科技法學評論，7 卷 2 期，頁 57（2010）

科法新論

從網路犯罪公約談我國妨害電腦使用罪章的修訂*

廖宗聖**、鄭心翰***

摘　要

電腦犯罪已成爲當代新興的犯罪類型，各國無不積極面對此一挑戰。我國在 2003 年新增刑法第 36 章妨害電腦使用罪章，除爲了解決電磁紀錄與動產、文書存在不同的屬性外，也希望藉由該章的制定，能對其他影響電腦系統安全、侵害電腦資料完整、保密及可使用的行爲加以規範。不過制定至今，該罪章產生不少解釋上或適用上的困難，爲解決種種相關的問題與爭議，本文在參考歐洲理事會網路犯罪公約的規範後（第 1 篇第 1 章第 2 條、第 4 條、第 5 條及第 6 條），嘗試對妨害電腦使用罪章提出相關修訂建議（第 358 條、第 359 第、第 360 條及第 360 條第 1 項、第 2 項），期能供立法者於未來修訂該罪章時的參考。

關鍵詞：電腦犯罪、網路犯罪、網路犯罪公約、濫用電腦、電磁紀錄

---

* 作者由衷感謝兩位匿名審查人寶貴的修正建議，讓本文更為完整，而作者亦獲益良多。

** 國立中正大學法律學系助理教授；美國威斯康辛大學麥迪遜校區法學博士。

*** 國立中正大學法律研究所碩士生。

投稿日：2010 年 7 月 18 日；採用日：2010 年 9 月 27 日

Cite as: 7 TECH. L. REV., Dec. 2010, at 57.

Amending Chapter 36 of the Penal Code of Taiwan on the Basis of the Study on the Cybercrime Convention

Tsung-Sheng Liao, Hsin-Han Cheng

Abstract

Computer crimes have become a new model of crimes and a new challenge for most countries over the world. In 2003, Taiwan enacted Chapter 36 of the Penal Code to deal with computer crimes. Although the new chapter avoided some application problems caused by treating electro-magnetic records as chattel and documents, the change of coping with computer crimes still raises other new problems. After exploring, this article argues that Taiwan could resolve those new problems by amending Chapter 36 of the Penal Code based on the comparison study of the Cybercrime Convention.

Keywords: Computer Crime, Cyber-crime, Cybercrime Convention, Misuse of Computer, Electro-magnetic Record

1. 問題的提出

電腦約莫在 1950 年誕生，它的發明使得大量的資料儲存、運算變的可能。初期僅用於軍事用途及科學運算，但後來隨著成本降低、體積縮小，逐漸在公司、個人間流行，作爲文書處理、商業管理、美術製圖及休閒娛樂的輕巧工具，可謂是繼工業革命後，影響人類最重要的發明，並經由網路的連結，形成了跨時代的「資訊革命」。

網際網路直到二十世紀末才正式興起，卻以驚人的速度席捲全球。1960 年代，美國國防部基於冷戰戰略上需要，開始發展電腦間的聯繫網路。到了 1990 年，網際網路正式開放給公眾使用，至今不過僅二十年的時間，卻已深深影響著人類的生活：舉凡市井小民上網閱讀報紙、購買商品、金融轉帳及聯絡通信，到跨國公司的子母公司間資訊傳遞、會議舉行，再到國與國間的聯繫、駐外代表會議等，無不因網路發展得以迅速、即時、低成本地進行著。

電腦與網際網路的發達帶給人類便利與好處，但也帶來許多挑戰。當中，如何預防、打擊電腦犯罪即是各國執法單位的一大挑戰。電腦犯罪具有身分隱匿、快速散布、證據難取得、證據容易銷毀、跨國管轄及修法落後等特質，因此，造成各國在偵查、執法上的困難，讓國家司法的公信力受到極大挑戰。

所謂的「電腦犯罪」有著不同的定義。最廣義的定義認爲，只要是跟電腦有關的犯罪都稱爲電腦犯罪，因此，不管是以電腦爲犯罪客體的犯罪或是以電腦爲犯罪工具的犯罪都稱爲電腦犯罪。歐洲理事會網路犯罪公約（The Council of Europe Convention on Cybercrime，以下簡稱「網路犯罪公約」[1]）即嘗試著規範此最廣義的電腦犯罪；最狹義的定義認爲，只有是以電腦爲犯

[1] The Council of Europe Convention on Cybercrime, Nov. 23, 2001, ETS NO. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [hereinafter Cybercrime Convention].

罪客體的犯罪才稱爲電腦犯罪，我國妨害電腦使用罪章即嘗試著規範此最狹義的電腦犯罪[2]。是以，我國妨害電腦使用罪章規範的電腦犯罪類型是含括於網路犯罪公約規範的電腦犯罪類型中。

2003 年刑法修訂時，我國考慮到電磁紀錄的可複製性不同於一般動產的性質，干擾電磁紀錄的本質與有形的毀損文書行爲亦不相同，因此，新增刑法第 36 章妨害電腦使用罪章，將原本第 323 條有關電磁紀錄以動產論的規定刪除，也將第 352 條第 2 項電磁紀錄的準文書規定刪除。

刑法第 36 章妨害電腦使用罪章規範無故入侵電腦的行爲；無故取得、刪除變更電磁紀錄的行爲；無故干擾電腦的行爲；製作惡意電腦程式的行爲等，使得我國電腦犯罪的規範體系更爲完整。但另一方面，卻也存在著諸多爭議與問題，尚待解決。諸如：1.刑法第 358 條：「破解」、「電腦系統之漏洞」存在解釋上的不確定性，而難以適用；該條同時具有舉動犯與結果犯的模糊性質。2.刑法第 359 條：「無故取得」與「無故刪除變更」二種行爲並無同類的關係，造成條文性質模糊；該條似乎爲雙重結果犯的立法方式，對刑事立法造成很大的挑戰。3.刑法第 360 條：「干擾」、「電腦程式」及「電磁方式」規定不夠明確，造成適用上的困難。4.刑法第 362 條：構成要件過度嚴格，容易造成適用時的漏洞；將製作犯罪物與行使犯罪物混同規定，使得規範不清。

爲解決前述種種問題與爭議，本文認爲我國未來修訂妨害電腦使用罪章時，可以參照網路犯罪公約關於狹義電腦犯罪部分之規定（保護法益係在確保電腦資料和系統的保密性、完整性和可用性），作爲修法時的參考。網路犯罪公約在 2004 年生效，而歐盟主要大國皆在這三、四年內批准，讓該公約對國內生效，美國亦是如此。由此可知，對於有效打擊電腦犯罪一事，各國尋求共同的刑事立法，乃爲世界之趨勢。對我國而言，雖然我國未能加入網路犯罪公約，但是在制定或修訂國內刑事法時，參酌網路犯罪公約規範，絕

2 參見林山田、林東茂、林燦璋，犯罪學，頁 513-515（2007）。

對是有助於我國電腦犯罪規範體系的完整。又網路犯罪公約是對締約國刑罰規範作最低程度的要求，締約國於立法、修法時，可依據國內電腦犯罪情形作較重的刑罰規定，因此，我國在參考網路犯罪公約修法時，亦須注意我國的特殊國情，適度調整之。

本文除問題提出部分外，另分爲四部分：第一部分介紹網路犯罪公約的制定與沿革；第二部分說明我國妨害電腦使用罪章的制定與沿革；第三部分以網路犯罪公約爲基礎，重新檢視我國刑法妨害電腦使用罪章，除了介紹刑法第 358 條、第 359 條、第 360 條及第 362 條的規範意涵外，亦探討與這些法條相關的爭議及評論，然後再說明網路犯罪公約的對應規範，並提出修法的建議；最後一部分則爲結論。

2. 網路犯罪公約的制定與沿革

在第 4 部分參照網路犯罪公約立法例，重新檢視我國妨害電腦使用罪章前，將於本部分及下一個部分就網路犯罪公約的訂定及我國妨害電腦使用罪章的制定與沿革加以說明，助於對網路犯罪公約架構有初步的認識，同時對我國妨害電腦使用罪章制定的前因後果有整體的瞭解，裨益第 4 部分的參照分析。

2.1 網路犯罪公約的訂定

經濟合作暨發展組織（Organization for Economic Co-operation and Development, OECD）從 1983 年開始進行一項網路犯罪立法研究，對各國網路犯罪立法從事比較分析，評估提出國際統一立法的可能性，並於 1986 年發表「電腦有關犯罪：法律政策分析」報告[3]。該報告提出一份研究各國立法例後的「最大公約數」網路犯罪清單，建議各國都應以刑罰相繩，這些犯罪分別

[3] Miriam F. Miquelon-Weismann, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 329, 332 (2005).

