **U.S. Navy/U.S. Marines:**  
<https://www.ncis.navy.mil/Resources/NCIS-Tips/>
- **U.S. Army:**  
Submit an iSALUTE Suspicious Activity Report at <https://www.inscom.army.mil/isalute/> or 1-800-CALL-SPY (1-800-225-5779) (CONUS ONLY)
- **Federal Bureau of Investigation (FBI):**  
Submit a tip online at <https://tips.fbi.gov/home>, contact your local FBI field office at <https://www.fbi.gov/contact-us/field-offices>, or <https://www.fbi.gov/contact-us/international-offices>; contact the FBI's National Counterintelligence Task Force at [ncitf@fbi.gov](mailto:ncitf@fbi.gov)

If you are a **resident or citizen of one of the following countries**, you can also contact one of these agencies:

- **Australia:** Department of Defence and Australian Defence Force personnel are obligated to submit XP188 contact reporting via the security incident coordinate centre in adherence to the Australian Government Contact Reporting Scheme.
- **Canada:**
  - Contact Canadian Forces National Counter-Intelligence Unit at [CFNCIUOPS-OPSUNCIFC@forces.gc.ca](mailto:CFNCIUOPS-OPSUNCIFC@forces.gc.ca) or 1-855-4CFNCIU (423-6248).
  - Contact Canadian Security Intelligence Service at 613-993-9620 or <https://canada.ca/en/securityintelligence-service/corporate/contact-us.html>
- **New Zealand:** Report a national security concern at <https://providinginformation.nzsis.govt.nz> or contact Defence Counterintelligence at [DEFICI@nzdf.mil.nz](mailto:DEFICI@nzdf.mil.nz)
- **United Kingdom:** Report a concern to MoD's Confidential Hotline, [www.gov.uk/guidance/mod-confidential-hotline](http://www.gov.uk/guidance/mod-confidential-hotline)

