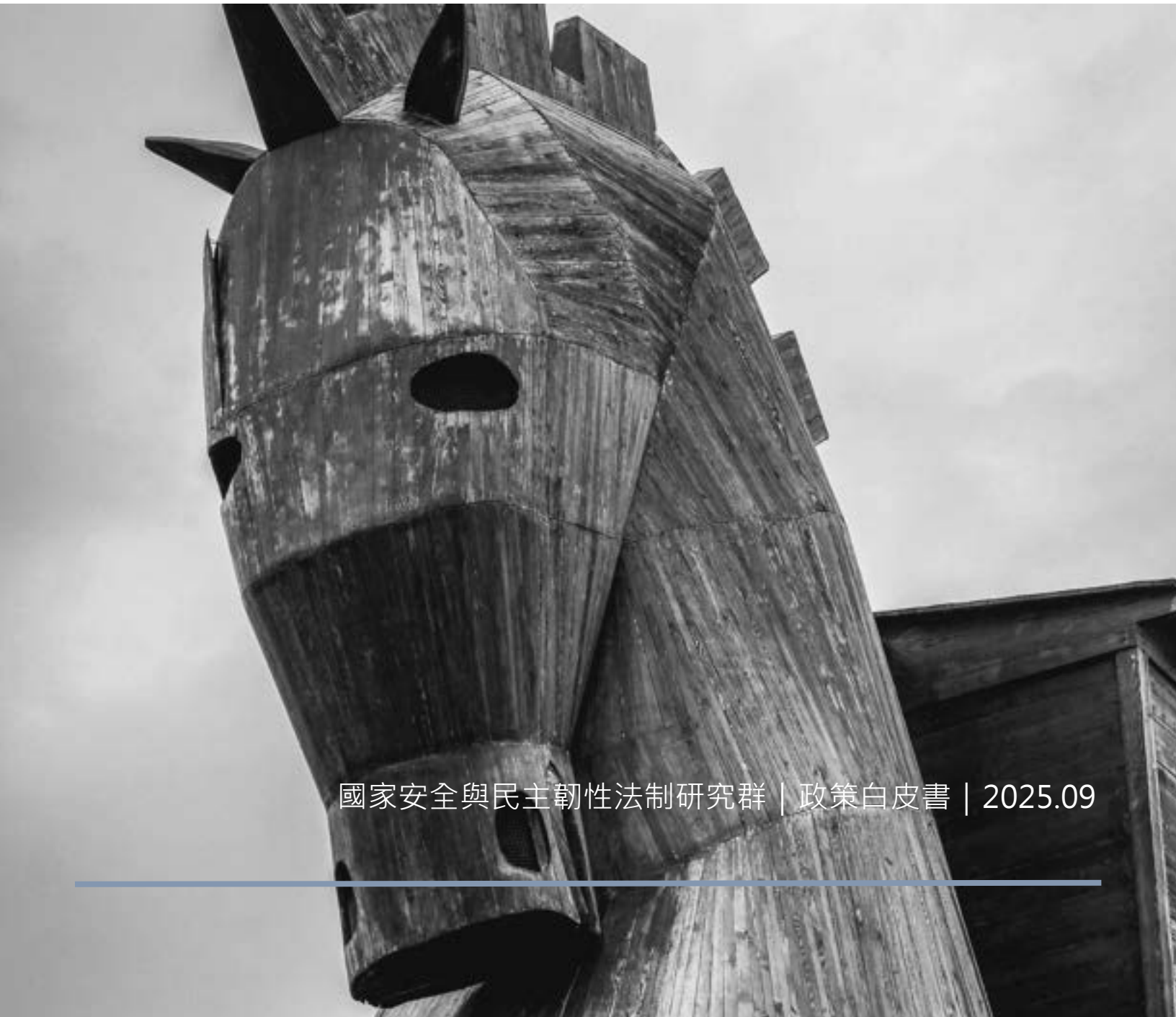
引進國家木馬
有效追訴國安犯罪

林鈺雄 教授

國立臺灣大學法律學院



國家安全與民主韌性法制研究群｜政策白皮書｜2025.09

摘要

我國在面對國安犯罪調查時，因加密通訊軟體廣泛使用而陷入「資訊斷鏈」困境。現行《通訊保障及監察法》僅適用於傳統電話監聽，無法有效處理端對端加密（E2EE）環境；我國也缺乏明確授權，允許執法單位在特定條件下植入「國家木馬」進行即時偵查，導致國安案件偵辦受阻。