爲：詐欺和僞造、修改電腦程式和資料、著作權和電腦通訊的阻斷、營業秘密的竊取、未經授權地進入電腦[4]。

隨著經濟合作暨發展組織報告發表，1989 年歐洲理事會[5]亦發表了 No. R. (89) 9 電腦相關犯罪建議[6]，提出必須制定新的刑事實體法，將透過電腦網路進行不法行爲加以犯罪化[7]；1996 年 11 月歐洲理事會所屬歐洲犯罪問題委員會（European Committee on Crime Problems, CDPC）作成 CDPC/103/21196 決定，設立了研究網路犯罪的專家委員會[8]。其主要設立的緣由是認爲：藉由連結通訊和資訊使用者，創造了所謂的「網路空間」（cyber-space），而該空間被用來做正當用途使用的同時，也被用來犯罪，例如：破壞電腦系統的完整性、可使用性及保密性；使用網路來犯傳統的犯罪等[9]。因此，刑事法必須與資訊、通訊科技一同發展，並藉由國際間的法律協定和各國間的合作來打擊網路犯罪，才能達到成效[10]。

1997 年 4 月歐洲理事會部長會議決定設立新的委員會，因而作成 No. CM/Del/Dec (97) 583 決定，設立「網路空間犯罪專家委員會」（Committee

---

4 *Id.* at 332-33.

5 歐洲理事會並非是歐盟理事會（European Council），該理事會於 1949 年 5 月 5 日由 10 個歐洲國家在法國 Strasbourg 設立，主要宗旨係在宣揚人權、民主及法治的基本價值，目前有 47 個成員國（歐洲國家），5 個觀察員身分的國家：美國、加拿大、日本、墨西哥及梵諦岡。*Council of Europe in Brief*, COUNCIL OF EUROPE, http://www.coe.int/aboutcoe/index.asp?page=quisommesnous&l=en (last visited June 25, 2005).

6 Recommendation No. R. (89) 9 of the Committee of Ministers to Member States on Computer-related Crime.

7 Amalie M. Weber, *Cybercrime: The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425, 429 (2003).

8 *Explanatory Report to the Convention on Cybercrime*, COUNCIL OF EUROPE, para. 7, *available at* http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm (last visited July 13, 2010) [hereinafter *Explanatory Report*].

9 *Id.* para. 8.

10 *Id.* para. 9.

of Experts on Crime in Cyber-space, PC-CY）[11]。該委員會開始負責草擬網路犯罪公約，並於 2000 年 12 月 31 日完成初步工作，稱爲「歐洲理事會網路犯罪公約草案」[12]。該公約草案與解釋報告（Explanatory Report）[13]在 2001 年 11 月 8 日由歐洲理事會部長會議接受，並於 2001 年 11 月 23 日在布達佩斯（Budapest）開放簽署（CETS No. 185）[14]。

歐洲理事會成員國中的 26 個國家及 4 個非成員國，在網路犯罪公約開放簽署時即完成簽署[15]。該公約在經過 5 個簽署國批准後（阿爾巴尼亞、克羅埃西亞、愛沙尼亞、匈牙利、立陶宛），於 2004 年 7 月 1 日生效[16]。至於，網路犯罪公約對歐洲理事會成員國已生效的重要國家爲：法國（2006 年 5 月 1 日生效）、挪威（2006 年 10 月 1 日生效）、荷蘭（2007 年 3 月 1 日生效）、義大利（2008 年 10 月 1 日生效）、德國（2009 年 7 月 1 日生效）、葡萄牙（2010 年 7 月 1 日生效）、西班牙（2010 年 10 月 1 日生效）；未生效的國家爲：英國（未批准）、瑞士（未批准）、瑞典（未批准）[17]。對非成員國的生效情況爲：美國（2007 年 1 月 1 日生效）、加拿大（未批准）、日本（未批准）、南非（未批准）[18]。

---

11 *Id.* para. 12.

12 *Id.*

13 解釋報告雖然不是解釋歐洲理事會網路犯罪公約的權威性文件，但在解釋報告中指出，在本質上該報告是可以在適用公約時協助公約的解釋。

14 *Explanatory Report*, *supra* note 8, para. 15.

15 在網路犯罪公約開放簽署時，歐洲重要國家多已完成簽署：德國、法國、英國、瑞士、瑞典、荷蘭、挪威、芬蘭、西班牙、葡萄牙、義大利等，另外美國、加拿大、日本、南非亦完成簽署。*Chart of Signatures and Ratifications*, COUNCIL OF EUROPE, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (last visited June 25, 2010).

16 *Id.*

17 *Id.*

18 *Id.*

2.2 網路犯罪公約的內容

2.2.1 網路犯罪公約的宗旨

網路犯罪公約設定的目標與宗旨可以從該公約的前言得知。前言提到[19]：

1.網路犯罪公約會員國考慮到歐洲理事會的目標是達成其會員國的一致和諧。

2.網路犯罪公約會員國承認和該公約非歐洲理事會會員國合作的價值。

3.網路犯罪公約會員國確認追求打擊網路犯罪、保護社會之共同犯罪政策的需求，尤其是透過接受適當的立法和國際合作。

4.網路犯罪公約會員國意識到電腦網路數位化、匯流化及全球化的深遠影響。

5.網路犯罪公約會員國注意到電腦網路和電子資訊可能被用於犯罪的風險，同時關於這些犯罪的證據可能被儲存或傳輸於電腦網絡中。

6.網路犯罪公約會員國承認會員國和私人企業合作共同打擊網路犯罪的需求，以及保護使用和發展資訊科技的正當利益的需求。

7.網路犯罪公約會員國相信有效打擊網路犯罪將有賴持續增加、快速及運作良好的國際合作。

8.網路犯罪公約會員國確認該公約在制止破壞或濫用電腦系統、網絡、資料的保密性、完整性及可使用性的必要，而該制止是藉由將不法行爲的犯罪化，同時加強國內外偵查、起訴之權限來有效打擊網路犯罪，並提供快速、可靠的國際合作協議。

綜前可知，網路犯罪公約主要係在調和國內刑事實體法對網路犯罪的規範，提供國內刑事程序法上的權力，用於偵查及起訴網路犯罪，同時提供快

---

19 Cybercrime Convention, *supra* note 1, pmbl; *See also* Jay Fisher, *The Draft Convention on Cybercrime: Potential Constitutional Conflicts*, 32 UWLA L. REV. 339, 343-44 (2001).

速、可靠及有效的國際合作機制，共同打擊網路犯罪，保護國際社會的安全。

2.2.2　網路犯罪公約各章節規定

網路犯罪公約除前言外，共分爲 4 章，48 個條文：第 1 章爲定義，第 2 章規範國內必須採取的措施，第 3 章規範國際間合作及第 4 章規範條約最後條款。第 2 章國內必須採取的措施再細分爲第 1 節刑事實體法、第 2 節刑事程序法及第 3 節管轄權。第 3 章國際間合作再細分爲第 1 節一般原則及第 2 節具體規定。

根據第 2 章第 1 節，網路犯罪的類型分爲：1.侵害電腦資料和系統保密性、完整性和可用性的犯罪（第 2 條至第 6 條）；2.電腦相關犯罪（第 7 條及第 8 條）；3.內容相關犯罪（第 9 條）；4.侵犯著作權及相關權利的犯罪（第 10 條）。各條規定分別爲：第 2 條非法進入罪、第 3 條非法截取罪、第 4 條干擾資料罪、第 5 條干擾系統罪、第 6 條濫用設備罪、第 7 條電腦相關僞造罪、第 8 條電腦相關詐欺罪、第 9 條兒童色情罪、第 10 條著作權侵害罪、第 11 條意圖、幫助或教唆、第 12 條公司責任及第 13 條處罰及措施。

前述第 2 條至第 6 條規範侵害電腦資料及系統保密性、完整性、可用性的犯罪，係對以電腦爲犯罪客體的犯罪加以規範，也就是我國妨害電腦使用罪章嘗試規範之最狹義的電腦犯罪類型。又網路犯罪公約雖然使用「網路」（cyber）一詞，但在規範以電腦爲犯罪客體的犯罪時（網路犯罪公約第 2 條至第 6 條），如同我國妨害電腦使用罪章一樣，並未排除未連接網路的電腦犯罪。

此外，根據第 2 章第 2 節，打擊網路犯罪的偵查程序分爲：1.偵查權限及人權保障共同條款（第 14 條及第 15 條）；2.迅速保存已儲存的電腦資料及迅速保存和部分揭露傳輸的資料（第 16 條及第 17 條）；3.電腦資料提供命令（第 18 條）；4.搜索及扣押已儲存的電腦資料（第 19 條）；5.即時傳輸資料的蒐集和內容資料的截取（第 20 條及第 21 條）。至於第 2 章第 3 節則

