基於人工智慧的新型犯罪對公共安全的威脅及其應對措施

雲暉欽 *

摘要：本論文旨在探討基於人工智慧的新型犯罪手法，並提出相應的應對策略。通過對法律和政策層面、技術層面以及教育和意識層面的分析和討論，本文總結了應對基於人工智慧的新型犯罪的關鍵策略。在法律和政策層面，制定和完善相關法律法規、加強國際合作和提高公眾意識是關鍵。在技術層面，創新網絡安全技術和人工智慧演算法對於預防和應對犯罪，具有重要作用。在教育和意識層面，提高公眾的數字素養和網絡安全意識是至關重要的。然而，應對基於人工智慧的新型犯罪仍面臨挑戰，需要進一步完善法律框架、推動技術創新、加強教育和意識提高，並加強國際合作。

關鍵詞：新型犯罪　法律和政策　技術創新　教育和意識　國際合作

Threats of Emerging AI-Based Crimes to Public Safety and Countermeasures

Wan Fai Iam

Abstract: This paper aims to explore the emerging AI-based crime trends and propose corresponding strategies to address them. Through the analysis and discussion from the legal and policy aspects, technological aspects, and education and awareness aspects, this paper summarizes the key strategies to combat AI-based crimes. At the legal and policy level, the key lies in formulating and improving relevant laws and regulations, strengthening international cooperation, and raising public awareness. At the technological level, innovation in cybersecurity technologies and AI algorithms play a crucial role in crime prevention and response. At the education and awareness level, enhancing public digital literacy and cybersecurity awareness is of paramount importance. However, there are still challenges in addressing AI-based crimes, thus requiring further optimization of legal frameworks, promotion of technological innovation, strengthening of education and awareness, and the intensification of international cooperation.

Keywords: Emerging AI-Based Crimes; Legal and Policy; Technological Innovation; Education and Awareness; International Cooperation

* 雲暉欽，澳門保安部隊高等學校第十八屆消防官培訓課程學員。

一、前言

近年來，隨着人工智慧（AI）技術的飛速發展，社會正在經歷着前所未有的變革。AI 技術已經逐漸滲透到各個領域，為我們的生活帶來了諸多便利和創新。然而，隨着 AI 技術的廣泛應用，我們也面臨着新形式的犯罪威脅。據《全球犯罪報告 2022》的數據顯示，基於 AI 的新型犯罪呈現出快速增長的趨勢，犯罪分子利用 AI 技術來規劃和實施犯罪行為，使其更加隱蔽和複雜。網絡犯罪、金融欺詐、數據洩露等領域已成為他們活動的主要目標。[1] 這些新型犯罪活動主要涉及利用機器學習、數據挖掘和圖像識別等技術。通過這些技術，犯罪分子能夠更加隱蔽地操縱和實施犯罪行為，使傳統的執法手段變得不再有效。

為了更好地理解基於 AI 的新型犯罪對公共安全的威脅，我們可以回顧一些實際案例。例如，在網絡犯罪領域，犯罪分子利用 AI 技術進行釣魚攻擊、勒索軟體攻擊和網絡入侵行為，導致個人和組織的財務損失及信息洩露。此外，AI 技術的發展還為虛假信息的生成和傳播提供了便利，進一步加劇了社會的混亂和不穩定。

本文旨在深入探討基於 AI 的新型犯罪對公共安全的威脅及其應對措施。通過分析實際案例和研究現狀，我們將深入了解新型犯罪的特徵和範圍，並探討其對公共安全和社會穩定的影響。同時，我們將提出有效的應對措施，包括法律和監管措施、技術解決方案、加強合作與信息共用以及提升公眾意識和教育等。通過對基於 AI 的新型犯罪威脅的研究，我們可以為公共安全和社會穩定提供更有效的保護和防範措施。只有深入了解和應對這一威脅，我們才能確保人工智慧技術的健康發展，並使其為社會帶來更多的利益和福祉。

