智慧警务新蓝图：人工智能在网络犯罪及诈骗防治策略的应用

■ 岑卓颖

摘　要　科技迅速发展，诈骗手法日益翻新，诈骗集团利用先进技术与社交工程攻击进行诈骗，加大警方侦查难度。为了有效打击新型犯罪科技，本文研究以“数据引领，智能护航”为原则的智能警务，以大数据及信息网为网络诈骗防治之本，借鉴各地防治策略、内地反诈骗体系与跨国情报共享经验，探索大数据与人工智能技术在诈骗防治的应用。智能警务系统融合数据可视化与智能决策，提升对新型犯罪识别能力。制度上仍需完善监管法规，考虑共同责任与多方合作，强化防诈生态。碍于海峡两岸及港澳地区法制不同，要彻底打击整条犯罪链不易，未来需要加强执法合作，打破地域与法制壁垒。通过多渠道教育提升公众意识，推动企业建立安全管理体系，以有效应对数字时代的诈骗威胁，保障公共安全。

关键词　智慧警务　人工智能　大数据　网络犯罪检测　诈骗防治　警务现代化

一、前言

（一）研究背景与意义

随着科技进步，网络诈骗、深度伪造、暗黑生成式人工智能，到虚拟资产犯罪与网络攻击及安全威胁等问题日益严重，而执法过程受限于地缘政治因素、法律框架及跨境司法管辖等挑战，令调查更具复杂性。犯罪分子利用先进技术与社交工程攻击进行诈骗，包括加密技术、虚构身份、虚拟私有网络、自动化网络钓鱼等，加大警方侦查难度。网络犯罪不仅使广大市民受害，甚至威胁国家安全。香港网络安全框架以多机构协作为核心，通过情报分享与骗款拦截应对诈骗。警方采取情报主导策略，联同内地执法部门捣破多个诈骗集团。警方在 2022 年 12 月成立的“科技罪案警政顾问小组”，汇聚网络安全、人工智能与区块链等方面的专家，推动数码警务发展。由于跨境加密货币交易的匿名性限制追踪成效，电话电邮诈骗仍依赖公众举报，尚待研究引入人工智能方案打击诈骗。2022 年推出的一站式诈骗陷阱搜寻器“防骗视伏器”和 2023 年推出的“转

作者：香港警务处高级督察

数快可疑识别代号警示”可有效识别假冒投资诈骗，但跨境资金流动与新兴诈骗手法仍需进一步整合人工智能解决方案。本研究参考内地“国家反诈中心 APP”并以香港“防骗视伏器”升级为切入点，借鉴世界各地防治策略、内地反诈骗体系与跨国情报共享经验，探索 AI 在网络犯罪防治中的应用。本研究盼望通过技术创新提升香港警务效率，保护市民与企业免受诈骗侵害，促进国际执法合作，强化金融与社会安全。

（二）研究问题

1．高科技诈骗的技术特征如何影响防治策略？

2．智慧警务如何借鉴世界各地及内地技术提升诈骗侦测效率？

3．如何以技术部署应对香港的金融环境与跨境诈骗挑战？

二、文献综述与理论基础

人工智能（AI）在警务领域的应用日益广泛且多元，涵盖犯罪预防、侦查、网络犯罪防治、交通执法、突发事件应对等多个方面，提升警务工作的效率和准确性，同时也带来了新的挑战。越来越多的国家将大数据分析技术引入警务系统中，从而提高事前预判能力。以下就网络犯罪范畴审视，AI 警务的主要应用层面。

（一）犯罪预防与风险预测

AI 在犯罪预防与风险预测中利用大数据分析与机器学习（Machine Learning；ML）主动防范，显著提升警务效率。透过历史犯罪数据（时间、地点、类型），AI 挖掘模式，识别高风险区域与时段，辅助警方优化巡逻与资源分配。基于 ML 的风险预测模型整合社会经济、气候及人口流动数据，动态评估犯罪概率。行为分析技术检测社交媒体与事务历史记录，识别异常行为作为犯罪预警。实证显示，美国预测性警务应用 AI 智能巡逻系统，依据风险热图制定高效路线，暴力犯罪率显著降低。然而，数据隐私与模型偏差问题需透过规范数据使用与技术应用解决，以确保公平性与可靠性。总体而言，AI 从被动防范转向主动预防，为智慧城市安全提供科学支持。