規定網路犯罪管轄之規範（第 22 條）。

最後，網路犯罪公約關於國際合作部分規定於第 3 章，分別爲第 1 節一般原則：1.關於國際合作的一般原則（第 23 條）；2.引渡原則（第 24 條）；3.關於互助的一般原則及自發資訊（第 25 條及第 26 條）；4.在欠缺可用國際條約下，有關請求互助的程序，以及使用上的保密與限制（第 27 條及第 28 條）。第 2 節具體規定：1.關於互助的臨時措施：已儲存電腦資料的迅速儲存（第 29 條）、已保存傳輸資料的迅速揭露（第 30 條）；2.偵查權限的互助：已儲存電腦資料取得的互助（第 31 條）、經由同意或公開資訊而跨境取得已儲存的電腦資料（第 32 條）、即時傳輸資料蒐集的互助（第 33 條）、內容資料截取的互助（第 34 條）；3.全年無休聯絡據點的建立（24/7 網絡）（第 35 條）。

3. 我國妨害電腦使用罪章的制定與沿革

3.1 1997 年修法

於 1997 年時（歐洲理事會亦於同年成立網路空間犯罪專家委員會，負責草擬網路犯罪公約），我國發現電腦犯罪問題日益嚴重，因而開始著手修法。修法的方向分爲 3 類，第 1 類是以電腦（電磁紀錄）作爲行爲客體的犯罪，修訂條文分別爲第 220 條準文書、第 323 條準動產和第 352 條毀損文書罪；第 2 類是以電腦作爲犯罪工具或手段的犯罪，增訂條文分別爲第 318 條之 1 洩漏電腦或相關設備秘密罪及第 318 條之 2 利用電腦或設備的加重罪；第 3 類是關於詐欺機器或電腦罪，增訂條文分別爲第 339 條之 1 不正利用收費設備詐欺罪、第 339 條之 2 不正利用自動付款設備詐欺罪及第 339 條之 3 不正使用電腦詐欺罪。

由於本文討論重心將於刑法第 36 章妨害電腦使用罪章，因此，在探討 1997 年修法沿革時，僅討論與第 36 章妨害電腦使用罪章密切相關的部分，亦即前述第 1 類以電腦（電磁紀錄）作爲行爲客體的犯罪：第 220 條準文

書、第 323 條準動產和第 352 條毀損文書罪。

3.1.1　電磁紀錄文書化

第 220 條和第 352 條的修正，都是把電磁紀錄文書化，而爲準文書。但是第 220 條所屬的章節爲僞造文書印文罪章，係在保護社會交往的安全與公正性，屬於社會法益的保護，而第 352 條屬於財產犯罪中毀棄損壞罪章，是用以保護個人利益：所有人的所有權與物的持有利益，因此，雖然將電磁紀錄文書化，但關於電磁紀錄的保護範圍不應一概而論。

一般而言，刑法僞造文書印文罪章所指之「文書」必須具備 5 個要件：1.該文書具有意思表示；2.該意思表示具有權利義務的內涵；3.該意思表示記載在有體物上；4.該意思表示的記載得由感官直接識別；5.該意思表示來源可得確認[20]。而電磁紀錄即便具有前述 1.、2.、3.及 5.的要件，實際上卻無法由感官直接辨別，因此，不屬於傳統「文書」的類別。然而，由於電腦之使用日漸普及，並逐漸取代傳統文書之製作，用爲權利義務內涵的記載，是以，爲了確保社會信用關係，1997 年刑法第 220 條增訂電磁紀錄爲準文書。第 220 條第 1 項規定：「在紙上或物品上之文字、符號、圖畫、照像，依習慣或特約，足以爲表示其用意之證明者，關於本章及本章以外各罪，以文書論。」同條第 2 項規定：「錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以爲表示其用意之證明者，亦同。」第 3 項則參照日本刑法第 7 條之 2 之立法例，將電磁紀錄加以定義：「以電子、磁性或其他無法以人之知覺直接認識之方法所製成之紀錄，而供電腦處理用者。」

刑法毀棄損壞罪章中毀損文書罪（第 352 條）所指的「文書」係與僞造文書印文罪章所指之「文書」相同，都必須具備 5 個文書的要件，而電磁紀錄由於不具備可由感官直接辨別此一要件，因此，1997 年刑法第 352 條第 2 項增訂電磁紀錄爲準文書。第 352 條第 1 項規定：「毀棄、損壞他人文書或

20　林東茂，刑法綜覽，頁 2-254（2006）。

致令不堪用，足以生損害於公眾或他人者，處三年以下有期徒刑、拘役或一萬元以下罰金。」同條第 2 項規定：「干擾他人電磁紀錄之處理，足以生損害於公眾或他人者，亦同。」

刑法第 352 條所指之「文書」應與僞造文書印文罪章所指之「文書」作相同意涵的理解，也就是此等文書必須具備權利義務的內涵。同樣地，刑法第 352 條所指之電磁紀錄（準文書）也必須具備權利義務的內涵。當對毀損此條的文書或電磁紀錄課以刑罰時，意涵著對「具備權利義務內涵」之物的毀損，而非僅是對一般物之毀損。惟 1997 年增訂理由中僅謂：「干擾他人電磁紀錄之處理，足以影響電腦正常之運作……」，似乎未清楚說明刑法第 352 條毀損文書罪與刑法第 354 條毀損器物罪之差異。

3.1.2 電磁紀錄動產化

1997 年刑法第 323 條修訂，將電磁紀錄增列爲準動產，因此，當偷竊他人的電磁紀錄，就能以竊盜罪加以評價。但因爲電磁紀錄的屬性特殊，造成某些規範在適用上發生困難。

傳統中竊盜犯罪，皆以有形動產或不動產爲侵害對象，且對於客體的侵害是具有消長關係的存在，也就是破壞財產的監督權（持有利益）[21]；行爲客體受到侵害後，不可能發生持有利益仍存在的情況。而電磁紀錄具有可複製性和無耗損性，所以形成對利益的持有得以共存的現象，不會有傳統竊盜犯罪所生財物支配關係消長的問題[22]。又準用動產的能量，雖然也是無體物性質，但卻具有消耗性，無法複製而共同持有支配，所以和電磁紀錄並不相同。

---

21 竊盜罪保護的法益為何，在學說上有「所有權」及「持有利益」的爭議。採所有權法益說者，認為竊盜犯罪係保護所有權人在民法上的所有權利益；採持有利益說者，認為竊盜犯罪係保護持有人對財產的監督權。本文採持有利益說。盧映潔，刑法分則新論，頁 585（2008）。

22 柯耀程，「刑法新增『電腦網路犯罪規範』立法評論」，月旦法學教室，第 11 期，頁 118（2003）。另參見柯耀程，「『電磁紀錄』規範變動之檢討」，月旦法學教室，第 72 期，頁 123（2008）。

雖然將電磁紀錄視爲動產，準用竊盜犯罪中動產之規定會產生前述扞格的情形，但於 1997 年修法時，仍在刑法第 323 條增列電磁紀錄：「電能、熱能及其他能量或電磁紀錄，關於本章之罪，以動產論。」而立法說明中僅提到：「增列熱能及其他能量或電磁紀錄關於本章之罪，以動產論之規定，以應需要。」

3.2　1999 年修法及 2002 年修法

1997 年刑法第 323 條修訂後，將電磁紀錄增列爲準動產。雖然該準動產規定僅於竊盜罪章中，但基於 1997 年刑法修訂前規定，準動產可透過刑法第 343 條而準用於刑法第 339 條普通詐欺罪、第 340 條常業詐欺罪、第 341 條準詐欺罪及第 342 條背信罪等罪，因此，電磁紀錄的準動產性質也將準用於前述各罪中。但因爲 1997 年刑法同時增訂第 339 條之 1 不正利用收費設備詐欺罪、第 339 條之 2 不正利用自動付款設備詐欺罪及第 339 條之 3 不正使用電腦詐欺罪等三罪，讓原先第 343 條的準用各罪出現「失誤」，僅能準用於第 339 條之 3、第 340 條、第 341 條及第 342 條之罪，是以，1999 年刑法修訂時，修正第 343 條爲：「第三百二十三條及第三百二十四條之規定，於前七條之罪，準用之。」換言之，電磁紀錄視爲動產的規定，在普通詐欺罪、不正利用收費設備詐欺罪、不正利用自動付款設備詐欺罪、不正使用電腦詐欺罪、常業詐欺罪、準詐欺罪及背信罪皆得準用之。

在 1997 年及 1999 年刑法修正後，電磁紀錄以動產論的規定已適用於竊盜罪章，準用於詐欺背信及重利罪章（不含重利罪的準用），但仍未準用於同屬於財產犯罪之搶奪強盜及海盜罪章中，因此，在 2002 年修法時，刑法增訂第 334 條之 1，使電能、熱能及其他能量或電磁紀錄以動產論之規定亦準用於搶奪[23]強盜及海盜罪章：「第三百二十三條之規定，於本章之罪準用

