# 國立交通大學

## 科技法律研究所

## 碩士論文

# 刑法妨害電腦使用罪章之檢討

**Rethinking the Law against Cyber and Computer Crimes**

研 究 生：古旻書

指導教授：林志潔　博士

中 華 民 國 一零二 年 八 月

# 刑法妨害電腦使用罪章之檢討

# Rethinking the Law against Cyber and Computer Crimes


研 究 生：古旻書　　Student：Min-Shu Gu

指導教授：林志潔　　Advisor：Chih-Chieh Lin


國 立 交 通 大 學

科技法律研究所

碩 士 論 文

A Thesis

Submitted to Institute of Technology Law

College of Management

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Law

August 2013

Hsinchu, Taiwan, Republic of China

中華民國一零二年八月

# 中文摘要

電腦與網路，可說是近代科技發展中影響人類社會最深遠的產物。然而，隨著人類社會廣泛運用電腦與網路，新型態的犯罪亦隨之迎運而生，而需要以資訊刑事法規加以規範。我國在西元 2003 年所修訂的刑法第 36 章「妨害電腦使用罪章」，即屬資訊刑事法規的里程碑。惟此一法規在修法時，就已獲得學界褒貶不一的評價；經過近十年的實務運作，也發現許多應該修正的地方。因此，本文將以文獻回顧為經，判決實證研究為緯，從我國妨害電腦使用罪章之規範對象與範圍談起，接著討論保護法益的爭議，並檢討各罪構成要件的修正方向，最後說明整合性立法之必要性與迫切性，期許我國能建立更完善的資訊刑法架構，建立高安全性之資訊使用與發展環境。

關鍵字：妨害電腦使用罪，電腦犯罪，網路犯罪，資訊，電磁紀錄，網路犯罪公約

# Abstract

Computer and internet are the most important inventions in contemporary society. Crimes against the safety of internet or using computers therefore become a big issue in the digital era. In Taiwan, the most important law regarding computer crimes is in the Penal Code, Chapter 36 -the Offenses Against the Computer Security The whole chapter is enacted in 2003. Although compared with the Penal Code which was original enacted in 1928, Chapter 36 is very young, it has been 10 years since the Chapter was enacted. It is believed that the law makers in Taiwan made a lot of efforts when enacted the offenses of Chapter 36; however, over these years, discussions and critics to the law and its application have never been stopped. In the article, the main research method would be literature reviewing and empirical studying of the judgment searched by the author. The author will then give a brief introduction to Chapter 36 and its legal background. Second, the authors analyze the controversy and legal arguments to the elements of these offenses. Third, the authors will see how the courts interpret the law by case studies. Finally, the authors will provide a proposal to revise and reconstruct the law to protect internet and computer safety.

Keyword: Computer crime, Cybercrime, information, Electromagnetic recording, Convention on Cybercrime

# 誌謝

為論文所苦的研究生間流傳著一個古老的說法，那就是當論文寫作遇到困難的時候，先寫誌謝就能有效加快寫論文的進度.....倘若真是這樣的話，恐怕這篇誌謝的長度會是本文的好幾倍才對。很顯然地，這個傳說跟拔獅子鬃毛生髮傳說一樣不可信，所以這篇論文若是有幸被未來為論文所苦的學弟妹所看到，或許這段誌謝所引述的「實證研究」會比內文更有價值也說不定。

言歸正傳，既然標題叫做誌謝，那麼理所當然就是要感謝人用的。本文的完成，最需要感謝的人是我自己。老實說，從小到大我最討厭的事情就是讀書，其次討厭的事情是作研究，對於寫文章雖然有一絲熱情，但是那僅限於自己隨想隨寫不受拘束的漫談而言，要寫論文這種正經八百又有既定格式的文章，對我來說實在是滿困難的。因此，本文之完成應居首功者，當然是按捺脾氣、磨著耐性、壓抑著自己對讀書和研究的厭惡拼命執筆完成這篇文章的自己，謝謝。