本政策白皮書對各國比較法進行分析，並提出建議兩大方向：一是法律授權，建立小木馬（針對重大一般犯罪，如詐欺、毒品）與大木馬（限國安案件，如間諜、境外資金）的分級制度，並確保比例原則、司法審查與外部監督。二是技術自主，避免過度依賴國際供應商，應成立跨部會研發團隊，自主發展透明、安全且可控的木馬工具。唯有同步推進法制與技術，才能在數位時代有效偵辦國安案件，兼顧安全與人權保障。

國安風險辨識與風險分析

隨著資訊科技與數位通訊工具的普及，現代社會的溝通模式早已從傳統語音電話、簡訊，轉變為依賴各式即時加密通訊軟體，如 LINE、WeChat、Telegram、Signal 等。這些應用程式普遍採用端對端加密（End-to-End Encryption, E2EE）技術，使傳輸過程中資料即便遭到攔截，也無法解密還原原始訊息內容。

然而，這項技術進步雖保障了個人隱私，也同時被境外敵對勢力利用為滲透、傳遞情報與策劃行動的安全工具。近年共諜案、洩密案以及涉及境外資金的選舉不法行為皆顯示，這些行為人多透過加密通訊軟體聯繫與下達指令，導致我國偵辦機關面臨資訊斷鏈、溯源困難的處境。例如 2020 年總統選舉前，台北地檢署偵破中國湖南台辦資助台商協會涉入賄選案件，關鍵證據來自微信對話記錄與手機截圖；該案若無當事人手機的實體扣押，將無從得知通訊內容與幕後金流。

現行《通訊保障及監察法》雖提供執法機關聲請通訊監察的法源，但其設計主要以傳統電話通訊為基礎，對於網路加密通訊平台的監控能力極為有限，特別是在無業者配合、無後門機制情況下，通訊封包即便被攔截，仍無法解碼重組為可用資訊，導致調查人員「有看沒有到」。

此外，我國仍未建立明確授權制度，允許在特定情況下秘密植入監控程式（國家木馬），蒐集來自端點的原始通訊或裝置資料。這使得即便執法單位具備技術能力，也無法依法行使駭客式取證手段，甚至恐涉違法偵查風險，進而限制國安案件之調查範圍與效率。

再者，根據現行法規，執法機關多依賴事後搜索與扣押手機進行資料還原，卻忽略這些加密應用多具備「閱後即焚」、「密碼刪除」、「遠端清除」等功能，使得過往通訊資料在被查扣前即遭銷毀，根本無法回溯資訊鏈條。因此，在無法即時掌握對話內容與指令下達者身份的前提下，無論是追訴、定罪或阻止國安危機，皆如緣木求魚。

面對此一結構性偵查困境，亟需建構現代化通訊監控法制體系，引進「國家木馬」作為合法偵查工具，補足執法機關在數位通訊環境下的偵查缺口，並兼顧程序正義與基本權保障。

比較法參考

在資訊犯罪與國安威脅升高的國際背景下，多數民主國家已陸續修法，賦予執法機關在嚴格審查與監督下，合法使用木馬程式進行來源端通訊監察與秘密線上搜索。

- **德國**

德國為針對國家木馬設立明確法律依據的國家之一。其《刑事訴訟法》第 100a 條於 2017 年增修後，允許針對特定重大犯罪進行來源端通訊監察（Quellen-TKÜ），即秘密植入小型木馬程式，攔截在加密前的輸入資料或在解密後的接收資料，以避開 E2EE 的技術障礙。若需蒐集設備中已儲存的非通訊資料，則適用第 100b 條的「秘密線上搜索」（Online-Durchsuchung），亦即大木馬程式的運用。