（二）网络犯罪检测

AI 在网络犯罪检测中透过自动化与智能化分析海量数据，快速识别威胁，提升警务效率。ML 模型分析网络流量与用户行为，动态检测异常模式，超越传统签名检测限制。在恶意软件检测中，深度学习基于行为特征与代码模式识别变种病毒，检测准确率较传统方法高 40%。针对网络钓鱼，AI 结合自然语言处理（NLP）与计算器视觉，分析伪造邮件与网站伪装，实时阻断欺诈；ML 提升 25% 高级威胁检测率，微软系统则提前 48 小时预警钓鱼攻击。然而，数据质量依赖与对抗性攻击挑战需透过迁移学习与持续学习解决。AI 的多模态检测与自动化响应将误报率降低超 50%，显著提升网络犯罪防护效率。

（三）犯罪侦查与证据分析

AI 在犯罪侦查与证据分析中透过多源数据整合与智能技术提升破案效率。利用大数据分析，AI 挖掘影像、通话录音及事务历史记录线索，NLP 提取语音特征揭示犯罪网络。人脸辨识技术快速识别嫌疑人，节省人工比对时间；深度学习自动分析影像，重建犯罪现场三维模型。智能审讯系统结合心理分析与谎言识别，辅助高效讯问。实证显示，AI 风险分级降低误报率，数字取证技术增强证据司法效力，但私隐保护与技

术误判问题需规范数据使用以确保公平性。AI 的数据融合与自动化技术推动警务智能化，为快速破案提供关键支持。

三、诈骗新动态与现行防治措施

（一）诈骗趋势概况、手法案例与技术特征

香港作为全球金融中心，面对高科技诈骗犯罪的快速演变，网络安全挑战日益严峻。根据香港警务处数据，2022 至 2023 年间，诈骗案件增长 42.6%，科技犯罪上升 49.6%，损失金额由 32.1 亿港元飙升至 54.9 亿港元，使香港人均诈骗损失居全球首位。2024 年，网络诈骗呈爆炸式增长，深伪与钓鱼诈骗尤为突出。

2024 年第一季度，深度伪造案件较去年同期激增 1000%，20% 涉及伪造文件，损失达数亿港元。一宗重大案例发生于 2024 年初，一跨国公司员工被深伪视频诱骗，向五个银行账户转账 2 亿港元，创香港深度伪造损失纪录。网络钓鱼（Phishing）诈骗同样猖獗，2024 年损失达 7.9 亿港元，较 2023 年增长三倍。电话诈骗多数案件为假冒内地官员，巧立名目甚至威迫利诱，心理操纵受害者转账。

其他高科技诈骗亦迅速蔓延。语音克隆诈骗利用社交媒体语音片段，冒充亲属或执法人员，单一损失从数万至数十万港元不等。AI 聊天机器人透过 WhatsApp 与 Tinder 进行网上情缘诈骗，案件骗款达千万港元。假网站与广告诈骗在 Facebook 与 Instagram 广泛流传，2024 年每月新增数千域名，损失数十万港元不等。

投资骗案屡见不鲜，2025 年一名公司董事因误信 600% 投资回报，遭骗去共逾 1900 万港元，是警方今年接获损失最大的网上投资骗案。求职与技术支持诈骗案件数量显著上升，特别针对年轻求职者与老年用户。诈骗集团利用香港金融中心地位、社会媒体普及性及市民对权威的信任，进行大规模欺骗。

综上所述的诈骗手法与案例，本研究归纳科技诈骗的六大特征：智能自动化、跨境虚拟化、社交工程化、跨平台数据化、高收益低风险及针对性本地化，这些高科技诈骗的技术特征提升犯罪效率，挑战传统执法。

生成式 AI 透过深伪视频与语音克隆，冒充银行或熟人诱骗受害者泄露数据或转账，投资诈骗则利用算法模拟市场波动吸引资金，2024 年香港假网站每月激增数千域名，造成数百万港元损失。跨境虚拟化依赖境外服务器、VPN 与动态 IP 隐藏行踪，伪装本地号码或域名，绕过执法管辖，增加取证难度。社交工程化结合 AI 分析受害者行为，生成个性化诱导内容，假冒紧急情境以增强说服力。