23　有學者認為縱使不將電磁紀錄視為「動產」，它也是一種「利益」，因此，強盜、恐嚇取財、詐欺、背信等有得利罪規定者，本可適用於對電磁紀錄的犯罪，至於海盜罪、擄人勒贖或侵占罪則可藉由解釋，得出包含「不法利益」的意涵，而對電磁

之。」在立法說明中，並未說明爲何準動產有準用於搶奪強盜及海盜罪章的必要，至於在立法院司法委員會的審查過程中，亦無詳細的說明，僅當時任職法務部檢察司蔡碧玉司長提及：「我們認爲搶奪、強盜、海盜罪亦屬於財產犯罪，對上述規定也有適用的必要，所以亦將之列入本章中。」[24]

3.3 2003 年修法

1997 年、1999 年及 2002 年修法時，皆傾向將電腦犯罪視爲傳統的犯罪類型，使用「以……論」、「亦同」等類比、準用的立法模式來解決電腦犯罪刑罰問題，但以現實的角度來看，電磁紀錄所具有的獨特性質並不同於其他財產犯罪客體的特性，因此，當時採用的類比式立法模式係有不妥之處，常招致實務及學者的批評。2003 年修法時，考慮到電磁紀錄的可複製性，並爲了使電腦及網路犯罪的規範體系更爲完整，因此，刑法新增第 36 章妨害電腦使用罪章，並將原本第 323 條有關電磁紀錄以動產論的規定刪除（修正後的規定爲：「電能、熱能及其他能量，關於本章之罪，以動產論。」），將竊取電磁紀錄之行爲納入新增之妨害電腦使用罪章中，同時詐欺罪、背信罪、搶奪罪、強盜罪及海盜罪也不再準用。由 2003 年第 323 條修正說明可窺其始末：

「本條係八十六年十月八日修正時，爲規範部分電腦犯罪，增列電磁紀錄以動產論之規定，使電磁紀錄亦成爲竊盜罪之行爲客體。惟學界及實務界向認爲：刑法上所稱之竊盜，須符合破壞他人持有、建立自己持有之要件，而電磁紀錄具有可複製性，此與電能、熱能或其他能量經使用後即消耗殆盡之特性不同；且行為人於建立自己持有時，未必會同時破壞他人對該電磁紀錄之持有。因此將電磁紀錄竊盜納入竊盜罪章規範，與刑法傳統之竊盜罪構

紀錄犯罪適用之，不過搶奪罪部分，則難以想像如何搶奪電磁紀錄。李茂生，「刑法新修妨礙電腦使用罪章芻議（上）」，台灣本土法學雜誌，第 54 期，頁 235-236（2004）。

24 立法院公報，第 89 卷第 69 期，頁 138，2000 年 12 月。

成要件有所扞格。爲因應電磁紀錄之可複製性，並期使電腦及網路犯罪規範體系更爲完整，爰將本條有關電磁紀錄部分修正刪除，將竊取電磁紀錄之行爲改納入新增之妨害電腦使用罪章中規範。」

雖然把電磁紀錄以動產論的規定刪除，但不表示完全排除其具有財產利益的屬性，只是排除將電磁紀錄直接視爲相當於動產的概念，並作有體性和無體性的區隔，所以適用時，不可認爲對電磁紀錄的侵害型態，全無財產犯罪侵害的意涵存在[25]。

1997 年刑法修訂時，如同第 220 條增訂電磁紀錄爲準文書，立法者在第 352 條第 2 項增訂電磁紀錄亦爲適用毀損文書罪的準文書。2003 年增訂刑法第 36 章妨害電腦使用罪章後，立法者認爲第 352 條第 2 項「干擾」行爲的規定不夠明確，容易產生適用上之困擾，且「干擾」電磁紀錄的本質與有形的毀損文書行爲並不相同，所以將第 352 條第 2 項電磁紀錄的準文書規定刪除，另外增訂第 36 章第 360 條干擾電腦或相關設備罪[26]。

3.4　2005 年修法

2005 年刑法修訂時，由於電磁紀錄的定義，除了適用於刑法第 220 條僞造文書印文罪章外，亦適用於第 36 章妨害電腦使用罪章，因此，將原本第 220 條第 3 項有關電磁紀錄之定義：「以電子、磁性或其他無法以人之知覺直接認識之方法所製成之紀錄，而供電腦處理用者」，適度修正，並增列「光學或其他相類之方式所製成」後，再移列於刑法法例章第 10 條第 6 項中：「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄」，以讓該定義適用於刑法分則編中。

25　參見柯耀程，「刑法新增『電腦網路犯罪規範』立法評論」，前揭註 22，頁 119-120。

26　本文認為將刑法第 352 條第 2 項電磁紀錄的準文書規定刪除後，關於「干擾電磁紀錄」的處罰乃同時由刑法第 359 條取得、刪除變更電磁紀錄罪及第 360 條干擾電腦或相關設備罪加以評價。

4. 重新檢視我國刑法妨害電腦使用罪章

4.1 刑法第 358 條：無故入侵電腦或相關設備罪

刑法第 358 條[27]規定的行爲態樣分爲二個層次，也就是透過無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞等方式（第一層次的行爲），而入侵（第二層次的行爲）他人之電腦或其相關設備。

立法說明中指出對無故入侵他人電腦之行爲以刑罰相繩已是世界立法的趨勢，且電腦系統遭惡意入侵後，系統管理者必須耗費大量的時間與人力進行檢查、修復，才能確保電腦系統的安全性，因此，此種行爲之危害性已經達到科以刑事責任的程度，爲保護電腦系統的安全性，特增訂無故入侵電腦或相關設備罪。

4.1.1 入侵、無故輸入他人帳號密碼、破解使用電腦之保護措施及利用電腦系統之漏洞的意涵

4.1.1.1 入侵

刑法第 306 條侵入住居罪中規定的「侵入」與前述的「入侵」是否相同？或有所不同？刑法第 306 條第 1 項規定屬於作爲犯態樣，而第 2 項屬於不作爲犯態樣，也就是隱匿住居所內或受退去之要求（形成作爲的義務）而仍留滯（違反作爲的義務）；至於刑法第 358 條規定的「入侵」，有論者認爲它和刑法第 306 條規定的「侵入」是不同的概念，因爲很難想像入侵電腦後而不退去的情形，只要將網路線或電源線拔除就達到退去的目的[28]。惟仔細思考，是不是真的只要將網路線或電源線拔除就退去了？

假若 A 在其電腦中架設一資料庫，供大眾透過各自電腦進入瀏覽、存取

---

27 刑法第 358 條規定：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

28 張紹斌，「刑法電腦專章及案例研究」，軍法專刊，第 54 卷第 4 期，頁 87-88（2008）。

資料，並聲明任何人可以任何方式瀏覽、存取之。B 爲了搜尋、取得資料方便，設計了一個常駐的程式在 A 電腦中，每日自動將設定的關鍵字資料回傳給 B。某日，A 突然不願意再提供其資料庫供公眾免費使用，聲明只有付費取得密碼者方可進入使用。雖然 B 得知 A 的聲明，但 B 認爲其常駐程式不會被 A 發現，仍每天透過常駐程式接收資料。在這種情形下，似乎將網路線或電源線拔除後，該常駐程式並未退去。

前述案例即可說明，「入侵」電腦是有可能受退去之要求而仍留滯，或是隱匿其內，構成所謂不作爲犯的情形。又有論者認爲：單純的不作爲形式是被排除在刑法第 358 條適用的範圍之外，只有故意的作爲犯類型才成爲處罰對象[29]。此或許是認爲刑法第 358 條中所規定的第一層次的行爲態樣使然，也就是「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」、「利用電腦系統之漏洞」等基本上是故意作爲犯的行爲類型，很難想像可以構成故意不作爲犯的行爲類型。唯若仔細思考，假設一行爲人在出賣電腦前即預先植入木馬程式，似乎是可構成「利用電腦系統之漏洞」的不作爲犯。

4.1.1.2　無故輸入他人帳號密碼

「無故輸入他人帳號密碼而入侵他人之電腦」是構成刑法第 358 條最常見的情形，也是妨害電腦使用罪章中最容易觸犯的犯罪。有論者更大膽地認爲：基本上只有此一「無故輸入他人帳號密碼」構成要件能夠被實務界加以使用，另外兩個行爲態樣的規定並無太大用處，只要此構成要件該當就已解決電腦犯罪一半以上的問題[30]。

依照多數實務見解，所謂的「無故輸入他人帳號密碼」，是指行爲人沒有正當理由，在輸入他人帳號密碼後，進入到他人電腦系統內部，並處於隨時可取得內部資訊情形，例如：離職員工對公司主機輸入客戶的帳號密碼，取得客戶與公司往來業務資料；連線到他人的電子郵件伺服器，輸入他人的