其次，當然是不免俗的要感謝對於本論文之完成有直接實質參與以及貢獻者。第一個要感謝的是指導教授林志潔老師，感謝老師鼓勵我將自己不成熟的發想架構成文，並幫我調整架構與條理，討論應該改進或加強的部分，除此之外，在與論文相關（或無關）的生活等瑣事上也甚有貢獻，謝謝老師。感謝口試委員林一平副校長，他除了曾是我就讀交大資工系時的院長外，也曾經在一堂科技與創意相關的課程中受到林副校長的啟發，能夠請到林副校長這麼重量級的資工領域大師指導，對我來說實在是莫大的榮幸，更直接的點出我許多未注意的盲點，使論文內容更加完整。感謝口試委員暨召集人蔡蕙芳老師，蔡老師是我進科法所後上的第一堂課《刑法總則》的授課老師，也是我刑事法基礎的啟蒙老師之一，除了要深深感謝蔡老師過去的指導外，口試時老師犀利的指教與豐富的學養如同照妖鏡一樣反映出我的無知，希望這本論文的完稿經過修改後，不至於讓蔡老師覺得臉上無光。

另外，在本論文的架構過程中，要感謝邱忠義老師在專討前後的指教，一針見血的提問與說明，均徹底協助我釐清原先較為模糊的思路；感謝徐仕瑋學長常常在我陷入困境的時候，抽空提點並與我詳談，往往能像及時雨一樣救我一命；感謝王立達老師在我冒昧寄信詢問電信法的相關問題時，詳盡而有耐性的魚雁往返教導我正確的觀念。

接著應該感謝的，是對本論文完成有著間接貢獻者（這就是所謂的層次性）。感謝佩錡這段時間不離不棄的陪伴，畢竟論文寫作過程中不可能一帆風順，會直接被風暴波及的佩錡對我而言，是穩定而重要的抒發對象，同時也是最佳的口說聽眾和評審。感謝媽媽三不五時打電話過來提醒我年紀老大不小了應該趕快寫完論文畢業，再加上志潔老師的叮嚀催促，讓我感覺就像是有兩個媽媽一樣受到加倍關心（也加倍嘮叨）。感謝敦威和芳儀在我逃離新竹的期間，貼心的分攤了一些我因為距離因素無法處理的工作，需要幫忙時也都義不容辭的協助，省去我來回奔波的時間與金錢成本。感謝貓咪牛奶與可可不定時賣萌的精彩表現，安撫了我論文寫作期間苦悶的心情，而且他們頂多只有十五年左右的壽命，但因為這篇誌謝搞不好就這樣變成另一種永恆了也說不定，這大概就是所謂的貓死留名吧？

碩士論文的完成代表的是碩士學位的取得，因此我必須感謝科法所碩士班期間劉老師、倪老師、敏銓老師、銘雄老師、建中老師、欣柔老師、在方老師、景文老師、浣翠老師與其他我曾教過我的老師們的指導與照顧。所上行政工作百務繁忙，碩士班生活又不免碰上疑難雜症，感謝助理玉佩姐、珮瑜姐、以欣姐、嫚君姐、慧茹姐和莉雯姐，實在是受妳們幫助甚多，難以一一勝數。感謝過去曾與我共事並且認真參與所上大小事務的同學、學長姊與學弟妹，儘管在團體中總是不泛投機偷懶之輩，而有時又需受到領導者經驗欠缺或決策錯誤的拖累，仍然集結了戮力做好工作者的團結力量，挑起了沈重的工作負擔，即便結果必非全部都盡如人意，至少都讓活動能夠落幕，除了對自己的良心有所交代外，更留下了許多難以抹滅的回憶，在此就不一一列舉了。

另外，過去的同學及現在一起打英雄聯盟（或其他遊戲） 的朋友們，雖然你們或許不知道自己對我的論文有了什麼貢獻，但我想那些時光的共同消磨與談天說地的放鬆效果，對我來說是絕佳的充電時間，讓我在這論文的漫漫長路不至於像電視廣告那耗盡電力的兔子一樣，失去打鼓的動力。

千頭萬緒其實也不知道還有什麼可以感謝的，或者該說需要感謝的太多了，反而更難以一一列舉。說穿了，碩士論文也好人生也罷，除了那些提供你及時幫助與拉你一把的貴人外值得感謝外，許多書籍或師長都曾教導我們要感謝帶給自己逆境的事情與人，因為那些磨練使自己成長。照這樣的邏輯來看，基本上沒什麼是不值得感謝的，所以要是漏了些什麼，就用這一段概括條款作個謝詞的補充吧！（其實這段的意思根本就等於「要謝的人太多了就謝天吧」這超級老梗啊！）