跨平台数据化从社交媒体与网购平台搜集用户数据，推送定制广告或盗用凭证，大幅提高诈骗成功率。高收益低风险模式利用区块链匿名性，仅需简单恶意软件即可造成单案数百万港元损失，吸引犯罪集团持续扩张。针对性本地化手法迎合香港文化，伪造内地官员或本地银行通讯，降低受害者戒心，进一步挑战执法与防范效能。

（二）原因分析

1．人工智能武器化推动诈骗升级

生成式 AI 被犯罪分子滥用，大幅提升诈骗技术的威胁性。地下网络市场充斥如 WormGPT 等工具，与 ChatGPT 相比，WormGPT 几乎无伦理限制，可依指令生成任何内容，制作钓鱼电邮，诱骗受害者

泄露资料。日本警方首次发现不法分子使用生成式 AI 开发恶意软件，加密计算机数据并勒索赎金。AI 驱动的变形恶意软件（Polymorphic Malware）能定期改变程序代码，避开传统防毒软件识别，增加侦测难度。深伪技术生成逼真音频与视频，用于冒充身份、散布虚假信息或勒索，严重影响网络信息可信度。

2．网络电话滥用助长诈骗泛滥

网络电话（VoIP）透过互联网提供低成本、高灵活性的通讯服务，成为诈骗分子惯用工具。利用开源软件或伪基站，诈骗者伪装本地或国际号码（如 +62、+44），自动化拨打电话或发送钓鱼短讯与 WhatsApp 视讯通话，冒充公安或银行职员，直呼受害者姓名，诱导转账或泄露资料。另外，WhatsApp 视讯通话可摄取受害者外貌，结合社交媒体数据进行身份盗用。VoIP 无需 SIM 卡即可操作，绕过电话卡实名制，使市民每日饱受诈骗讯息困扰，其匿名性与低技术门坎令诈骗规模迅速扩大，执法追查困难。

3．钓鱼诈骗结合 AI 技术

钓鱼诈骗手法层出不穷，融合 AI，不再局限传统电邮与短讯，透过高仿品牌专页及搜索引擎优化提升欺骗成功率。诈骗者伪装成电讯商、零售奖赏计划或政府部门，发送短讯、电邮、语音或 QR 码（Quishing），声称账户异常或需兑换积分，诱导点击假网站，窃取凭证、信用卡资料或个人信息。骗徒利用 QR 码绕过电邮安全扫描，如假冒港铁年票的 QR 码骗局，盗取资料。克隆钓鱼（Clone Phishing）复制电邮，替换恶意附件，企业防护难以拦截。

4．网络犯罪服务兴起加剧犯罪威胁

网络犯罪服务（CaaS）指不法分子向其他罪犯提供网络犯罪工具、基础设施及服务以换取报酬，即使技术能力有限也能从事复杂攻击活动，推动网络犯罪快速增长。互联网的匿名性与网络保安技能缺口为网络罪犯服务提供了发挥机会。犯罪分子将技能与资源商品化，透过恶意软件服务（勒索软件、间谍软件）、漏洞服务（零日漏洞）、殭尸网络服务及黑客雇佣服务，协助其他罪犯绕过保安措施。2023 年，香港发生多宗软件攻击勒索巨额赎金并威胁泄露数据；2024 年，全球勒索软件攻击数量创历史新高。新型攻击利用漏洞渗透系统，显示犯罪组织化与专业化加深，威胁企业与网络安全。

（三）现行防治措施

1．多方协作框架

香港网络安全框架以多机构协作为核心，包括反诈骗协调中心（ADCC）、香港计算机保安事故协调中心（HKCERT）、香港金融管理局（HKMA）、数码政策办公室（DPO）及政府计算机保安事故应变小组（GovCERT. HK）。这些机构与政府资讯科技总监办公室（OGCIO）、联合财富情报组（JFIU）及国际伙伴合作，通过情报分享与骗款拦截应对诈骗。例如执法以外，HKCERT 在 2024 年间利用 AI/ML 检测并主动移除 370 万个钓鱼网址，涵盖电商与社交媒体。

2．执法与跨境合作

警方采取情报主导策略，开展大型执法行动。2023 至 2024 年，香港联同内地执法部门捣破多个境外诈骗集团，涉及 900 宗案件，拘捕 54 人，涉款逾 6886 万港元。警方在 2022 年 12 月成立“科技罪案警政顾问小组”，汇聚网络安全、AI 与区块链等专家，提供策略建议，推动数码警务发展。因跨境交易的匿名性限制追踪成效，电话电邮诈骗