29　柯耀程，「刑法新增『電腦網路犯罪規範』立法評論」，前揭註 22，頁 123。

30　張紹斌，前揭註 28，頁 88。

帳號密碼而進入[31]。相對地，雖然行爲人無權或越權使用他人電腦，只要他人的電腦已經開啓，無須輸入他人的帳號密碼即可加以使用，行爲人縱使處於隨時可取得該電腦系統內部資訊情形，實務見解認爲此並不構成刑法第 358 條之罪[32]。

4.1.1.3 破解使用電腦之保護措施

「破解使用電腦保護措施」是刑法第 358 條另一種第一層次的行爲態樣。實務案例中認爲，以欺騙的方式取得新密碼入侵電腦，此時帳號密碼機制是屬於所謂的「電腦保護措施」。法院認爲：得知他人帳號密碼後，如果直接輸入他人原本的帳號密碼，則構成「無故輸入他人帳號密碼」的行爲態樣，但輸入的若不是原本的帳號密碼，也就是另外取得新的密碼後而入侵，就是「破解使用電腦之保護措施」[33]。

4.1.1.4 利用電腦系統之漏洞

「利用電腦系統之漏洞」而入侵電腦的行爲態樣，目前實務上並無相關案例存在，再者，由於「電腦系統之漏洞」是一個相對性的用語，隨著科技的進步而有所不同，也因爲不同電腦系統廠商的製造能力不同而有所不同，實務上難以客觀認定，檢察官亦舉證困難[34]，因此，此一行爲態樣被認爲是不妥當的立法方式[35]。

---

31 台灣高等法院台南分院 96 年度上訴字第 153 號判決，司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm（以下所引用之判決來源本均相同）；台灣高等法院高雄分院 95 年度上易字第 872 號判決；蔡榮耕，「Matrix 駭客任務：刑法第 358 條入侵電腦罪」，科技法學評論，第 5 卷第 1 期，頁 108（2008）。

32 台灣高等法院 94 年度上易字第 1418 號判決。

33 台灣高等法院高雄分院 95 年度上訴字第 1589 號判決；蔡榮耕，前揭註 31，頁 111-112。

34 欲證明「漏洞」時，是要參照微軟的安全報告？其他系統軟體商的安全報告？行政院國家資通安全會報技術服務中心的通報？系統使用者所發現的安全問題回報？還是駭客組織所流傳的作業系統缺陷資訊？不一而足，因此難以舉證。參見張紹斌，前揭註 28，頁 89。

35 同前註，頁 89-89。

4.1.2　相關爭議問題

在立法理由中，對於入侵的解釋所涵蓋的範圍並未特別加以限制或說明，似乎可以看出我國刑法第 358 條可處罰行爲態樣的廣泛性，但在條文中對於入侵的方式，卻以第一層次的三種行爲類型加以限制，造成這三種行爲以外的入侵方式，在罪刑法定的原則下，不能以刑法第 358 條加以規範。就日新月異的電腦技術而言，這種第一層次行爲的規定，很有可能無法追上電腦科技進步的速度，造成規範上的漏洞。

從實務或學者對「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」、「利用電腦系統之漏洞」這三種行爲態樣的見解或意見中，可清楚得知，除了「無故輸入他人帳號密碼」外，「破解使用電腦之保護措施」與「利用電腦系統之漏洞」這二個類型的行爲態樣存在解釋上的不確定性。論者認爲：「破解」似乎非刑法用語，存在許多不確定性，執法人員如果沒有技術背景是無法理解它的真正意涵，但即便有技術背景者也很難想出適用情形，造成解釋上的困難，而難以適用[36]；同樣地，「電腦系統之漏洞」是一個相對性的用語，實務上難以客觀認定，執法者亦舉證不易。

至於，透過「無故輸入他人帳號密碼」此行爲態樣雖然可以解決大多入侵電腦的犯罪，但當行爲人無權或越權使用他人電腦，只要未輸入他人的帳號密碼，行爲人縱使處於隨時可取得該電腦系統內部資訊情形，並不構成刑法第 358 條之罪，造成和一般大眾的法感情相背離。

另外，依照我國刑法第 358 條二個層次的行爲類型觀之，該條是屬於舉動犯的性質，抑或是結果犯的性質，也存在著爭議。如果從第一層次的三個行爲類型來看，「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」與「利用電腦系統之漏洞」皆暗示著該條似乎是舉動犯的性質，也就是只要一從事這些行爲，構成要件即該當，無須等待特定結果的發生[37]。如果從我

36　同前註，頁 88。

37　柯耀程，「刑法新增『電腦網路犯罪規範』立法評論」，前揭註 22，頁 123。

國刑法第 358 條的立法說明觀之，該條保護的法益爲：電腦系統的安全性，因此，只要從事第一層次的行爲，即會對電腦的系統造成安全上的疑慮，也將該條指向是舉動犯的性質[38]。但是另一方面，第二層次的行爲態樣爲「入侵」，似乎要求必須有「侵入的結果」存在，構成要件才會該當，是以，該條應屬於結果犯類型[39]。我國刑法第 358 條規定似乎是舉動犯的類型，又似乎是結果犯的類型，造成本質上的矛盾，造成適用上的困擾。

4.1.3 網路犯罪公約規定：非法進入罪

網路犯罪公約第 2 條爲非法進入罪（illegal access）：「當故意且無權地進入全部或部分電腦系統時，每一個締約國須在其國內法採取可能必要的立法和其他措施而建立此一刑事犯罪。締約國可以要求犯罪的構成是：在意圖獲取電腦資料或其他不誠實的意圖下，而侵犯安全措施的行爲；或在一個電腦系統連結至另一電腦系統情況下的行爲。」

在原文中「非法進入」用字爲「illegal access」，「access」雖可翻譯爲「接觸」[40]，但「接觸」和本條規定：在意圖獲取電腦資料或電腦連結狀態下，而侵犯安全措施，會有想像上的差距。又解釋報告中指出，「access」包括對電腦系統的全部或任何部分的進入（電腦系統則包括：硬體、元件、已安裝的系統資料、目錄、與傳輸或內容相關的資料）[41]，故本文建議譯成「進入」，不僅較容易想像其非法情狀，也和一般認知不致產生過多的差距[42]。

---

38 同前註。

39 同前註。

40 參見馮震宇，「網路犯罪與網路犯罪公約（上）」，月旦法學教室，第 4 期，頁 133（2003）。

41 *Explanatory Report*, *supra* note 8, para. 46.

42 美國在 1986 年為了對抗電腦犯罪，制定了 CFAA（The Computer Fraud and Abuse Act），主要的處罰行為態樣並非入侵，而是無權或是越權使用電腦，其中第 1080 條(a)(2)為常用於對抗非法入侵電腦的條文，該條文禁止無權或越權「進入」電腦進

網路犯罪公約第 2 條前段是一個廣泛的規範，只要是故意且無權地進入電腦系統則該當構成要件，而該條後段則列出締約國可以附加的構成要件要素：1.意圖獲取電腦資料；2.其他不誠實的意圖；3.侵犯安全措施；或 4.在一個電腦系統連結至另一電腦系統情況下[43]。由締約國依據國內情況，自行決定是否要增加構成要件要素以及增加的範圍。

網路犯罪公約第 2 條規定與我國刑法第 358 條規定類似，皆認爲沒有權利而故意進入他人電腦的行爲須加以處罰。不過我國學說及實務對於第 358 條特別規定第一層次的三種行爲態樣有不少批評，認爲如此的立法方式過於限縮可能的行爲態樣，反而會形成立法漏洞。本文認爲網路犯罪公約第 2 條前段可以作爲我國修法時的參考，也就是將我國刑法第 358 條修訂爲：「無故入侵電腦或其相關設備，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」如此即可避免因電腦科技進步，而產生相關法律漏洞。至於網路犯罪公約第 2 條後段，關於締約國可以自行選擇增加的構成要件要素，我國於未來修法時可以參考之：是否需增加特定心意趨向的某種「意圖」？還是需要增加犯罪時的特定情狀？本文認爲並不需要，因爲參照前段所訂定的「無故入侵」已可明顯地彰顯出行爲的可非難性。

此外，關於我國刑法第 358 條二個層次的行爲類型規定，造成該條規定似乎是舉動犯的類型，又似乎是結果犯的類型，形成本質上的矛盾或不明

而取得資訊，其中對於進入（access），美國學理上提出兩種可能的解釋：虛擬進入說（virtual entrance）和下達指令說（instruction entrance）。

虛擬進入說認為電腦是電腦世界裡的一個空間，進入電腦則好像進入該處所，所以須使用鑰匙才能進入該處所，而鑰匙就是帳號密碼，輸入正確的帳號密碼才能進入內部，反之則不能；下達指令說認為在討論電腦犯罪，不用類比現實生活的空間，進入電腦就是使用者向電腦下達指令，而指令為電腦所接收。其時在大部分情形下，兩說會得到相同的結果，但在解釋上，下達指令說的範圍會比虛擬進入說還廣。蔡榮耕，前揭註 31，頁 113-116；EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET 62-63 (2d ed. 2004).