從裝甲兵軍營到學校，從竹旬穴到龍潭貓穴，三年的時光倏忽即逝，碩士學位的取得只是未來起步的開始而已，願自己能保有前進的動力與熱情，也願那些值得活著的好人們能事事順心。

2013 年夏 於龍潭貓穴

# 目錄


中文摘要.....i
Abstract.....ii
誌謝.....iii
目錄.....vi
第一章 緒論.....1
第一節 研究動機與研究目的.....1
第二節 研究方法與研究限制.....2
（一）研究方法.....2
（二）研究限制.....4
第三節 論文架構.....4
第二章 從定義談起.....6
第一節 電腦犯罪、網路犯罪與資訊犯罪.....6
（一）電腦犯罪（computer crime）.....6
（二）網路犯罪（cybercrime）.....7
（三）從電腦和網路犯罪之定義範圍談資訊犯罪.....9
第二節 我國修法歷程.....11
（一）我國刑法中與資訊犯罪相關條文之修正沿革.....11
（二）判決個案分析：臺灣高等法院 95 年度上易字第 2110 號判決.....13
第三節 妨害電腦使用罪章規範對象與範圍.....15
第四節 小結：以抽象定義劃定規範對象與範圍之優勢.....19
第三章 保護法益的爭議.....22
第一節 實務與學說的爭論.....22
第二節 以法解釋學觀點主張本章保護社會法益之討論與缺點.....23
第三節 比較法上德國法將資訊犯罪定性為個人法益所面對的問題.....25
第四節 小結：試論近程及遠程之法益爭議解決方案.....26
第四章 構成要件的檢討.....29
第一節 第 358 條.....29
（一）學界評論.....30
（二）判決個案分析：臺灣高等法院 101 年度上訴字第 2540 號判決...32
（三）判決個案分析：臺灣高等法院 100 年度上易字第 2136 號判決...33
（四）修法建議.....37
第二節 第 359 條.....39
（一）學界評論.....40

（二）判決個案分析：最高法院 97 年度台上字第 3817 號判決.....42
（三）判決個案分析：最高法院 98 年度台上字第 3015 號判決.....44
（四）判決個案分析：最高法院 100 年度台上字第 52 號判決.....47
（五）判決個案分析：最高法院 100 年度台上字第 6468 號判決.....50
（六）修法建議.....55
第三節　第 360 條.....56
（一）學界評論.....57
（二）判決個案分析：最高法院 101 年度台上字第 739 號判決.....58
（三）判決個案分析：臺灣高等法院高雄分院 95 年度矚上訴字第 4 號判決.....62
（四）修法建議.....63
第四節　第 362 條.....64
（一）學界評論.....65
（二）判決個案分析：臺灣高等法院台中分院 98 年度上更（一）字第 35 號判決.....66
（三）修法建議.....68
第五節　第 361 條及第 363 條.....69
（一）學界評論.....70
（二）判決個案分析：本章之罪引用第 361 條加重後是否仍須告訴乃論.....72
（三）判決個案分析：最高法院 101 年台上字第 5295 號判決.....77
（四）修法建議.....82
第五章 資訊刑法之定位與修法必要性.....84
第一節 立法整合之缺失與資訊刑法之定位.....84
第二節 與其他法律相關之判決.....86
（一）判決個案分析：與個人資料保護法相關判決.....86
（二）判決個案分析：與營業秘密法相關判決.....88
（三）判決個案分析：與電信法相關判決.....91
第三節 小結：修訂資訊刑法之展望.....95
第六章 結論.....99
附錄：本章條文修正方向建議.....101
參考文獻.....102

# 第一章 緒論

## 第一節 研究動機與研究目的

電腦（computer，或譯為計算機）可以說是影響近代人類社會最重大的發明之一，其後隨著網際網路（Internet）的普及使用，更是讓人類的日常生活幾乎完全離不開電腦與網路。然而，新技術、新事物的產生，很自然的就會帶來新的問題，電腦與網路亦然。在刑法領域中，我們所面對的，便是各種與電腦與網路有關的犯罪類型，從單獨一台電腦就能遂行的犯罪類型，例如無權複製他人儲存於電腦的資訊，到需要透過網路遂行的網路詐欺、網路媒介性交易、駭客（hacker）或快客（cracker）入侵、網路病毒攻擊等等。