仍依赖公众举报，尚待研究引入 AI 方案打击诈骗。

3．公众宣传与防骗工具

警方透过多渠道宣传提升市民对诈骗与网络风险的警觉性，定期更新防骗信息并举办活动。“防骗视伏器”自 2022 年 9 月推出，录得逾 600 万次搜寻，预警 83 万次风险，市民透过公众举报平台举报 31 万个可疑来电及 32000 个网站，其拦截功能自动识别诈骗来电与网站。警方亦将数据转交电讯商，封锁号码或网站，提升防御效率。

4．银行业合作与技术升级

HKMA 诈骗与洗钱情报工作组（FMLIT）促进银行、储值支付工具及零售支付系统的情报交换。警方与银行业合作，2023 年推出“转数快可疑识别代号警示”，2024 年扩展至网上银行、柜台交易及自动柜员机，交易前发出风险警示。“防骗视伏器”与转数快风险警示有效检测假冒投资诈骗，但跨境资金流动与新兴诈骗手法仍挑战现有技术，需进一步整合 AI 解决方案。

（四）防治措施的挑战

尽管采取多项措施，香港防治高科技诈骗仍面临显著挑战，诈骗集团透过多渠道渗透与技术快速演进突破防线。以下分析三大重点：

1．被动拦截为主，缺乏主动预警

现行防御以被动拦截为主，高度依赖受害者举报或资金转移后追踪。2023 年，逾 90% 的深度伪造调查始于受害者报案显示传统执法的滞后限制。跨境资金流动快速，特别是加密货币交易的匿名性，令拦截行动缓慢。缺乏主动预警系统（如实时 AI 分析社交媒体异常行为或语音克隆检测），限制了预防能力，无法有效遏制诈骗传播。

2．跨部门协作机制尚未完善

虽然 ADCC、HKCERT 与 HKMA 等机构协作，但跨部门数据整合与实时共享不足。诈骗情报分散于不同平台，未能精准打击骗子。例如，银行与电讯商的诈骗数据库未完全同步，影响可疑账号警示的覆盖率。跨境执法受限于地缘政治因素、法律框架及跨境司法管辖等挑战，犯罪分子利用科技漏洞、加密技术及虚拟私有网络，增加侦查难度。例如，超过 70% 的逮捕行动针对傀儡账户持有者，显示执法聚焦低层执行者，显示传统执法难以应对科技诈骗运作，未能有效打击幕后主脑。

3．公众防范意识与技术差距

公众对深伪、AI 聊天机器人等新兴诈骗的认知不足，与日新月异的诈骗技术形成差距。尽管“防骗视伏器”推广广泛，宣传活动未能深入覆盖弱势群体，老年与非科技背景市民使用率低，难以应对 Quishing 或克隆钓鱼等新手法。同时，企业员工对深伪视频的辨识能力不足，未能防范巨额诈骗案发生，公众教育仍需更精准与普及。

四、数据引领，智能护航

（一）借鉴世界各地防治策略

高科技诈骗犯罪利用 AI、加密技术及社交工程攻击，对全球执法框架构成严峻挑战。世界各地防治策略展示数据驱动与 AI 技术如何应对跨境诈骗。香港作为金融中心可借鉴各地整合 NLP、区块链分析与行为预测，主动预警与精准打击。

1．英国：警务数据整合与跨产业共享策略

英国政府主导的“网络欺诈宪章”联合 Amazon、Google、Meta 等科技巨头，推动数据共享与安全措施，建立快速举报与监

测机制，协同打击网络诈骗。英国防诈联盟（Stop Scams UK）整合银行（如汇丰、巴克莱）、科技公司及电信商，实时共享可疑URL与异常交易数据，每日传输数万数据点，提升侦测效率。警务方面，“Holmes 2侦查系统”整合拘留、刑案、鉴识及CCTV数据，支持跨案件智能分析以人查案、以案追人等功能，快速追查犯罪线索。此外，英国电信公司创新应用AI技术，开发“AI奶奶”主动干扰诈骗电话，增加诈骗成本。英国跨产业数据共享克服单一机构视野局限，数据互通形成协同防诈网络，构建高效反诈体系。