43 *Explanatory Report*, *supra* note 8, para. 50.

確。當第 358 條修訂爲「無故入侵電腦……」，即明確指出該條爲結果犯的類型，除了可避免前述類型上的矛盾或不明確，亦不會造成刑罰過早介入的弊病。至於，是否需對未遂行爲加以處罰，例如，輸入他人帳號密碼、破解電腦的保護措施、利用電腦系統漏洞入侵他人電腦，最後因自己力有未逮，而不該當犯罪，此一問題則有待考量社會對入侵電腦犯罪瞭解程度、執法單位適用入侵電腦犯罪情況，以及入侵電腦犯罪的實際發展情況後，再進一步討論、確定即可，無須過於躁進[44]。

4.2 刑法第 359 條：取得、刪除或變更電磁紀錄罪

刑法第 359 條[45]爲取得、刪除變更電磁紀錄罪，係基於「電腦已成爲今日日常生活之重要工具，民眾對電腦之依賴性與日俱增，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害……」等立法理由而訂定。

在 1997 年我國刑法增訂第 323 條，將電磁紀錄以動產論，而使之能以竊盜罪加以評價。1999 年及 2002 年修法後，電磁紀錄以動產論的規定除了適用於竊盜罪章外，擴大範圍亦準用於詐欺背信及重利罪章（不含重利罪的準用）及搶奪強盜及海盜罪章中。但因電磁紀錄具有可複製性和無耗損性，與傳統財產犯罪的客體「物」並不相同，所以 2003 年修法時刪除刑法第 323 條有關電磁紀錄以動產論的規定，而將原先「竊盜電磁紀錄」的行爲以刑法第 359 條加以評價。

此外，1997 年刑法修訂時，增訂第 352 條第 2 項將干擾他人電磁紀錄之處理亦以毀損文書罪論。2003 年刑法修正時，認爲第 352 條第 2 項「干擾」行爲的規定不夠明確，容易產生適用上之困擾，且干擾電磁紀錄的本質與有

44 參見蔡榮耕，前揭註 31，頁 127。

45 刑法第 359 條規定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

形的毀損文書行爲並不相同，是以，將第 352 條第 2 項電磁紀錄的準文書規定刪除，另以第 36 章第 359 條取得、刪除或變更電磁紀錄罪及第 360 條干擾電腦或相關設備罪加以評價。

4.2.1 無故取得、刪除或變更的意涵

刑法第 359 條所規範的第一種行爲類型是：「無故取得」，此係基於修法時將刑法第 323 條有關電磁紀錄以動產論的規定刪除後，原先「竊盜電磁紀錄」的行爲不再該當犯罪，所做的調整。企圖讓無故取得他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，仍受到刑罰的規範。無故取得是指在無正當原因下，也就是未被授權下，擅自取得屬於他人的電磁紀錄。行爲人須出於惡意，且因本條無未遂犯之規定，所以必須有所取得才該當刑法第 359 條。

刑法第 359 條所規範的第二種行爲類型是：「無故刪除或變更」，此則係因爲 2003 年修法時認爲第 352 條第 2 項「干擾」電磁紀錄的本質與有形的毀損文書行爲並不相同，將該項電磁紀錄的準文書規定刪除後，所做的調整。無故刪除或變更是指無正當原因而損壞、改變他人電腦或其相關設備的電磁紀錄而言，並且不論手段爲何，或是電磁紀錄可否事後回復。如果是破壞他人的硬體設備，進而導致電磁紀錄亦被損毀，則只能成立一般毀損罪，非這裡所謂的無故刪除或變更電磁紀錄[46]。

4.2.2 相關爭議問題

我國刑法第 359 條規定被認爲背離法定明確性原則的要求，因爲無故取得、刪除與變更他人電磁紀錄，會造成一種規範出現性質迥異的行爲態樣；「無故取得」和「無故刪除與變更」二類型的行爲並無前置的關係，亦無同類的關係，若將此二類型行爲置於同一條文中，會使該條文性質變的模糊不

46 柯耀程，「刑法新增『電腦網路犯罪規範』立法評論」，前揭註 22，頁 124-125。

清，無法明確[47]。再者，論者亦認爲，我國刑法第 359 條除了規定「無故取得、刪除與變更他人電磁紀錄」此一行爲結果外，另外加上「致生損害於公眾或他人」此一第二層次的結果要件，形成所謂雙重結果犯的立法模式，如此將會對刑事立法造成很大的挑戰，應使用「足生損害於公眾或他人」此一作爲行爲侵害的確認性佐證用語，較爲妥當[48]。

4.2.3 網路犯罪公約第 4 條：干擾資料罪

網路犯罪公約第 4 條爲干擾資料罪（data interference），第 1 項規定：「當故意且無權地損壞、刪除、破壞、修改、隱匿電腦資料時，每一個締約國須在其國內法採取可能必要的立法和其他措施而建立此一刑事犯罪。」第 2 項規定：「締約國可保留權利要求符合第一項描述的行爲造成嚴重危害才構成該罪。」此條規定主要係在提供電腦資料類似有體物不受到故意損害的保護，而保護的法益是電腦資料的整體性、正常運作性及儲存資料的可使用性[49]。

網路犯罪公約第 4 條類似於我國刑法第 359 條的立法規範，皆在保障電腦資料（電磁紀錄）不受到損害。不過二者在行爲手段上的要求上存在些許差異：公約第 4 條第 1 項列出五種行爲態樣：損壞、刪除、破壞、修改、隱匿，而我國刑法第 359 條只有三種行爲態樣：取得、刪除、變更。又論者批評我國刑法第 359 條同時規定「無故取得」和「無故刪除與變更」二種類型迥異的行爲，造成該條文性質模糊不清，違反法定明確性原則。是以，本文認爲網路犯罪公約第 4 條第 1 項可以作爲我國修法時的參考，也就是將我國刑法第 359 條修訂爲：「無故刪除、破壞、變更或隱匿他人電腦或其相關設備之電磁紀錄……。」關於刪除「無故取得」此一行爲態樣，一方面可以本文建議修訂後的刑法第 358 條「無故入侵」加以規範，另一方面也可避開違

47 同前註，頁 127。

48 同前註，頁 128。

49 *Explanatory Report*, *supra* note 8, para. 60.

反法定明確性原則此一問題。至於新增「破壞」、「隱匿」此二行為類型，則可更清楚顯示出我國刑法第 359 條所規範的行為態樣，進一步達到法定明確性原則。

網路犯罪公約第 4 條第 2 項規定，締約國可以訂定，在符合干擾電腦資料的行為時，仍必須該行為造成嚴重危害才加以處罰；我國刑法第 359 條亦訂有「致生損害於公眾或他人」此一結果要件，似乎與網路犯罪公約規定相呼應，皆是為了避免刑罰過早介入責難性不高的犯罪行為。透過立法方式，將原先僅須從事干擾電腦資料的行為，即應受到刑罰負面價值評價一事，也就是單純進行特定行為時，構成要件即該當的立法方式，提高至同時需有特定結果發生，而刑罰亦對該結果為負面的價值評價，此時構成要件才該當的立法方式。

4.3　刑法第 360 條：干擾電腦或相關設備罪

1997 年我國刑法修正時，增訂第 352 條第 2 項，將電磁紀錄準文書化，當被害客體是電磁紀錄時，可用毀損罪加以處罰，但之後增訂妨害電腦使用專章，則將第 352 條第 2 項刪除，相關犯罪行為以刑法第 359 條及第 360 條加以評價，而第 360 條[50]係處罰干擾電腦或相關設備使用的行為。

4.3.1　相關爭議問題

「干擾」一詞的意義為何？2003 年刑法修正時，將第 352 條第 2 項電磁紀錄的準文書規定刪除，當中一個理由是認為第 352 條第 2 項「干擾」行為

50　刑法第 360 條規定：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」立法說明中指出：「鑑於電腦及網路已成為人類生活之重要工具，分散式阻斷攻擊（DDOS）或封包洪流（Ping Flood）等行為已成為駭客最常用之癱瘓網路攻擊手法，故有必要以刑法保護電腦及網路設備之正常運作，爰增訂本條。又本條處罰之對象乃對電腦及網路設備產生重大影響之故意干擾行為，為避免某些對電腦系統僅產生極輕度影響之測試或運用行為亦被繩以本罪，故加上『致生損害於公眾或他人』之要件，以免刑罰範圍過於擴張。」