這些隨著科技發展而產生的犯罪類型中，與網路相關的犯罪類型得以影響的範圍相當大。透過連結世界各國的網際網路，此種犯罪不受時空的侷限，而可能是跨國性甚至影響全球的嚴重犯罪行為。[1] 縱然是利用單獨一台電腦從事的犯罪，例如無權複製電腦中資訊的行為，在資訊電子化、數位化已經成為主流的現代，藉此盜取機密技術或個人私密資料等行為，其可能的損害結果也不能等閒視之。因此，世界各國針對此種因科技發展而產生的新型態刑事問題，大多抱持謹慎而重視的態度，建立相對應的刑事規範來處理。

不論是舊瓶裝新酒的「使用電腦」犯罪，例如傳統詐欺透過網路手法進行、透過網路聊天室媒介性交易等；或是傳統刑法無法規範（或者是規範適用上可能顯得勉強）者，例如製造電腦病毒的行為等等，各國均以廣狹不一的法律試圖規制此類行為，以避免規範上的漏洞。我國亦然，刑法對應資訊發展所為的修法次數頗多，然而學界、實務對歷次修法的評價大多褒貶不一。其中至為關鍵者，以

[1] 以我國早期網路犯罪為例，1999 年由我國一位資訊工程系學生製作的 CIH 病毒，便曾造成全球網路使用者的恐慌，造成跨國性的損害。相關新聞可參「CIH 病毒作者 陳盈豪今接受約談」，中國時報，1999 年 4 月 30 日，新聞連結：http://ago.gcaa.org.tw/env_news/199904/88043003.htm（最後點閱時間：2012 年 12 月 1 日）。

民國 92 年修訂的「妨害電腦使用罪章」為規模最大、影響也最為深遠的一次修法，特別針對電磁紀錄的相關犯罪訂立刑法分則的罪章，使電腦或網路犯罪中較具有特殊性、而傳統刑法適用上可能有所困難的罪名獨立成章，也表彰了政府重視此一領域之刑法規範的決心。

質言之，既然透過電腦與網路進行的資訊犯罪行為，已實質跳脫了傳統刑法設計所能全盤規制的範疇，突破了時間和地理的侷限，甚至有著強烈的跨國性質，則若要能夠有效防堵此類犯罪的產生，勢必需要由世界各國分別建立相對應的國內刑事法規範，再以此為出發點，建立司法互助與跨國刑事合作，才能真正有效的遏阻此類資訊犯罪的產生。[2]

在修法已近十年的今日，資訊科技的進步從未停止，對於修法完成時就已經引起學界廣泛討論、批評的妨害電腦使用罪章，本文試圖透過整理過去的相關文獻看法，以及利用檢索相關判決的實證研究方式，檢驗過去近十年來我國對於資訊犯罪的規範成效，並針對其不足之處及未來應修正的方向，提出本文粗淺的看法，以期拋磚引玉，為當局提供可能的改革修正方向，此即本文最主要的研究動機與目的。

## 第二節 研究方法與研究限制

### （一）研究方法

本文主要採用的研究方法，首先係透過探討妨害電腦使用罪章、電腦犯罪、網路犯罪等相關主題之文獻整理，架構出學說對於我國妨害電腦使用罪的批評與討論，以及相關外國法例的引薦、比較，以此作為基石規整學說上給予負面評價的問題，再透過分類的方式將問題分門別類，讓讀者能對本文所欲探索的核心問題一目了然。

[2] 實務工作者於修法前的研修會議，便曾提出我國因缺乏對於駭客行為，或垃圾電子郵件阻礙伺服器運作等行為的刑事規範，致使縱然他國曾請求協助調查，但因我國法規付之闕如而無法可管的窘境。參法務部，《刑法有關電腦（網路）犯罪研修資料彙編》，2002 年 12 月，頁 4。

其次，本文引入實證研究的概念，對修法前後我國關於妨害電腦使用罪的相關判決進行檢索、蒐集與整理，並與前開核心問題作比較與對照，藉以探究學說與實務的觀點是否有所落差？學說認定可能面臨的問題是否有實務案例作佐證？實務判決是否凸顯了法規面的問題？透過學說與實務間的交叉比較，拼湊出妨害電腦使用罪章運作與設計最真實的態樣。