2．新加坡：防诈骗过滤与共同责任策略

新加坡透过共同责任架构（SRF）与智能反诈骗机器人（ScamShieldBot）打造智慧反诈体系。2024年实施的SRF明确金融机构与电信公司的防诈责任，银行需确保数字安全凭证，电信公司则负责拦截诈骗电话与讯息，失责方须赔偿受害者。2020年新加坡推出ScamShieldBot结合AI与大数据，透过WhatsApp让用户举报可疑讯息，快速比对诈骗数据并提供防范建议，背景自动过滤诈骗电话与讯息并向警方报告，短讯骗案三个月内减少七成。新加坡推动三方合作，金融机构与电信公司数据共享与联合监控，及时发现可疑交易与诈骗行为，强化公众警觉与防诈生态，提升安全保障与打击诈骗效率。

3．美国：区块链追踪与AI检测系统

美国的区块链情报平台TRM Labs提供跨33条区块链的资金追踪，支持7000万资产，运用150多种风险指标与专有威胁情报，2024年协助执法部门锁定犯罪资金。Chainalysis推出AI驱动的诈骗预防系统，监控每月80亿美元交易，保护1亿用户，降低60%交易所诈骗率。AI/ML模型（如随机森林）为监管提供支持，分析交易数据，识别诈骗模式，准确率达99%。金融机构如JPMorgan的COiN平台减少67%假阳性，Bank of America多层身份验证降低85%账户接管事件。这些技术整合区块链透明性与AI实时检测，构筑强大防线。

4．欧洲：网络犯罪中心与犯罪预测分析系统

欧洲刑警组织（Europol）旗下的欧洲网络犯罪中心（EC3）通过打击高利润网络诈骗，支持成员国调查与现场行动，并监测AI驱动的新型犯罪趋势，提供反制策略。意大利KeyCrime软件是一款于2008年创立的AI犯罪预测与分析系统，在米兰警察局试用，后由其同名公司商业化运营。该系统通过系统化收集犯罪数据，统计和AI算法进行相似性匹配，挖掘犯罪模式与连续性，有效预防犯罪。数据显示，2008至2017年间，米兰零售抢劫案件下降58%，银行抢劫下降89%，侦破率分别提升至63%与60%。

（二）内地经验与技术基础

透过法律保障、技术创新与多部门协作，内地形成全方位的防诈与打击机制，有效应对诈骗新动态。法律与协同治理方面，2022年《反电信网络诈骗法》的施行，为反诈工作奠定坚实法律基础，明确公安、金融、电信、网信等部门的协同职责，要求电信业者、银行及互联网平台建立风险防控机制，并强化公众防诈骗宣传教育，形成社会共治格局。全国跨省级反诈平台数据对接与28个省级互联网反诈系统构建共享与协作机制，形成全国范围的数据联动，全流程检测与预警诈骗行为，进一步提升反诈效率。

在大数据与AI技术应用层面，内地反

诈骗体系以大数据和 AI 为核心，整合公安、电信、金融及互联网等多源数据。七大反诈利器的“国家反诈中心 APP”具备实时预警、诈骗线索举报及防诈骗知识普及功能，已发送数亿次预警，受理数千万条举报线索。96110 预警劝阻专线与 12381 涉诈短信系统利用大数据分析潜在受害者，精准发送预警信息，预警准确率超 60%。此外，全国移动电话卡“一证通查”与云闪付“一键查卡”功能，帮助用户核查身份信息。公安反诈大数据平台整合多维数据，支持信息分析与侦查指挥，通过 AI/ML 与行为模式识别，精准锁定诈骗行为。

在数据可视化与智能决策方面，反诈平台透过数据可视化技术，将复杂数据转化为直观图表、地图及关联图谱，展示资金流向、诈骗态势及团伙结构，实时检测与风险评估模型毫秒级响应，智能报告提升办案效率。“企查查”等平台利用智能算法识别虚假企业，助力跨境诈骗案侦破；“亚信科技反诈云系统”则事前预警、事中拦截与事后溯源，降低报案量。内地反诈体系结合法律、技术与协同治理，形成多层次防诈骗防线，提升公众防诈骗能力与打击效率。

（三）系统设计与核心技术

借鉴全球及内地反诈骗策略，本研究提出“数据引领，智能护航”的智能警务系统，通过与科技公司及金融机构合作，深度整合大数据与 AI/ML，实时威胁检测与异常行为识别。AI 技术融合警方报告、社交媒体等多元数据，深度分析诈骗行为模式与受害者特征，提升预警精准度。智能预警系统结合大数据，实时过滤诈骗电话与讯息。生成式 AI/ML 侦测虚假网站与评论，聊天机器人则主动对抗骗徒，增加诈骗成本。多模态数据融合整合语音、图像、文本，支持智能决策，强化诈骗识别与社会防诈意识。系统核心技术包括：