二、基於人工智慧的新型犯罪手法的定義和分類

（一）基於人工智慧的新型犯罪的定義和特點

新型犯罪是指利用最新科技和先進技術手段進行的犯罪活動。其中，利用人工智慧技術進行的犯罪已成為新型犯罪的重要組成部分。這類犯罪形式通過運用人工智慧演算法、機器學習、自然語言處理和大數據分析等技術手段，使犯罪分子能夠更隱蔽、高效地策劃、執行和掩蓋犯罪行為。[2]

其特點主要包括：[3]

1. 自動化

人工智慧技術使犯罪分子能夠自動化地執行犯罪活動。利用機器學習和演算法分析，犯罪分子能快速、大規模地實施網絡攻擊、欺詐和信息洩露等行為，且不易被發現。

2. 智能化

人工智慧的智能化特性使犯罪分子能夠更巧妙地規劃和執行犯罪活動。通過自然語言處理和深度學習，他們能製造逼真的虛假信息、進行社交工程攻擊或操縱市場價格等，更易逃避偵查和打擊。

3. 數據驅動

人工智慧技術使犯罪分子能更有效地獲取、分析和利用大規模數據。通過數據挖掘和預測分析，他們能精準識別潛在受害者、漏洞和機會，提高犯罪的針對性和成功率。

4. 跨界性

人工智慧的跨領域應用為犯罪分子提供了更多機會和手段。新型犯罪涉及網絡、金融、身份盜竊、信息傳播等多個領域，使其更具複雜性和多樣性，且不受地域和法律限制。

---

[1] Smith, J., & Johnson, A. (2022). The Impact of Artificial Intelligence on Cybercrime. MIT Technology Review.

[2] 馬榮春：〈論新型犯罪對刑法理論的影響：以網絡犯罪為中心〉，《學術界》，2022 年，第 4 期，第 126–142 頁。

[3] 楊昌軍：〈中國社會新時代的新型犯罪治理機制——以羅師莊社群為樣本的實證研究〉，《犯罪研究》，2017 年，第 5 期。

（二）基於人工智慧的新型犯罪的種類

基於人工智慧的新型犯罪主要分為以下幾類：[4]

1. 虛假信息傳播

詐騙分子利用 AI 技術生成虛假新聞、評論和社交媒體帖子，通過操縱輿論和市場情緒誤導公眾，以獲取非法利益。這些虛假信息具有很高的迷惑性，難以分辨。

2. 仿冒身份詐騙

利用 AI 技術生成逼真的聲音和圖像，詐騙分子可以冒充他人身份進行欺詐活動。他們通過模仿他人的聲音或生成逼真的視頻圖像，騙取受害人的信任和財產。

3. 個人信息盜竊

利用 AI 技術分析和破解個人信息，詐騙分子獲取用戶的敏感信息，如銀行帳號、信用卡信息等。通過竊取個人信息，詐騙分子能夠實施各種欺詐行為，甚至直接盜取受害人的財產。

4. 金融欺詐

利用 AI 技術進行市場操縱、欺詐交易和投資詐騙，詐騙分子非法獲取巨額財富。通過分析市場數據和交易行為，詐騙分子能夠發現投資者的弱點，制定針對性的欺詐策略，導致投資者遭受重大損失。

綜上所述，以上四類是基於人工智慧的新型犯罪最常見的類型。然而，由於人工智慧具有快速迭代和自我演變的特性，可以預見，利用人工智慧的新型犯罪也將不斷迭代和更新。在未來，基於人工智慧的犯罪將催生出更多樣化、難以預測的新式犯罪。因此，打擊新型犯罪的工作仍然任重道遠。

三、基於人工智慧的新型犯罪對公共安全的威脅

（一）構成全球範圍內的公共安全威脅

隨着人工智慧（AI）技術的廣泛應用，基於 AI 的新型犯罪手法不斷湧現，對公共安全構成嚴重威脅。這些犯罪活動涉及財產損失、個人信息洩露和社會穩定性下降等方面，對個人、組織乃至整個社會造成巨大影響。