在判決檢索的部分，礙於時間精力之限制，本文採用的第一個研究方式，是**案由搜尋法**。從最高法院為起點向下搜尋，將所有過去最高法院以「妨害電腦使用罪」為案由的案件全部列出並且進行一次瀏覽，將與法律爭點直接相關的判決從中挑出，嗣後延伸觀察其下級審法院就事實認定與法律爭議的見解，加以比較和探討。此一階段，最高法院部分共搜尋出 28 個判決，按照判決時間，最早的判決是在民國 93 年 10 月 7 日宣判的最高法院 93 年度台上字第 5170 號判決，最晚的判決則搜尋至民國 101 年 8 月 29 日宣判的最高法院 101 年度台上字第 4173 號判決為止。

第二個研究方式，則是**其他關鍵字搜尋法**。礙於實務上多數案件多與第 358 條和第 359 條相關，而其他法條判決數量較少，關於第 360 條以及其後條文的判決較為匱乏，故改以關鍵字檢索方式，對象從最高法院起，擴及臺灣高等法院及各分院，藉此增大搜尋範圍，逐個檢視該搜尋結果中判決內文爭點，摘錄較具討論價值者研析之。除以**條號**為關鍵字，例如「刑法第 360 條」等關鍵字搜尋外，也嘗試使用**可能爭點**的關鍵字例如：「妨害電腦使用&電磁紀錄」、「妨害電腦使用&保護法益」、「妨害電腦使用&科技中立」等等，試圖藉此找尋前開搜尋過程的漏網之魚。此一階段因進行時間較晚，故搜尋結果中發現判決時間最晚者，係民國 101 年 10 月 19 日宣判的最高法院 101 年度台上字第 5295 號判決。

若在搜尋過程中若發現與本罪章有關，但爭點卻並非直接與某一條文有關者，則列入紀錄後，用於補充修法歷程、與其他法律的關係等章節，作為實務看法的補充，以其論述能具有完整與真實性，而不至於脫離現實流於空泛論述。

### （二）研究限制

本文面臨之研究限制主要有二。首先，筆者礙於語言能力之障礙，對於歐洲相關比較法之資料，往往需透過第二手文獻進行研究，或透過網路搜尋官方翻譯為英文版本的內容，在不諳歐洲語言的阻礙下，實難以直接研讀第一手資訊與資料，就此一部分探討深度不足，且不同語言經過翻譯後語意失真或篇插在所難免。就此限制，筆者在閱讀二手文獻時，已盡力搜尋相關資料；引用的法條或公約內容，亦係官方翻譯版本，應能將語意錯誤與偏差減到最小。

其次，判決檢索部分礙於時間精力所限，僅能盡可能透過精準關鍵字搜尋縮小範圍，找尋適當的案例進行討論，篩選過程中應不免有所遺漏。雖然如此，筆者認為目前所揀選的案例，應均有一定代表性或討論價值，而不至於有離題或過度偏頗。就此二點研究限制與相關說明，在此先行敘明，供讀者參考。

## 第三節 論文架構

本文共分為六章。第一章緒論，由本文研究動機與目的開始，其次談及本文所使用的研究方法，主要包括了文獻整理與實務判決研究。研究限制部分，則說明本文寫作時面臨的語言障礙，以及判決實證蒐集的困難等，已如前述。

第二章從定義談起，將從本文研究的標的開始說明，分析學說上電腦犯罪、網路犯罪之定義，然後說明本文所謂「資訊犯罪」此一用語的定義與範圍。次節則回顧歷史，將我國歷來刑法針對電腦與網路犯罪所為的修法歷程作簡單的介紹，並且提出與電磁紀錄相關的判決給讀者參考。接下來則談及本文認為本罪章的第一個重大問題，亦即對於本罪章規範對象與範圍的定義不清所可能產生的缺陷，並試於末節提出以抽象定義之方式作為定義規範對象與範圍的可能解答。

第三章則談及本罪章的第二大問題，亦即學說實務爭論不休的保護法益問題。本文將以文獻回顧及實務所產生的爭議為引，說明不同的論點。其次針對主張以法解釋學方法將本罪章定位為社會法益之罪的論點，進行討論與評析。接下來將

