

Programa Específico de Apoio Financeiro para Projectos-Chave de I&D de Macau 2024

Guia de Candidatura na Área da Tecnologia Digital (cibersegurança)

I. Contexto

A cibersegurança é uma questão importante na era digital, que não só relacionada com a segurança nacional, a segurança social e a segurança da informação, mas também estreitamente relacionada com a vida quotidiana de cada cidadão. O “14.º Plano Quinquenal” nacional enfatiza “reforçar das capacidades de detecção, monitorização e alerta de ameaças à segurança das redes, do comando de emergência e da rastreabilidade dos ataques. Melhorar a I&D de tecnologias-chave de cibersegurança, acelerar a inovação da tecnologia de segurança da inteligência artificial e aumentar a competitividade global da indústria de cibersegurança”. O 14.º Plano Quinquenal para a Informatização Nacional indica que “insistir na segurança é um pré-requisito para o desenvolvimento e o desenvolvimento é uma garantia de segurança; para construir uma defesa forte da segurança dos dados, o primeiro é promover a classificação e a organização hierárquica dos dados e a partilha e utilização seguras dos dados”.

O Governo da RAEM atribui grande importância ao reforço da capacidade de cibersegurança, e propôs de forma clara no Segundo Plano Quinquenal de Desenvolvimento Socioeconómico da Região Administrativa Especial de Macau

(2021-2025) que “elaborar a estratégia geral do desenvolvimento de segurança cibernética, reforçar a protecção dos sistemas e redes informáticos das infra-estruturas críticas, apreciar e deliberar anualmente o Relatório Geral de Cibersegurança da RAEM”; no Relatório das Linhas de Acção Governativa para 2024, afirma-se que “foi optimizada a construção da cibersegurança e elevada sem qualquer interrupção a qualidade de resposta aos riscos e incidentes da cibersegurança”.

A fim de integrar ainda mais os recursos vantajosos existentes e reforçar a capacidade tecnológica de Macau em termos de cibersegurança, o Fundo para o Desenvolvimento das Ciências e da Tecnologia investigou e lançou, após ter recolhido as opiniões dos investigadores científicos das áreas relacionadas de Macau e recorrido a apoios dos especialistas do Interior da China, o presente Programa de Apoio Financeiro para Projectos-Chave, de modo a atender de forma planeada, passo a passo, às necessidades do Estado. Centrando-se na situação actual e nas necessidades do desenvolvimento económico e social de Macau, reforçará a protecção para construir juntos uma linha sólida de defesa de cibersegurança através da inovação tecnológica e salvaguardará ainda mais a segurança nacional.

II. Objectivo Geral

Na actual situação complicada da cibersegurança, devemos fazer um bom trabalho na salvaguarda de cibersegurança, reforçar a contenção de vários tipos de ciberataques, continuar a reforçar a segurança das redes de informação e dos sistemas

informáticos e melhorar a capacidade de protecção inteligente no campo da segurança da informação, de modo a construir juntos uma linha sólida de defesa de cibersegurança de Macau.

III. Área de Investigação

Área de Investigação: Investigação e aplicação da tecnologia de construção de grande modelo de linguagem na área da segurança da informação

- (1) Investigação dos métodos de construção de grande modelo de linguagem na área vertical de segurança da informação. Investigação dos métodos de micro-ajuste do grande modelo de linguagem de segurança da informação, de disposiç leve do modelo, etc., para resolver os problemas de baixa precisão e consumo excessivo de recursos da análise e processamento de ameaças de grande modelo no campo da segurança da informação.
- (2) Investigação dos métodos de produção automatizada do conjunto de dados. Investigação dos métodos de produção automatizada do conjunto de dados para grande modelo de linguagem na área de segurança da informação, incluindo a limpeza e o pré-processamento de dados no campo da segurança da informação, o processamento dinâmico de dados e o reforço inteligente de dados, de modo a formar conjuntos de dados de elevada qualidade e sistema de produção automatizados no campo da segurança da informação.
- (3) Investigação dos métodos de construção de agentes de IA. Investigação dos métodos de construção de agentes de IA de grande modelo de linguagem no campo da

segurança da informação, formação de agentes inteligentes como a fusão de dados heterogêneos de alarme de múltiplas fontes, a avaliação de alarmes, a análise e o julgamento de ataques, a extracção de informações sobre ameaças, a análise de comportamentos anormais e o ensaio de ataques inteligentes em rede.

- (4) Investigação dos métodos de reforço da segurança para agentes de IA. Investigação dos métodos de detecção de alucinações, defesa contra ataques de envenenamento e defesa contra amostras.
- (5) I&D de uma plataforma de serviços inteligentes para o campo da segurança da informação, que suporta perguntas e respostas inteligentes, detecção e defesa de ataques, operações de segurança e outros cenários.

Indicadores de avaliação:

- (1) Construção de um grande modelo no campo da segurança da informação.
- (2) Construção de um banco de conhecimentos em matéria de cibersegurança em grande escala, abrangendo activos, vulnerabilidades, ataques e outras dimensões, e construção de um banco de conhecimentos em matéria de cibersegurança com mil milhões de entradas, com pelo menos cinco tipos de dados heterogêneos de múltiplas fontes fundidos.
- (3) A precisão do alarme de agente inteligente construído e da imagem do comportamento de ataque deve ser superior a 85%, a precisão da extracção de informações sobre ameaças deve atingir 90%, a precisão da detecção de ataques típicos na Web deve ser superior a 90% e a

precisão da classificação do tráfego de rede deve superior a 95%.

- (4) É capaz de defender, pelo menos, cinco tipos de ataques de envenenamento; com os ataques de contra-amostra existentes, a precisão da detecção e a precisão da classificação não devem diminuir mais de 10%; a precisão da detecção de alucinações de saída deve ser superior a 85%.
- (5) Construção de uma plataforma de agentes de IA, incluindo a fusão de dados heterogêneos de alarme de múltiplas fontes, a avaliação de alarmes, a análise e o julgamento de ataques, a extracção de informações sobre ameaças, a análise de comportamentos anormais e outras funções de cenário, sendo o tempo médio de processamento em ciclo fechado para um único evento de ameaça inferior a 20 segundos.
- (6) O Nível de Prontidão da Tecnologia (TRL) deve atingir o nível 7.

IV. Requisitos de Candidatura

- (1) A entidade principal deve ser uma instituição de Macau. A candidatura deve ser liderada ou contar com a participação de empresa, e a empresa deve fornecer fundos complementares não inferiores a 50% do montante de apoio financeiro. Se a empresa for uma entidade participante, deve ser uma empresa de Macau ou de Hengqin.
- (2) Se o projecto for um projecto de cooperação, deve ser apresentado um acordo formal de cooperação.
- (3) O prazo de execução do projecto é de três anos. O

montante requerido máximo por cada projecto é de 15 milhões de patacas.

V. Especialistas envolvidos na elaboração

Li Dan	Professor da Universidade de Tsinghua
Zhang Weizhe	Professor do Instituto de Tecnologia de Harbin
Li Hongwei	Professor da Universidade de Ciência e Tecnologia Eletrónica da China
Weng Jian	Professor da Universidade Jinan
Dong Changyu	Professor da Universidade de Guangzhou