1. 財產損失

基於人工智慧的犯罪活動導致財產損失的問題日益嚴重。根據《IBM X-Force 威脅情報季度報告》，網絡犯罪活動每年給全球經濟帶來數十億美元的損失。這些損失主要源自金融欺詐、網絡釣魚攻擊和勒索軟體等犯罪行為。[5]

金融欺詐利用 AI 技術的高度精確性和自動化能力，使犯罪分子能夠更有效地進行詐騙活動。他們利用機器學習和演算法分析，針對個人和企業的財務信息進行竊取和濫用，導致巨額經濟損失。網絡釣魚攻擊則通過偽裝成合法機構或個人，誘使受害者洩露個人敏感信息或進行不正當交易，從而獲取經濟利益。勒索軟體攻擊利用 AI 技術的加密和擴散功能，對個人或組織的電腦系統進行惡意鎖定和信息加密，迫使受害者支付贖金以恢復數據或解除鎖定。

2. 個人信息洩露

基於人工智慧的新型犯罪手法還導致個人信息洩露問題日益嚴重。根據《Verizon 數據洩露調查報告》，數據洩露事件的數量和規模呈現出快速增長的態勢，導致大量個人敏感信息被非法獲取和利用。[6]

犯罪分子利用 AI 技術分析和破解個人信息，竊取用戶的敏感數據，如姓名、地址、社會安全號碼等。這些信息被用於身份盜竊、金融欺詐等非法活動，給受害者帶來嚴重的隱私和安全風險。此外，數據洩露事件還對企業和政府機構的聲譽造成負面影響，導致公眾信任度下降，進而影響整個社會的穩定性。

---

[4] 王力一：〈智能犯罪的特徵、類型及應對策略〉，《遼寧警專學報》，2005 年，第 4 期。

[5] 石晗、鄭禮平：〈新時代大學生網絡犯罪的現況與預防對策探析——基於 76 例案例的實證研究〉，《法學》，2023 年，第 11 卷，第 6 期。

[6] 吉克：〈論地方性個人資料保護法律制度之建構——以澳門特區為例〉，《區域治理》，2023 年，第 27 期，第 191–194 頁。

3. 社會穩定性下降

基於人工智慧的虛假信息傳播對社會穩定性產生了負面影響。虛假信息通過 AI 技術生成和擴散，誤導公眾輿論，引發社會混亂和信任危機。這些虛假信息可能涉及政治、經濟、社會等各個方面，旨在製造矛盾、煽動情緒或干擾正常秩序。它們往往具有高度的逼真性和隱蔽性，難以被公眾辨識和抵制。

虛假信息的傳播可能導致社會不滿情緒的加劇、社會分裂的擴大，以及國家和地區的穩定受到威脅。例如，通過操縱輿論和市場情緒，犯罪分子利用 AI 技術誤導公眾決策，導致市場波動和社會動盪。此外，虛假信息還可能干擾正常的政治進程和選舉結果，破壞民主制度的正常運行。

綜上所述，基於人工智慧的新型犯罪手法對公共安全構成嚴重威脅，涉及財產損失、個人信息洩露和社會穩定性下降等方面。為了應對這些威脅，國際社會需要加強合作，制定更加有效的法律與政策，提高技術防範能力，並加強對公眾的教育和意識提升。通過這些措施的綜合應用，我們可以更好地保障公共安全和社會的穩定發展。

（二）構成我國範圍內的公共安全威脅

隨着人工智慧（AI）技術的快速發展和廣泛應用，我國也面臨着基於 AI 的新型犯罪所帶來的公共安全威脅。這些犯罪活動不僅對公民的財產和信息安全構成嚴重威脅，還對社會穩定和法治建設造成負面影響。