與我國現行法規結構較為相近的德國為例，說明現行法以及將本罪章定義為個人法益此一論點的優劣。最後提出法益爭議的近程與遠程解答。

第四章則進入本文所認為的第三大問題，亦即法條構成要件的檢討。本章大抵依序以第 358 條、第 359 條、第 360 條、第 362 條，然後將篇幅較小且具有關聯的第 361 條及第 363 條併為一節，各節均以學界評論為始，其次將本文所檢索到的相關判決進行介紹與評析，最後提出該條文的修法建議。

第五章介紹本文所主張「資訊刑法」的立法展望與定位，首先論及現行立法的相關缺失，其次介紹實務上與現行妨害電腦使用罪章相關、同時也牽涉到其他特別法的刑事規定之案件，藉以強調現行立法紊亂而缺乏整合性的現象。最後則提出本文看法，認為應以整合性、全面性的檢討現行與資訊相關的所有刑事法令，並且透過建構資訊刑法，作為所有利用資訊平台運作的刑事法基礎，在有特別需要保護的其他法益時，以特別法優先於普通法的方是作競合，可以清楚建立上下分明、保護法益清晰的資訊刑事體系。

第六章則將整理本文所有內容，進行結論的探討與論述，由回顧與檢討現行法令，重申在妨害電腦使用罪章立法已近十年的今日，應有逐步建立更先進的資訊刑法之展望。

# 第二章 從定義談起

## 第一節 電腦犯罪、網路犯罪與資訊犯罪

### （一）電腦犯罪（computer crime）

電腦犯罪此一名詞，有認為係過去網際網路尚不發達的時代時產生。[3]當時我國學界主要分為三種不同的見解，即「廣義說」、「狹義說」與「折衷說」。

首先，「廣義說」主要的定義，是「與電腦相關的犯罪均屬之」。在此見解下，所有與電腦有關的犯罪，不論其係將電腦作為犯罪工具的犯罪，例如利用電腦進行詐騙行為，或是涉及電腦內部資訊的犯罪，例如破壞電腦內儲存之文件等行為，均屬於電腦犯罪。[4]

「狹義說」則是天平的另一個極端，係「指與電子資料有關且侵犯某種特定法益的犯罪行為」，如限定在侵害財產或人格法益的犯罪行為。[5]舉例而言，入侵他人電腦窺視私密照片，其與電子資料（私密照片）有關且侵害特定法益（隱私權），故構成電腦犯罪。

「折衷說」則引入「電腦特質」之觀念，認為「濫用電腦或使用足以破壞電腦系統正常運作之行為，而形成與電腦特質有關的犯罪」方係電腦犯罪。[6]此種定義對於電腦特質此一要素的強調，主要是為了排除單純使用電腦作為工具（例如拿起電腦毆打他人的傷害罪）或犯罪客體（將電腦主機破壞的毀損罪）卻缺乏與「電腦特質」相關的犯罪類型，而將電腦犯罪的概念限縮在與電腦特質（例如電腦內儲存的文件、與電腦運算相關等等）相關的犯罪。

在外國文獻中，亦有對此一名詞的定義，認為電腦犯罪係指與電腦**有關**而違

[3] 徐振雄，「網路犯罪與刑法『妨害電腦使用罪章』中的法律語詞及相關議題探討」，國會月刊，第 38 卷第 1 期，2010 年 1 月，頁 44。
[4] 徐振雄，同前註。
[5] 徐振雄，同前註。
[6] 徐振雄，同前註。

反刑事法規的犯罪行為。[7]由此定義出發，以與電腦發生關聯性的方式去作區分，吾人可將電腦犯罪分成三大類：（一）使用電腦為工具（instrument）進行犯罪。此種工具之使用，係指透過電腦的運作與對電腦的操作，例如利用公司電腦盜取公司經費之行為。[8]（二）以電腦為標的（focus）之犯罪。此種犯罪類型未必使用或操作到電腦，絕佳的例子便是去偷商店中販賣的電腦和週邊設備的犯罪。[9]（三）將電腦作為證據儲存媒介（repository of evidence）的犯罪。舉例而言，若行為人在家用電腦中儲存大量盜拷的版權物，此時縱然該電腦本身並未作為犯罪使用（可能並非進行盜拷的那台電腦）亦非犯罪標的，在此定義下仍然構成電腦犯罪。[10]