• 预测性分析：随机森林与 LSTM 预测高频通话、异常转账，提升风险预警。

• 深度学习：CNN 与 Transformer 检测深伪、网络钓鱼及 AI 生成诈骗内容。

• 大数据与区块链 :Hadoop、Spark 结合 Chainalysis 追踪资金流向。

• 图神经网络：GNN、Neo4j 映像犯罪网络，挖掘诈骗团伙结构。

• 用户行为分析：UEBA 整合社交、电邮通讯及交易数据，构建行为基线。

• 持续学习：增量学习与对抗训练，适应诈骗技术迭代。

五、智能警务系统的技术设计与应用

随着网络诈骗迅速增长，传统执法策略难以应对复杂的跨国诈骗活动。香港作为国际金融中心，需要一个主动、精准、AI 辅助的反诈骗警务系统面对深度伪造、跨境洗钱及社交媒体诈骗等挑战。以下考虑香港的法律、技术及社会环境，研究升级现有的“防骗视伏器”，新增自动化数据整合、预测性社交图谱、金融风控及连接证据收集功能至警方案件系统，与现有诈骗搜寻、来电及网站警示及举报功能互补，整合先进技术转型诈骗防治新蓝图。参考全球及内地的多源数据融合与实时分析，以下从四个技术层面阐述系统架构。

（一）自动化数据整合与跨行业协作

建基于现有 FMLIT 与警方、银行、储值支付工具及零售支付系统的情报交换，系统可采用联盟链交易与区块链分析技术打破数据孤岛，整合银行（如汇丰）、电讯商（如

香港电讯）、社交平台（如微信）及政府部门的脱敏数据（如帐户哈希值、异常行为标签）。整合现有的 JFIU 可疑交易举报，系统运用 Hadoop 数据湖、Spark 与 Chainalysis 分析银行账户、转数快及虚拟货币交易数据的可疑模式，预测性分析标记异常交易。系统强化认识你的客户（KYC）协议，通过地理空间分析审查交易地点，图谱分析挖掘犯罪团伙结构，生成统一风险数据库，与金融机构共享诈骗情报。系统自动检测可疑跨境交易，与现有转数快可疑识别代号警示联动，改善现有系统须要用户主动查询，促进银行、电讯商与警方的实时情报交换，提升检测效率。

（二）预测性社交图谱分析

AI 预测性社交图谱分析是技术核心。参考全球反诈骗的多源数据融合，图神经网络（GNN）与 Neo4j 可融合社交媒体、通信及交易数据，构建用户关系图谱，预测诈骗团伙与受害者风险。NLP 与 BERT 模型分析社交平台记录，识别诈骗语言模式（如保证高回报）；ResNet 检测深度伪造视频异常。大数据分析标记高风险传播节点，推送实时警报，降低诈骗成功率。研究显示，AI 基于一周数据预测违法事件准确率达 95.83%。香港可参考新加坡反诈骗机器人或意大利 KeyCrime，通过用户授权实时监测社交群组，识别投资诈骗路径与洗钱节点，参考内地可视化平台呈现犯罪网络，辅助警方主动干预。相较现有单点检测，AI 网络化预测显著提升效率，强化香港反诈能力。

（三）金融风控与实时警报

与现有 App 的警示不同，金融风控与实时警报功能聚焦诈骗事前预防。“防骗视伏器”新增用户自选风控模块，参考内地“延时到帐”，利用随机森林模型分析交易模式（如分散转入集中转出），触发“大额转账二次验证”或“陌生账户延迟到账”。在用户自愿授权下，用户行为分析（UEBA）整合社交媒体互动、电子邮件模式、电话通讯及金融交易数据，构建用户行为基线，配合 NLP 协助识别深伪钓鱼邮件或可疑短讯。异常检测模型（如孤立森林或自编码器）识别偏离基线的行为，如突然大量转账或点击假网站。UEBA 可协助分析诈骗集团模式，如多账户间快速资金流动，协助锁定犯罪网络，实时推送警报并联动银行与警方。系统主动检测高风险交易，动态风险评分优先处理高风险事件，自动化生成事件摘要，缩短反应时间，提升防范效率。