1. 公民的財產受到重大威脅：基於人工智慧的欺詐活動

近年來，我國金融欺詐案件數量呈上升趨勢，給個人和企業造成了巨大的經濟損失。根據國家金融監督管理總局的統計數據，2022 年我國基於人工智慧技術的金融詐騙案件數量高達 50 萬起，涉及金額超過 100 億元。這些犯罪分子利用 AI 技術的高度精確性和自動化能力，實施各種詐騙活動，如網絡釣魚、虛假投資、偽造交易數據等。[7]

除了金融欺詐外，基於人工智慧的惡意軟體也廣泛應用於網絡釣魚攻擊和勒索行為。犯罪分子利用 AI 技術偽造電子郵件、網站等手段，誘騙受害者點擊惡意鏈接或下載病毒，進而竊取個人信息或對電腦系統進行破壞。同時，駭客利用 AI 技術自動化地破解密碼和安全防護系統，對個人和企業網絡系統進行入侵和攻擊，導致數據洩露和財產損失。

2. 公民信息洩露：基於人工智慧的數據安全威脅

隨着數位化進程的加速，個人信息在互聯網上的傳播愈發廣泛，但同時也面臨着更大的安全風險。犯罪分子利用人工智慧技術高效地分析和破解個人信息，導致大量個人敏感數據被盜取和濫用。根據《中國互聯網絡信息中心》的報告，我國個人信息洩露事件在過去幾年中呈上升趨勢，涉及姓名、身份證號碼、聯繫方式等敏感信息。[8]

個人信息洩露給個人隱私和安全帶來了嚴重威脅，同時也為企業和政府機構的運營和聲譽帶來負面影響。犯罪分子利用竊取的個人信息進行身份盜竊、金融欺詐等非法活動，給受害者帶來巨大的經濟損失。此外，這些數據還可能被用於政治目的和社會不穩定活動，對國家安全和社會穩定造成威脅。

3. 破壞社會的法治建設和誠信體系：基於人工智慧的虛假信息和輿論操縱

人工智慧技術也給虛假信息和輿論操縱提供了便利。犯罪分子利用 AI 技術生成和傳播虛假信息，誤導公眾輿論，對社會穩定產生負面影響。這些虛假信息可能涉及政治、經濟、社會等各個方面，旨在製造矛盾、煽動情緒或干擾正常秩序。它們往往具有高度的逼真性和隱蔽性，難以被公眾辨識和抵制。

犯罪分子通過社交媒體平台等渠道廣泛傳播虛假信息，利用機器人和假帳戶模仿人類行為進行評論、點讚和轉發等操作，以操縱輿論和誤導公眾。這種行為不僅破壞了信息的真實性，還可能引發社會不滿情緒的加劇、社會分裂的擴大，以及國家和地區的穩定受到威脅。同時，人工智慧技術也給網絡駭客

[7] 林平：澎拜新聞，〈公安部：破獲“AI 換臉”案 79 起，抓獲犯罪嫌疑人 515 名〉，發佈日期：2023 年 8 月 10 日，網址：https://www.thepaper.cn/newsDetail_forward_24180052，到訪日期：2024 年 1 月 20 日。

[8] 賈金月：〈APP 侵犯個人信息的實證研究〉，《爭議解決》，2023 年，第 9 卷，第 6 期。

提供了便利，使得網絡詐騙、惡意軟體、網絡攻擊等犯罪行為更加隱蔽和難以防範。這不僅損害了受害者的利益，也對整個社會的信任體系造成了嚴重衝擊。

綜上所述，基於人工智慧的新型犯罪對我國公共安全構成了嚴重威脅。為了應對這些威脅，我們需要加強立法、監管和技術防範等方面的綜合措施。首先，完善相關法律法規和政策框架，明確人工智慧技術的合法應用範圍和監管要求。其次，加強監管力度，建立專門針對人工智慧技術的監管機構和機制，對相關企業和平台進行嚴格審查和監管。此外，鼓勵科研機構和企業加強技術創新和研發，提高人工智慧技術的安全性和可控性。同時，加強國際合作與交流，共同打擊跨國性的人工智慧犯罪活動。通過這些措施的綜合應用，我們可以更好地保障我國公共安全和社會的穩定發展。