甚至有論者直言，因為電腦犯罪此一名詞定義分歧，難以一語劃清其範圍，故由實際已經被立法規範的犯罪行為去反推出電腦犯罪的範圍可能是更恰當的方式。[11]基於這樣的理論，論者認為電腦犯罪的範圍應從諸如美國電腦詐欺與濫用法案（U.S. Computer Fraud and Abuse Act）或英國電腦濫用法（UK Abuse Act）等法律所規範的行為去歸納。[12]準此，電腦犯罪可能包括竊取電腦服務、無權存取受保全的電腦、軟體使用之隱私、竊取電腦所儲存之資料、透過電腦詐欺等等行為。[13]

總的來說，不論在我國或是外國，「電腦犯罪」一詞的涵義多變均是不爭的事實。不論所採用定義的廣狹，共通點都是與電腦**相關**。在此種不確定的定義下，本文以為，電腦犯罪之定義易生爭議，使用上本應格外注意，當用在講求明確的刑事法領域時更是如此。

## （二）網路犯罪（cybercrime）

網路犯罪一詞，則是泛指以電腦網路為工具或環境所進行的犯罪行為。[14]如同

---

[7] ROBERT MOORE, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME 3 (2nd ed., 2011).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET 37 (3rd ed., 2011).
[12] *Id.*
[13] *Id.*
[14] 徐振雄，前揭註 3，頁 40。學者 Casey 氏的定義則認為：網路犯罪是指犯罪行為中牽涉了電腦

電腦犯罪定義分歧，網路犯罪的定一語範圍也有類似現象。例如學者 Roger LeRoy Miller 和 Gaylord A. Jentz 將網路空間中的犯罪，區分為五大類，即（一）網路騷擾、（二）身份竊取、（三）網路色情、（四）網路恐怖、（五）網路賭博。[15]而 Gerald Ferrera 氏則以所侵害的法益與對象，區分為（一）侵害個人或企業、（二）侵害實體財產或無體財產、（三）侵害政府或政府機能等三種類型。[16]

Susan W. Brenner 則是透過傳統犯罪（crime）和網路犯罪（cybercrime）間的區分來解釋，認為所謂的犯罪是指政府為了維持秩序所定義的某些禁止行為，可以透過受害客體為對象區分為個人、財產、政府和道德四類。網路犯罪與傳統犯罪相同之處，都是造成了對社會秩序的威脅，而最大的不同之處只在於進行犯罪的方式不同。[17]她認為大部分所謂的網路犯罪僅僅只是犯罪方式的更新，將現實生活的犯罪轉移到網路空間（cyberspace）進行而已。[18]

至於我國學者則從網路在犯罪中所扮演的角色作區分，分成三大類：（一）以網路空間為犯罪場所、（二）以網路及連結在網路的電腦系統為犯罪工具、（三）以網路及連接在網路的電腦系統為攻擊目標。[19]實務工作者亦有以網路是否為絕對必要的媒介工具與否作區分，將單純作為媒介工具的犯罪類型，例如網路色情等犯罪，與必須以電腦和網際網路為**絕對必要工具**的類型，例如分散式阻斷服務攻擊（DDoS）等作出區分。[20]

就國際比較法的觀點來看，最值得一提者係歐洲理事會（Council of Europe）《網路犯罪公約》（Convention on Cybercrime）所作的界定，認為網路犯罪是指「以網路為媒介」與「以網路及其週邊設備為目標」的犯罪類型，包括（一）侵犯電

---

與網路，但是電腦可能是、也可能不是扮演工具（instrument）的角色。但他並未明確指出在電腦並非扮演犯罪器材時，是否意指電腦扮演的是犯罪環境的角色。*Supra* note 11 at 4.

[15] 徐振雄，前揭註 3，頁 42。

[16] 徐振雄，前揭註 3，頁 42-43。

[17] SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 9 (2010).

[18] *Id.* at 9, 10.

