2024 年度澳門重點研發資助計劃
數字科技（網絡安全）領域申報指南

一、背景

網絡安全是數字時代的重要議題，不僅關乎國家安全、社會安全、信息安全，也和每個公民的日常生活密切相關國家“十四五”規劃強調“提升網絡安全威脅發現、監測預警、應急指揮、攻擊溯源能力。加強網絡安全關鍵技術研發，加快人工智能安全技術創新，提升網絡安全產業綜合競爭力”。《“十四五”國家信息化規劃》指出“堅持安全是發展的前提，發展是安全的保障，築牢數據安全保障防線，首先要推進數據分類分級管理、數據安全共享使用。”

澳門特區政府高度重視提升網絡安全能力，《澳門特別行政區經濟和社會發展第二個五年規劃（2021-2025 年）》中明確“制定總體網絡安全發展策略，加強對關鍵基礎設施資訊系統與網絡的保護”；《2024 年財政年度施政報告》中提出“優化網絡安全建設，不斷提高應對網安風險及事故的水平。”

為進一步整合現有優勢資源，提升澳門網絡安全技術能力，科學技術發展基金在徵求澳門相關領域科研人員意見建議基礎上，依託內地專家力量，研究提出本領域重點研發計劃，有計劃、有步驟地配合國家所需、發揮澳門所長，針對澳門經濟社會發展現狀和需求，以科技創新築牢澳門網絡安全防線，進一步維護國家安全。

二、總體目標

在當前複雜的網絡安全形勢下，做好各項網絡安全保障工作，加強遏制各類網絡攻擊，持續提升資訊網絡和電腦系統的安全性，提高信息安全領域的智能防護能力，築牢澳門網絡安全防線。

三、研究方向

研究方向：面向信息安全領域的大語言模型構建技術研究與應用

（1）研究信息安全垂直領域的大語言模型構建方法。研究信息安全大語言模型的微調方法、模型的輕量化部署方法等，解決信息安全領域的大模型威脅分析與處理準確度不高、資源消耗過大的問題。

（2）研究自動化數據集製作方法。研究面向信息安全領域大語言模型的自動化數據集製作方法，包括信息安全領域數據的清洗和預處理、數據的動態處理、數據的智慧增強方法，形成信息安全領域的高品質數據集及自動化製作系統。

（3）研究 AI 智能體構建方法。研究基於信息安全領域的大語言模型的 AI 智能體構建方法，形成多源異構告警數據的融合、告警評價和攻擊研判、威脅情報抽取、異常行為分析、網絡紅方智能攻擊演練等智能體。

（4）研究 AI 智能體的安全增強方法。研究幻覺檢測、投毒攻擊防禦、對抗樣本防禦方法。

（5）研發面向信息安全領域的智能服務平台，該平台支持智能問答、攻擊檢測與防禦、安全運營等多

種場景。

考核指標：

（1）構建 1 個信息安全領域的大模型。

（2）構建涵蓋資產、漏洞、攻擊等多維度的大規模網絡安全知識庫，建成的網絡安全知識庫達到 10 億條目，融合的多源異構告警數據類型不少於 5 種。

（3）所構建的智能體告警與攻擊行為映像準確率大於 85%，威脅情報抽取準確率達到 90%，針對典型 Web 攻擊檢測準確度大於 90%，網絡流量分類準確度大於 95%。

（4）至少抵御 5 種投毒攻擊；在現有的對抗樣本攻擊下，檢測準確率、分類準確率下降不超過 10%；對於輸出幻覺的檢測準確率大於 85%。

（5）構建 AI 智能體平台，包括多源異構告警數據的融合、告警評價和攻擊研判、威脅情報抽取及檢測異常行為分析等場景功能，單一威脅事件的平均閉環處理時間低於 20 秒。

（6）技術成熟度應達到 7 級。

四、申報要求

（1）牽頭單位須為澳門機構，必須有企業牽頭或參與，企業須提供不少於資助經費 50%的配套經費。如企業為參與單位，則須為澳門或橫琴企業。

（2）如為合作項目，須提供正式合作協議。

（3）項目實施年限 3 年。每個項目的申請金額上限為 1,500 萬澳門元。

五、參與編制的專家

李 丹 清華大學教授
張偉哲 哈爾濱工業大學教授
李洪偉 電子科技大學教授
翁 健 暨南大學教授
董長宇 廣州大學教授