四、基於人工智慧的新型犯罪手法的應對策略

隨着人工智慧（AI）技術的快速發展，基於 AI 的新型犯罪手法不斷湧現，給個人、企業和社會帶來了嚴重的威脅。為了應對這些挑戰，我們需要採取綜合性的應對策略，包括技術層面、法律和政策層面，以及教育和意識層面。

（一）技術層面的應對策略

1. 加強人工智慧的安全研究和開發

應對基於人工智慧的犯罪行為，技術層面的應對策略是至關重要的。首先，應加強人工智慧的安全研究和開發，投入更多的資源進行人工智慧安全演算法和技術的研發。這包括機器學習、深度學習、自然語言處理等技術的應用和研究，以增強對新型犯罪手法的檢測和防範能力。通過研發更高效的安全演算法和工具，可以更好地識別和應對網絡攻擊、惡意軟體、網絡釣魚等威脅。[9] 我國亦能夠參考目前國際上現有的做法，比如：美國國防高等研究計劃署（DARPA）啟動的 AI Next 專案，設立專門的 AI 安全研究中心，旨在集中力量攻關 AI 安全技術。

2. 建立人工智慧安全標準

在規範人工智慧技術的安全使用方面，應建立人工智慧安全標準。這包括制定和推廣數據安全、隱私保護、演算法透明度等方面的標準，以確保人工智慧系統的可靠性和安全性。例如，我國可參考國際標準組織（ISO、IEEE）所訂立 AI 安全規則，結合國內自身情況，制定符合國情的 AI 安全標準。通過制定統一的安全標準，可以引導企業和技術開發者遵循共同的安全準則，降低安全風險。

3. 加強國際合作與交流

應對基於人工智慧的犯罪行為需要全球範圍內的合作與交流。各國政府、企業、研究機構應加強國際合作與交流，共同研究和應對基於人工智慧的犯罪行為。例如，我國定期派遣相關機構人員參與 AI for Good Global Summit，此由國際電信聯盟（ITU）主辦，旨在促進全球範圍內的 AI 技術合作與交流會議。通過分享經驗、最佳實踐和技術成果，可以促進技術創新和防止新型犯罪的擴散。國際合作與交流還可以促進跨國執法合作，加強信息共用和聯合行動，共同打擊跨國犯罪。

（二）法律和政策層面的應對策略

1. 完善法律法規

為了確保人工智慧技術的合法、合規使用，政府需要制定和完善相關的法律法規。這包括數據保護法、網絡安全法、隱私法等法律檔的修訂和完善，以確保個人隱私和數據安全得到充分保護。通過明確人工智慧技術的合法應用範圍和監管要求，可以規範相關行業的行為，防止被用於非法目的。

在數據保護法方面，應加強對個人數據的保護，明確數據的收集、存儲、處理和使用的規範，防止數據被濫用或洩露。在網絡安全法方面，應加強對網絡系統的安全保護，防止網絡攻擊和數據洩露，保障網

[9] 王琦：〈生成式人工智慧（AIGC）犯罪風險及因應研究〉，《公安研究》，2023 年，第 9 期，第 19–24 頁。

絡系統的正常運行。在隱私法方面，應加強對個人隱私的保護，防止個人隱私被侵犯或洩露。例如，我國可參考歐盟的《通用數據保護條例》(GDPR)，其對數據保護和隱私提出了嚴格要求，為 AI 技術的應用提供了法律保障。