的規定不夠明確，容易產生適用上的困擾，但當以第 360 條干擾電腦或相關設備罪加以評價時，卻又繼續沿用「干擾」一詞，似乎未解決舊法的問題。再者，立法者爲了避免「干擾」一詞範圍過度廣泛，因此，加上了特定的行爲方式（科技手段）來限制——以電腦程式或其他電磁方式，然而，「電腦程式」及「電磁方式」對於法律人而言也難以認知[51]。

另外，亦有論者認爲，從增修理由中可知干擾行爲和物理性的毀壞並不相同，也將輕微的垃圾郵件轟炸排除，同時立法說明中指出，該條文是處罰「產生重大影響之故意干擾行爲」，是以，立法者似乎以爲只要將行爲類型加以限定，再將干擾結果最強部分和最弱部分去除之後，就可得到「干擾」的意義，但事實上是相反的，干擾一詞仍未被明確定義，日後適用上的恣意是無法避免[52]。

4.3.2 網路犯罪公約第 5 條：干擾系統罪

網路犯罪公約第 5 條爲干擾系統罪（system interference）：「當故意無權地藉由輸入、傳輸、損害、刪除、破壞、修改、隱匿電腦資料，而嚴重阻礙電腦系統的運作，每一個締約國須在其國內法採取可能必要的立法和其他措施而建立此一刑事犯罪。」此條規定主要係在處罰藉由使用電腦資料或影響電腦資料，而故意阻礙電腦系統的合法使用，保護的法益是電腦系統或通訊系統能夠適當地運作，供操作者及使用者使用[53]。

網路犯罪公約第 5 條干擾系統罪和第 4 條干擾資料罪的構成要件規定有部分重疊，二者皆有「當故意且無權地損壞、刪除、破壞、修改、隱匿電腦資料」等規定，但二者保護的客體及法益有明顯的不同。干擾資料罪保護的客體是「電腦資料」，保護的法益是要確保電腦資料的整體性、正常運作性

51 張紹斌，前揭註 28，頁 97。

52 李茂生，「刑法新修妨礙電腦使用罪章芻議（下）」，台灣本土法學雜誌，第 56 期，頁 207-208（2004）。

53 *Explanatory Report*, *supra* note 8, para. 65.

及儲存資料的可使用性；干擾系統罪保護的客體是「電腦系統」，保護的法益是要確保電腦系統適當地運作。由於構成要件要素的重疊，當該當網路犯罪公約第 5 條之罪時，往往也該當網路犯罪公約第 4 條之罪（也就是第 4 條可以含括第 5 條），此時則需以競合理論加以處理，但卻不必然一定會該當網路犯罪公約第 4 條之罪，因爲，如果藉由「輸入、傳輸電腦資料」而嚴重阻礙電腦系統的運作時，並不會該當網路犯罪公約第 4 條之罪，例如：藉由分散式阻斷攻擊（DDOS）或封包洪流（Ping Flood）來癱瘓網路即屬之。

網路犯罪公約第 5 條類似於我國刑法第 360 條的規定，皆在保障電腦及網路設備之正常運作。不過二者在行爲手段上的要求上存在些許差異：公約第 5 條規定的行爲態樣是：「藉由輸入、傳輸、損害、刪除、破壞、修改、隱匿電腦資料而阻礙」，而我國刑法第 360 條規定的行爲態樣是：「以電腦程式或其他電磁方式干擾」。

論者批評我國刑法第 360 條所規定的「干擾」不夠明確，容易產生適用上之困擾。又立法者爲了避免「干擾」一詞範圍過度廣泛，因此，加上了特定的行爲方式（以電腦程式或其他電磁方式）來限制，不過「電腦程式」及「電磁方式」二個用語仍舊充滿適用上的難題：何謂以電腦程式來干擾？何謂以電磁方式來干擾？似乎非常不明確。是以，本文認爲網路犯罪公約第 5 條可以作爲我國修法時的參考，將我國刑法第 360 條修訂爲：「無故以輸入、傳輸、損害、刪除、破壞、修改、隱匿電磁紀錄，阻礙他人電腦或其相關設備，致生損害於公眾或他人者……。」用「輸入、傳輸、刪除、破壞、變更、隱匿電磁紀錄」來取代原先「以電腦程式或其他電磁方式」的規定，除了列舉出可能的行爲手段態樣（實際上幾乎已包含可能發生的所有行爲類型），讓原本相當不明確的「以電腦程式」、「以其他電磁方式」變的相對明確外，也讓我國刑法第 360 條行爲結果的因果歷程明顯易懂，亦即該條罰的是：透過輸入、傳輸電磁紀錄（通常指傳送癱瘓網路的電腦資料）或刪除、破壞、變更、隱匿電磁紀錄（通常指透過電腦病毒破壞電腦系統，而使其無法正常運作），進而「阻礙」電腦的運作，如此在適用上也就變的更加

明確、容易，同時解決「干擾」一詞一直存在模糊內涵的困擾。至於一個阻礙電腦系統運作的犯罪行為（刑法第 360 條）若同時該當刪除變更電磁紀錄罪（刑法第 359 條），則藉由競合理論加以處理即可。

4.4 刑法第 362 條：製作專供犯本章之罪之電腦程式罪

我國刑法第 362 條[54]的訂定是為了防止惡意電腦程式的危害，可以稱為是駭客條款，其規範的構成要件有三：1.第一層次的行為：製作犯本章之罪的電腦程式；2.第二層次的行為：供自己或他人犯本章之罪；3.侵害結果：致生損害公眾或他人。而本條所規範的並非是利用他人製造的電腦程式所為的侵害行為，因為這些行為有刑法第 358 條至第 360 條加以規範，所以本條真正處罰的是惡意電腦程式的製作行為[55]。

4.4.1 相關爭議問題

從我國刑法第 362 條觀之，如果惡意電腦程式製作人自行使用該程式，而侵害他人電腦系統安全，則必須同時符合前述三個構成要件才該當犯罪，這似乎是過度嚴格的規範方式[56]。而且若參照偽造貨幣罪章來看，如此的規範，彷彿將偽造貨幣行為和行使偽造貨幣的行為混為一同，同時對一個混合行為加以處罰，使得該規範模糊不清[57]。再者，如果是他人使用該程式而侵害他人電腦系統安全時，製作惡意電腦程式的製作人是否該當該條之罪，卻

54 刑法第 362 條規定：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」立法說明中指出：「鑑於電腦病毒、木馬程式、電腦蠕蟲程式等**惡意之電腦程式，對電腦系統安全性危害甚鉅**，往往造成重大之財產損失，致生損害於公眾或他人，一九九九年四月二十六日發作之 CIH 病毒造成全球約有六千萬台電腦當機，鉅額損失難以估計，即為著名案例，因此實有對此類程式之設計者處罰之必要，爰增訂本條。」

55 柯耀程，「刑法新增『電腦網路犯罪規範』立法評論」，前揭註 22，頁 125-126。

56 同前註，頁 128。

57 同前註。

取決於他人是否使用該電腦程式，如此的情況下，使得刑罰的發動變的相當不確定，不但造成適用的困境，規範功能也會喪失[58]。最後，該條文規定惡意電腦程式的製作必須爲了「專供犯本章之罪」而作，依照罪刑法定原則，當該惡意電腦程式也可供其他非法犯罪之用時，例如：洗錢、賭博，是否要該當本條之罪，則充滿爭議[59]。

4.4.2 網路犯罪公約規定：濫用設備罪

網路犯罪公約第 6 條爲濫用設備罪（misuse of devices）：

1.當故意且無權地從事下列行爲，每一個締約國須在其國內法採取可能必要的立法和其他措施而建立此一刑事犯罪。

a.生產、販售、採購供使用、進口、散布或以其他方式提供：

i.一個設備（包含電腦程式）被設計或改造成主要目的爲犯第 2 條至第 5 條之罪。

ii.電腦密碼、登入代碼或相類似的資料，藉由這些資料，全部或部分的電腦系統能夠被進入使用，而意圖讓其被用於犯第 2 條至第 5 條罪之目的。

b.持有 a.i 或 a.ii 中的任何項目，而意圖讓其被用於犯第 2 條至第 5 條罪之目的。締約國可以立法規定當持有一定數量的項目後，才需課以刑事責任。

2.本條不得被解釋爲對如下行爲課以刑事責任：第 1 項所提之販售、採購供使用、進口、散布或以其他方式提供或持有，並非爲了犯第 2 條至第 5 條罪之目的，例如：經授權而測試或爲保護電腦系統。

