Australian Government
Australian Security Intelligence Organisation

Te Pā Whakamarumaru
New Zealand Security Intelligence Service

Safeguarding OUR SECRETS

China's military intelligence services use Western online job platforms to lure Five Eyes nationals with access to sensitive information

THE THREAT

China's military intelligence services are using an increasingly wide array of **professional networking sites and online job platforms** to target Five Eyes government and military personnel—and anyone with access to classified or privileged information.

These actors use an aggressive online recruitment strategy whereby intelligence officers or their affiliates pose as employees of private consultancies, think tanks or human resources (HR) firms, and place online job advertisements for foreign policy and defense analysts (or similar).

Successful candidates are pressured to provide "non-public" information for unspecified clients who are associated with the Chinese government. China's military intelligence services **ultimately seek to acquire privileged military, political and economic intelligence that can provide China with a strategic and tactical advantage over the Five Eyes.**

Who is at RISK?

Chinese intelligence officers attempt to recruit and cultivate long-term relationships with the following types of individuals in exchange for classified or privileged information:

- Security clearance holders, particularly those who specialize in defense, foreign affairs and security & intelligence.
- Military personnel, including those stationed in the Indo-Pacific region, with knowledge of regional capabilities and general activities.
- Persons with either indirect or peripheral access to government information, e.g. academics, journalists, freelance writers, think tank employees, or anyone with links to defense, security, policy and economic sectors.

RECRUITMENT

Chinese intelligence officers pose as online HR recruiters or consultants who represent fake, but often legitimate-looking, "cover companies" and claim to be located in countries other than China.

1 **First contact.** Recruiters post job ads on professional networking platforms and online hiring and freelance "gig work" websites like LinkedIn, Indeed, and Upwork. Resumes are ranked based on likelihood of access to sensitive information; recruiters begin their contact strategies.

2 **Interview.** When they are required, interviews are held virtually. Recruiters conceal their identity, and may start probing applicants about access to government contacts. Military members may be asked about their roles and unit activities, home base or naval vessel.

3 **Initial testing.** Candidates are asked to write a trial report on a topic such as China's bilateral relations, the Indo-Pacific region, and related defense issues, or international trade.

4 **Subsequent requests and platform shift.** Recruits are informed that for additional reports, the client requires more privileged information. At some point in the recruitment process, intelligence officers typically move the conversation to a more "secure" platform, such as encrypted messaging applications.

5 **Payment.** Recruits receive anywhere from a few hundred to several thousand dollars per report, and may be offered more money in return for increasingly sensitive information. Payment methods include third-party payment platforms, such as PayPal, Payoneer, Zelle, Skrill, and Wise, as well as Western Union, e-transfer and cryptocurrency. Recruits will often be compensated by an account belonging to an individual they have not met as part of the recruitment process.

Why does it MATTER?

While applicants often have no direct access to classified information, **even unclassified information** on government policy, or on military strategy, capabilities and installations, can be collected and combined with more sensitive reporting to form a comprehensive operational picture.

Certain types of data can place the lives of frontline military or other personnel at risk, can weaken our economic prosperity, and enable interference in our democratic processes.

Applicants who provide their resumes and other personally identifiable information risk compromises of personal privacy.

Individuals engaged in the unauthorized disclosure of sensitive or classified information could face a number of consequences including prosecution under national laws such as those relating to espionage.

Five Eyes agencies have identified individuals who have undertaken these activities, leading to criminal prosecutions, job losses, and security-clearance revocation.

REPORTING incidents

If you or someone you know is being targeted via any of the means listed above, contact your institution or department's corporate security office for further guidance and direction. Our respective agencies are liaising with corporate security offices regarding this threat.

To report non-immediate threat information related to national security:

Federal Bureau of Investigation

By phone: 1-800-CALL-FBI (1-800-225-5324)

Online: tips.fbi.gov

In-person: Visit your local FBI field office

References in this alert to any specific commercial product, process or service, or the use of any corporate name, 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 Five Eyes intelligence community.