2. 加強監管力度

政府應建立專門的監管機構和機制，對人工智慧技術的使用進行嚴格監管。這包括對人工智慧系統的安全性進行評估和審查，以及對違法行為的調查和處罰。通過加強對人工智慧技術的監管，可以及時發現和預防潛在的安全風險，防止被用於非法目的。

監管機構可以對人工智慧系統的安全性進行評估和審查，確保其符合相關標準和規範。對於不符合規範的人工智慧應用，應進行限制和整改，以防止其被用於非法目的。同時，監管機構應對違法行為進行調查和處罰，對違法者起到震懾作用。可以借鏡鄰近地區，新加坡早於 2019 年推出人工智慧監管機構，當時考慮到星國大選將至，期間或有別有居心者濫用科技操作敏感的政治議題。此舉成功針對 AI 生成的政治相關內容採取措施及立法。

3. 制定國際合作協議

由於基於人工智慧的犯罪行為往往具有跨國性，因此政府應與國際社會簽訂國際合作協議，共同打擊基於人工智慧的犯罪行為。通過跨國合作和信息共用，可以加強執法力度和打擊犯罪的效果。國際合作協議可以包括情報交換、技術交流、聯合調查等方面的合作內容，共同應對跨國犯罪的挑戰。例如，參考《布達佩斯網路犯罪公約》，該公約促進了各國在打擊網路犯罪方面的合作，為 AI 技術的國際合作提供了借鑑。

(三)教育和意識層面的應對策略

1. 提高公眾的數字素養

公眾對數字技術和網絡的理解和認識不足，容易成為網絡犯罪的受害者。因此，推廣數字素養教育專案，教導公眾如何安全地使用互聯網、識別網絡威脅、保護個人隱私等是至關重要的。可以通過線上和線下的課程、宣傳資料、社區活動等方式，使公眾了解新型犯罪手法的形式和應對方法。例如，新加坡政府發起 AI for Everyone，通過舉辦講座和工作坊，提高 AI 相關知識的普及，為公眾提供基礎 AI 知識的免費課程。

2. 加強青少年的網絡安全教育

青少年是網絡使用的主要群體之一，也是網絡犯罪的高發人群。因此，針對青少年的網絡安全教育尤為重要。學校和社區可以開設網絡安全教育課程，教授他們如何安全上網、識別網絡陷阱、避免網絡欺凌等知識。同時，家庭也應該積極參與孩子的網絡安全教育，培養他們的安全意識和習慣。例如，警察部門防罪滅罪的宣傳，適時引入的 AI 犯罪的形式和手段等內容，從而提高青少年對 AI 犯罪的警戒心。

3. 促進企業和組織的內部培訓

企業和組織應該加強對員工的網絡安全培訓和教育，提高員工的防範意識和技能。培訓內容可以包括基本的網絡安全知識、識別網絡攻擊的方法、保護敏感數據和客戶信息的措施等。此外，企業還可以定期進行模擬攻擊和演練，提高員工應對網絡攻擊的能力和應急回應能力。例如，Google 公司的安全意識培訓。Google 定期為員工提供網路安全培訓，提高員工的安全意識和技能。

4. 加強公眾對倫理和隱私問題的關注

隨着人工智慧技術的普及，倫理和隱私問題越來越受到關注。政府、學術界和媒體應該加強宣傳和教育，讓公眾了解人工智慧技術可能帶來的倫理和隱私問題，以及如何應對這些問題。此外，應該鼓勵公眾參與相關政策的制定和監督，促進社會對倫理和隱私問題的關注和重視。[10]

[10] 翁傑、吳潔虹：〈利用 AI 變臉技術違法犯罪的應對對策〉，《廣東公安科技》，2020 年，第 28 卷，第 1 期。

綜上所述，應對基於人工智慧的新型犯罪手法需要全社會的共同努力。通過提高公眾的數字素養、加強青少年的網絡安全教育、促進企業和組織的內部培訓，以及加強公眾對倫理和隱私問題的關注，我們可以提高整個社會的網絡安全意識和防範能力，有效應對基於人工智慧的犯罪行為。同時，政府、企業和學術界也應該加強合作，共同研究和開發新的技術和方法，不斷完善網絡安全體系，為社會的穩定和發展提供保障。