德國法制上明確區分使用小木馬與大木馬的適用條件，並設有高標準的司法審查機制，要求由特定法官簽發令狀，並需具備必要性、適當性與比例性等法治要件。此外，所有使用記錄皆需存檔、接受外部監督，以防濫權與侵害基本權。

- **英國**

英國則於 2016 年通過《調查權力法案》（Investigatory Powers Act 2016, IPA），授權情報與執法機關得在獲得授權下進行「設備干預」，本質上即為國家木馬機制，涵蓋大、小木馬的使用情境。英國並保留業者協力義務制度，要求通信業者或平台提供特定技術配合，包括解密支援或資料協助，違者將面臨刑罰。此外，英國也設立獨立的監督機關進行事後審查，確保資訊取得與使用合法合憲，維持公眾對執法程序的信賴。

- **其他國家**

瑞士刑事訴訟法明文規定，可對特定重大犯罪案件施行來源端通訊監察，並限制其適用範圍與資料使用方式。其他如荷蘭、法國亦有專門法律制度支援類似監控技術，並強調跨國合作的重要性，如 EncroChat 跨境加密手機案件，即為歐洲執法機關透過木馬取得犯罪通訊之成功案例。

- **與我國之比較**

反觀我國，目前無明確法源授權執法機關植入木馬，僅有《通訊保障及監察法》與《刑事訴訟法》部分條文授權傳統掛線監聽或扣押資訊設備使用，但無法對應通訊及裝置加密等特性。即

便我國於 2024 年 7 月踏出第一步開始科技偵查的法制化，整體立法進度仍遲緩，造成執法技術與法制明顯脫節，對於國安案件的查緝與情報任務形成阻礙。

因應策略的政策建議

面對日益複雜的國安威脅與加密通訊所造成的偵查斷點，我國亟需從法律制度與技術發展兩個面向，雙管齊下，以有效補足目前國家安全偵查的制度與工具空缺。

A. 法律上明確授權使用國家木馬，分級適用

（1） 建議儘速推動修法，明文授權執法機關於特定情形得使用國家木馬程式。小木馬（來源端通訊監察）可應用於毒品、詐欺、人口販運等重大一般犯罪案件，透過植入方式取得通訊內容，避開端對端加密限制，以因應通訊加密化的趨勢。

（2） 大木馬（秘密線上搜索）：因其侵入範圍涵蓋裝置中所有資料，並具備錄音、定位等主動監控功能，應限定於涉及國家安全、間諜滲透、境外資金控制選舉等重大國安案件使用，且程序控制採最高規格，需經由高等法院專責法官個案核准，並納入外部監督機制。

（3） 如此設計，既可提供執法機關必要之數位偵查工具，也能防止過度擴權、侵害人權，符合比例原則與程序正當性。

B. 技術上發展國家本土木馬，擺脫技術依賴

（1） 除了法律授權，我國亦須重視國家木馬背後所涉及之核心技術問題。目前國際上可用於執法目的的監控工具，多由少數國家控制，如以色列、德國、美國等，其供應受限於地緣政治與出口管制法規。在台灣面對區域衝突與戰略風險上升的背景下，若過度仰賴境外供應商，一旦局勢惡化，將陷入「有法可用、無技可執」的困境。

（2） 政府應積極投入資源，建立跨部會「國家級數位偵查技術研發團隊」，結合資安專家與白帽駭客能量，自主研發符合我國法治與執行需求的木馬系統，並強化程式模組的透明性、安全性與可控性，避免被滲透或誤用。

（3） 唯有在法制授權與技術自主兩方面同步建構完整架構，我國才能真正建立數位時代的國安偵查體系，面對境外勢力滲透時有法可循、有技可施，確保國家安全與民主法治兼得。