3.每一締約國可以有權保留不適用本條第 1 項，只要保留不涉及販售、散布或其他方式提供本條第 1 項 a.ii 中的任何項目。

網路犯罪公約第 6 條第 1 項第 a 款第 i 目所處罰的是：以生產、販售、散布等方式提供一個設備，而其主要目的是爲了被用於犯網路犯罪公約第 2

58 同前註。

59 參見張紹斌，前揭註 28，頁 99。

條至第 5 條的罪；網路犯罪公約第 6 條第 1 項第 a 款第 ii 目所處罰的是：以生產、販售、散布等方式提供電腦密碼等，使得電腦系統能夠被進入，而意圖讓其被用來犯網路犯罪公約第 2 條到第 5 條的罪；網路犯罪公約第 6 條第 1 項第 b 款則規定，締約國可規定當持有一定數量的項目（設備、電腦密碼等）後才課以刑事責任。此條規定主要係在處罰藉由濫用設備（設計）或濫用進入電腦系統的資料，而意圖違反網路犯罪公約第 2 條到第 5 條之罪，進而侵害電腦系統或資料的完整性、保密性及可使用性。由於違反網路犯罪公約第 2 條到第 5 條之罪，常常需事先從黑市中取得進入電腦系統的資料或取得進入電腦系統的工具（駭客工具），因此，爲了有效打擊網路犯罪公約第 2 條到第 5 條之犯罪，有需要參照僞造貨幣之規定，將處罰的行爲提前至生產、販售、散布這些資料或工具者[60]。

網路犯罪公約第 6 條所規定的濫用設備罪和我國刑法第 362 條規定類似，但網路犯罪公約的規定較我國規定詳細：我國刑法第 362 條只處罰「製作」行爲，但網路犯罪公約第 6 條處罰態樣除了「生產」（製作）外，還包括其他態樣：販售、採購供使用、進口、散布或以其他方式提供（例如：放置於網站上，供人自由下載使用）；第 362 條製作的客體是「電腦程式」，但網路犯罪公約第 6 條製作、販售、散布等的客體還包括「電腦密碼」等；第 362 條是規定「專供」犯第 36 章之罪，網路犯罪公約第 6 條則規定「意圖」犯第 2 條到第 5 條之罪。

我國刑法第 362 條所規定的三個構成要件爲：製作犯本章之罪的電腦程式、供自己或他人犯本章之罪、致生損害公眾或他人，被認爲是過度嚴格的規範方式，而且若供自己犯罪使用，則將製造行爲和行使行爲混爲一同，若供他人犯罪使用，則取決於他人是否使用該電腦程式來決定構成要件是否該當，使得刑罰的發動變的相當不確定。另外，刑法第 362 條所規定，惡意電腦程式的製作必須爲了「專供」犯本章之罪，該用語亦產生適用上很大的爭

60 *Explanatory Report*, *supra* note 8, para. 71.

議。是以，本文認爲網路犯罪公約第 6 條可以作爲我國未來修法時的參考，將我國刑法第 362 條修訂爲第 1 項：「意圖供犯本章之罪之用，而製造、販售、散布、交付或以類似方式提供電腦程式，足生損害於公眾或他人……」，第 2 項：「意圖供犯本章之罪之用，而製造、販售、散布、交付或以類似方式提供電腦密碼或類似的資料，足生損害於公眾或他人，依前項之規定處斷。」

如此而後，原本第二層次的行爲規定「供自己或他人犯本章之罪」修改爲「意圖供犯本章之罪之用」，即可解決製造行爲和行使行爲混爲一同、刑罰發動不確定、規範過度嚴格及「專供」用語無法適用等問題。此外，在第 1 項規定「電腦程式」外，在第 2 項增訂「電腦密碼或類似的資料」，使得當處罰行爲提前時，不會有漏洞產生，造成只處罰和「電腦程式」相關部分，漏了處罰和「電腦密碼」相關部分。

5. 結論

我國身爲世界上資訊科技產業重要國家，且上網人口已超過 1,500 萬人，台灣電腦犯罪的嚴重性當然不低於歐美大國。依據刑事局偵九隊內部統計資料，2009 年 1 月至 9 月的電腦犯罪發生數爲 20,980 件，主要的犯罪類型爲：網路詐欺占 11,465 件、妨害電腦使用占 3,216 件、妨害風化占 1,920 件、侵害商標權占 1,359 件、侵害著作權占 1,098 件、妨害名譽（信用）占 731 件、違反兒童及少年性交易防制條例占 434 件。當中妨害電腦使用犯罪占居第二，又電腦犯罪具有高犯罪黑數，若以電腦犯罪的犯罪黑數達 80%以上來推估[61]，我國妨害電腦使用犯罪在 2009 年 1 月至 9 月應高達 15,000 件以上，可見妨害電腦使用犯罪在我國的嚴重性不容低估。

2003 年我國刑法新增第 36 章妨害電腦使用罪章，除爲了解決電磁紀錄與動產、文書存在不同的屬性，刪除第 323 條有關電磁紀錄以動產論的規定

61 林山田、林東茂、林燦璋，前揭註 2，頁 525。

及第 352 條第 2 項電磁紀錄的準文書規定外，亦希望能對其他影響電腦系統安全、侵害電腦資料完整、保密及可使用的行爲加以規範，以期建構完整的我國電腦犯罪規範體系。唯適用至今，不論學者或實務界都提出不少的批評與檢討。爲解決種種相關的問題與爭議，本文參考網路犯罪公約第 1 篇第 1 章第 2 條、第 4 條、第 5 條及第 6 條，提出未來修法的建議。分列如下：

刑法第 358 條修訂爲：

無故入侵電腦或其相關設備，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。（刪除：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞」）

刑法第 359 條修訂爲：

無故刪除、破壞、變更或隱匿他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。（刪除：「無故取得」）

刑法第 360 條修訂爲：

無故以輸入、傳輸、損害、刪除、破壞、修改、隱匿電磁紀錄，阻礙他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。（刪除：「無故以電腦程式或其他電磁方式干擾」）

刑法第 362 條第 1 項修訂爲：

意圖供犯本章之罪之用，而製造、販售、散布、交付或以類似方式提供電腦程式，致生損害於公眾或他人，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。（刪除：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪」）

增訂第 2 項爲：

意圖供犯本章之罪之用，而製造、販售、散布、交付或以類似方式提供電腦密碼或類似的資料，致生損害於公眾或他人，依前項之規定處斷。

如同本文最初所說，網路犯罪公約企圖規範最廣義的電腦犯罪，因此，該公約中除了規範與我國妨害電腦使用罪章一樣的犯罪外，在刑事實體法方面仍對電腦相關僞造罪、電腦相關詐欺罪、兒童色情罪、著作權侵害罪加以規範，此部分亦值得我國刑法修訂時的參考，因此，仍待有志之士或筆者他日再撰文補充，以期能建構一套完善且效率的打擊電腦犯罪規範。

參考文獻

中文書籍

林東茂，《刑法綜覽》，修訂 4 版，一品文化出版，台北（2006）。
林山田、林東茂、林燦璋，《犯罪學》，增訂 4 版，三民出版，台北（2007）。
盧映潔，《刑法分則新論》，新學林出版，台北（2008）。

中文期刊

李茂生，〈刑法新修妨礙電腦使用罪章芻議（上）〉，《台灣本土法學雜誌》，第 54 期，頁 235-247，2004 年 1 月。
李茂生，〈刑法新修妨礙電腦使用罪章芻議（下）〉，《台灣本土法學雜誌》，第 56 期，頁 207-220，2004 年 3 月。
柯耀程，〈刑法新增「電腦網路犯罪規範」立法評論〉，《月旦法學教室》，第 11 期，頁 117-129，2003 年 9 月。
柯耀程，〈「電磁紀錄」規範變動之檢討〉，《月旦法學教室》，第 72 期，頁 117-127，2008 年 10 月。
張紹斌，〈刑法電腦專章及案例研究〉，《軍法專刊》，第 54 卷第 4 期，頁 86-100，2008 年 8 月。
馮震宇，〈網路犯罪與網路犯罪公約（上）〉，《月旦法學教室》，第 4 期，頁 124-136，2003 年 2 月。
蔡榮耕，〈Matrix 駭客任務：刑法第 358 條入侵電腦罪〉，《科技法學評論》，第 5 卷第 1 期，頁 103-134，2008 年 4 月。

其他中文參考文獻

立法院公報，第 89 卷第 69 期，2000 年 12 月。

英文書籍

CASEY, EOGHAN, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET (2d ed. 2004).

英文期刊

Fisher, Jay, *The Draft Convention on Cybercrime: Potential Constitutional Conflicts*, 32 UWLA L. REV. 339 (2001).

Miquelon-Weismann, Miriam F., *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 329 (2005).

Weber, Amalie M., *Cybercrime: The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425 (2003).

其他英文參考文獻

Chart of Signatures and Ratifications, COUNCIL OF EUROPE, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (last visited June 25, 2010).

Council of Europe in Brief, COUNCIL OF EUROPE, http://www.coe.int/aboutcoe/index.asp?page=quisommesnous&l=en (last visited June 25, 2005).

Explanatory Report to the Convention on Cybercrime, COUNCIL OF EUROPE, *available at* http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm (last visited July 13, 2010).