（四）证据收集与调查支援

有别于现有公众举报平台仅收集情报，智能证据收集功能强化警务调查的科学性与效率，优化证据管理。系统连接证据收集与分析功能至警方案件系统，协助调查。在用户预先自愿授权下，系统记录证据链，配合 NLP 提取通话录音的语音特征，确保通话记录及交易数据的完整性。运用 GNN 与 Neo4j，系统可识别诈骗指向同一暗网钱包，锁定主谋；AI/ML 分析历史诈骗数据，预测新兴集团模式，提升调查效率。系统与内地方面及国际刑警合作，应对跨境诈骗。法律方面建议设立反诈数据绿色信道，允许受害者签署“数据调取同意书”，快速调取证据，避免由申请法院令状延迟，缩短破案时间。此模块通过知识图谱与多源数据融合，推动侦查从单点分析转向系统性洞察，应用 AI 技术提升犯罪网络识别能力。

总结而言，“防骗视伏器”的智能警务系统通过自动化数据整合、预测性社交图谱、金融风控、证据收集，构建全链条防范

体系。香港可透过试点项目、自愿授权及专项立法，借鉴内地“全民反诈 App”与新加坡“ScamShield”的经验，逐步实施，长期融入智慧城市框架，为香港市民与企业提供强大安全保障。

六、结论与展望

为应对深度伪造、虚拟资产犯罪及社交工程攻击，智能警务系统借鉴全球及内地反诈经验，融合数据可视化与智能决策，提升对新型犯罪识别能力，长远联合科技企业、金融机构及电信商，开发大数据、信息网及深度伪造检测技术，建立数据共享平台，优化可疑 URL 与交易数据的实时互通，提升预警效率。借鉴各地防治策略、内地反诈骗体系与跨国情报共享经验，结合警方科技罪案警政顾问小组，协调反诈骗技术应用。参考内地“国家反诈中心 APP”,“防骗视伏器”的智能警务系统提供实时预警与防诈知识，增强市民防范意识，构筑一个坚韧的数字生态系统。分阶段应用、技术支持与国际协作是成功实施的关键。智能警务系统整合多源数据融合与 AI 技术，提升应对跨境洗钱与深度伪造等犯罪的能力。长远制度上需完善监管法规，参考内地反诈策略及新加坡共同责任与多方合作框架，强化防诈生态。有效的诈骗预防不仅保障金融系统，亦支撑经济稳定并保护投资者信任，但诸多考虑包括算法偏见的处理、确保可解释性，以及 AI 辅助证据在司法程序中的可接受性需要透明政策的支撑。未来应持续构建联防联控反诈骗生态系统，为香港智能城市建设提供实践蓝图。碍于海峡两岸及港澳地区法制不同，需要加强执法合作，打破地域与法制壁垒。通过分阶段部署及国际协作，多渠道教育提升公众意识，推动企业建立安全管理体系，促进金融与社会安全。

参考文献：

[1]初殿清．电信网络诈骗案件紧急止付的规范基础——兼论《反电信网络诈骗法》第二十条[J]．法学家．2022．6

[2]李益斌、刘洋．后疫情时代欧洲刑警组织数据保护的新态势探究[J]．信息资源管理学报．2021．4

[3]邱柏讯、周逸凡、简大为．智能巡逻结合5G边缘运算之创新应用[J]．电工通讯季刊．2020．25

[4]苏清伟、黄家扬．台湾地区内政部警政署“前瞻警政、科技警察”智慧联网项目．政府机关信息通报．2018．1

[5]萧舜文、孙雅丽、陈孟彰．虚拟化环境之僵尸网络恶意软件行为侧写与侦测[J]．Journal of Advanced Technology & Management．2015．1

[6]杨单璇、李灿松、胡伟、赖足兰、葛旭瑞．基于文献计量的智慧边境研究进展与展望[J]．Tropical Geograph．2025．1

[7]汤凯杰、洪长春、吴悦．新兴科技对社会包容之影响及其因应对策探讨[M]．财团法人国家实验研究院科技政策研究与信息中心．2023

[8]张玮玲．基于行为分析与机器学习的Android恶意软件检测方法[D]．清华大学资讯工程学系所学位论文．2015

[9]张亚伟、霍敏霞、贾全秋、薛富城基于区块链的反诈骗系统框架设计与分析[J]．Computer Science and Application．2022．12

责任编辑　张树彦