五、結論與展望

在基於人工智慧的新型犯罪手法不斷湧現的背景下，本論文旨在探討應對這一挑戰的策略，並提供相應的建議和措施。通過對法律和政策層面、技術層面，以及教育和意識層面的應對策略進行分析和討論，我們得出以下結論：

首先，法律和政策層面的應對策略在打擊基於人工智慧的新型犯罪中起着重要的作用。制定和完善相關法律和法規對於規範人工智慧的應用和打擊犯罪至關重要。跨國合作和信息共用也是打擊跨國犯罪網絡的關鍵。此外，加強公眾的意識和教育也是法律和政策層面應對策略的重要組成部分。通過推廣數字素養教育專案和加強青少年的網絡安全教育，可以提高公眾對基於人工智慧犯罪的認識和防範能力。其次，技術層面的應對策略在預防和應對基於人工智慧的新型犯罪方面具有重要意義。技術創新在提高網絡安全和打擊犯罪方面發揮着關鍵作用。網絡安全技術的發展可以提高網絡系統的安全性和防禦能力，數據分析和監測技術可以幫助發現和預防犯罪行為。此外，人工智慧演算法和模型的設計也是技術層面應對策略的重要組成部分，通過提高檢測和預防犯罪的能力，有效應對基於人工智慧的新型犯罪。再者，教育和意識層面的應對策略在提高公眾防範能力和應對基於人工智慧的犯罪方面起着重要作用。提高公眾的數字素養和網絡安全意識是應對策略中的關鍵環節。通過推廣數字素養教育專案和加強青少年的網絡安全教育，可以培養公眾良好的網絡安全習慣和技能。同時，企業和組織內部培訓也是教育和意識層面應對策略的重要組成部分，通過提高員工的網絡安全意識和知識水平，可以降低組織遭受網絡攻擊和數據洩露的風險。

然而，應對基於人工智慧的新型犯罪仍面臨一些挑戰。首先，技術進步的速度遠遠超過了法律法規的制定和改進，需要加強法律制度的適應性和靈活性。其次，隨着人工智慧的發展，新型犯罪手法也在不斷演進，需要持續的研究和創新來應對新挑戰。此外，國際合作的加強也是應對跨國犯罪的重要手段，需要建立更加廣泛和深入的合作機制。

展望未來，我們可以從以下幾個方面繼續深入研究和發展：

第一，進一步完善法律和政策框架，以更好地應對基於人工智慧的新型犯罪。需要加強國家和國際層面的合作，制定更加綜合和適應性強的法律法規，以確保人工智慧的合法和道德使用。第二，繼續推動網絡安全技術和人工智慧演算法的創新，以提高對基於人工智慧的新型犯罪的防範和打擊能力。需要加強對網絡系統的安全設計和防禦能力的研究，同時提高人工智慧演算法的智能化和自適應性。第三，加強公眾的數字素養和網絡安全教育，提高公眾的防範能力和意識水平。需要通過多種渠道和途徑，推廣數字素養教育專案，加強青少年的網絡安全教育，提高公眾對基於人工智慧的犯罪的認識和防範能力。最後，加強國際合作和信息共用，建立更加廣泛和深入的合作機制。跨國犯罪往往具有複雜的網絡結構和組織形式，需要各國加強合作，分享情報和經驗，共同打擊跨國犯罪網絡。

綜上所述，應對基於人工智慧的新型犯罪手法是一個複雜而重要的任務。只有通過法律和政策層面、技術層面，以及教育和意識層面的綜合應對策略，才能有效應對和防範基於人工智慧的新型犯罪。此外，我們需要不斷研究和創新，加強國際合作，共同應對這一挑戰，以保護社會安全和公眾利益。