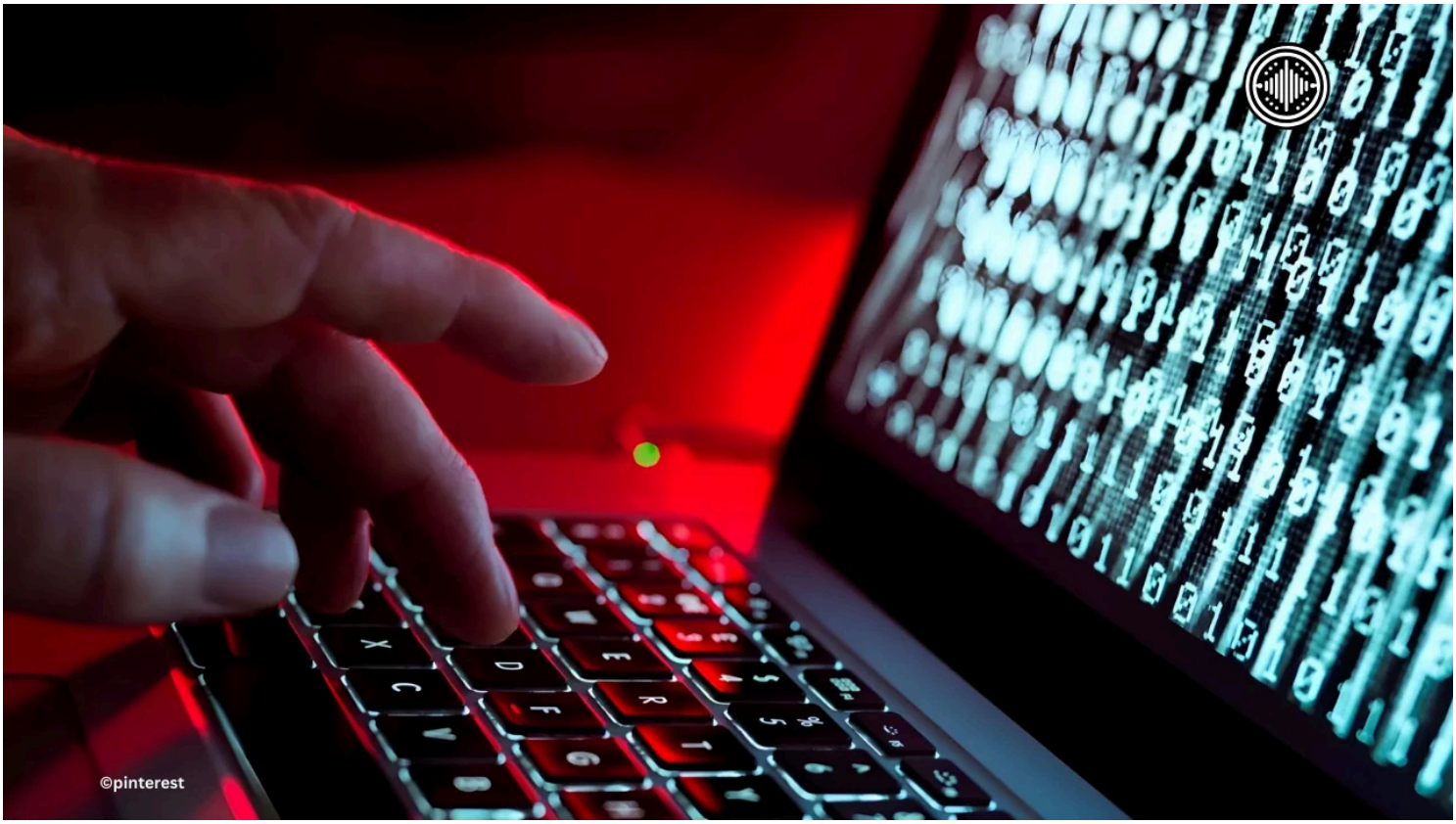
OpenVoiceNews

Transparent. Unbiased. Yours.

Australia weighs cyber militia amid skills gap

August 24, 2025

— Categories: Defence & Security



Download IPFS

Australia is considering unconventional measures to address growing cyber threats as the nation faces a critical shortage of skilled professionals in the field. Experts have proposed exploring the creation of a volunteer “cyber militia,” composed of citizens with relevant knowledge, to provide potential support in defending government systems and critical industries.

The proposal comes as Australia experiences a rise in hostile cyber activity, including state-backed intrusions and ransomware attacks targeting businesses, hospitals, and

government agencies. Officials have warned that the country's ability to protect itself is hampered by a shortage of trained personnel, leaving gaps in both public and private sector defenses.

Australia's cyber defenses have been tested in recent years by increasingly sophisticated campaigns. Incidents such as the 2022 Optus data breach and ongoing attacks on healthcare networks have underscored the vulnerability of critical infrastructure. With global demand for cybersecurity specialists outpacing supply, Australia is struggling to recruit and retain enough skilled professionals.

Industry figures indicate that tens of thousands of positions remain unfilled nationwide. Without swift action, experts argue, the shortage could worsen, leaving the country exposed.

Supporters of the cyber militia concept argue that tapping into the expertise of technically skilled volunteers could help close the gap. These volunteers, many drawn from the private sector or academia, would not replace professional cyber defenders but could be deployed to assist during major incidents.

Similar initiatives have been trialed abroad. Countries such as Estonia, which have faced repeated cyberattacks, have incorporated civilian specialists into national defense frameworks. Proponents believe Australia could adapt such a model to its own needs.

Critics, however, caution that relying on volunteers raises issues of oversight, accountability, and national security. Any civilian participation would require strict vetting and coordination to prevent unintended risks.

While the Australian government has not formally endorsed the idea of a cyber militia, it has acknowledged the scale of the skills shortage and pledged investment in training programs. Initiatives are underway to expand university courses, vocational training, and incentives to attract more workers into cybersecurity.

Officials maintain that building a professional workforce remains the priority, but experts stress that time is critical. Experts warn that unless the skills gap narrows quickly, Australia may need to consider unconventional measures to strengthen its digital defenses.