[19] 徐振雄，前揭註 3，頁 43。

[20] 徐振雄，前揭註 3，頁 43。事實上，本文認為這種區分方式用白話來說，就是「使用電腦網路為工具犯罪」和「利用電腦網路特質犯罪」的區分方式，想法上類同電腦犯罪的區分方法。

腦資料與系統機密性、完整性與可利用性、（二）與電腦有關的犯罪、（三）與內容（content）有關的犯罪、（四）侵犯著作權與鄰接權的犯罪。[21]

整體來說，網路犯罪的定義方式其實與電腦犯罪很類似，只是牽涉的對象多了網路空間，造成突破時空限制的能力遠大於電腦犯罪而已，不論是採用歸納的方式，或是透過法益侵害作分類，大抵仍不脫與電腦網路**相關**此一大原則。本文以為，以上定義大多承認網路犯罪的定義中，包括單純使用電腦網路為**工具**的犯罪類型，與利用電腦網路**特質**犯罪兩大類。

## （三）從電腦和網路犯罪之定義範圍談資訊犯罪

此處值得討論的問題有二。首先，電腦犯罪與網路犯罪間的定義與互動，是第一個需要解決的問題。從前開定義可以看出，不管是電腦犯罪還是網路犯罪本身均難找到所有人都同意的範圍與定義，加上這兩個名詞出現似有先後關係，牽涉的技術器物有所雷同，則吾人不免懷疑，其定義上是否可分？彼此重疊的區域又該如何定位？彼此的互動關係為何？

我國學界對於電腦犯罪與網路犯罪的概念可分性，大抵有正反兩說。採否定說者，**認為網路犯罪是電腦犯罪的延伸**，是電腦系統與通訊網路相結合的犯罪行為，只有在電腦犯罪中部分需透過網際網路進行的犯罪才是網路犯罪。[22]採肯定說者，則認為**網路犯罪是透過網路特性為工具或手段的網路濫用行為**，本質上與電腦犯罪仍有所不同。[23]

從技術面來看，網際網路確實是奠基於電腦的互連架構上，要說網路犯罪不是一種電腦犯罪，似乎有些牽強。不過，若回過頭從前開電腦犯罪與網路犯罪的定義方式來看，所謂電腦或網路的「特質」似乎一直都是最被強調的。若以特質

---

[21] 馮震宇，「網路犯罪與網路犯罪公約（上）」，月旦法學教室，第 4 期，2003 年 2 月，頁 133-136；徐振雄，前揭註 3，頁 47。

[22] 徐振雄，前揭註 3，頁 49。也就是說，否定說認為網路犯罪只是電腦犯罪的一種類型而已，或可稱網路犯罪是電腦犯罪的子類型，而非獨立的概念。

[23] 徐振雄，前揭註 3，頁 49-50。換言之，此說則認為網路犯罪雖仍有電腦犯罪的特性（技術上先天就是奠基在電腦上），但是電腦犯罪的定義範圍並不及於網路世界，而係透過網路犯罪的用語去填補定義該區塊的犯罪行為。

為定義核心觀察，電腦犯罪和網路犯罪所著重的「特質」又確實有所不同，似乎也不能夠直接斷言網路犯罪因為同時也有「電腦特質」就應該被納入電腦犯罪的定義範圍內。

本文在此並無意表達支持正反兩方其中一方說法之意。事實上，在觀察角度不同的前提下，單獨採納正反任一方的理論（而暫時撇開與對造理論上的矛盾）時，均有其道理。此處，本文要提出較為不同的看法，亦即並不去使用傳統的「電腦犯罪」或「網路犯罪」之名詞與定義，而是以「資訊犯罪」來定義本文所要討論的範圍。如同前開定義，本文所謂「資訊犯罪」，其核心係指利用**資訊科技（information technology）特質**進行犯罪者而言。**在此定義下，不論是電腦或網路之特質，其實都包括在「資訊科技特質」之中。**[24]

本文以為，電腦與網路所使用的虛擬空間，作為一個平行於現實空間的平台，此平台卻能與現實空間彼此交互影響。[25]此時，不論是所謂的電磁紀錄、數位訊號等等原本被囊括在電腦或網路特質中的詞彙，事實上都可以共同架構一個新的平台，在該平台上人類有著不同於現實世界的一些行為，對於該行為我們做出價值評斷，認定某些行為在資訊的平台上是不應該被允許、擾亂了該平台秩序的嚴重行為，而建立相對應的刑事規範。換言之，本文所謂的資訊特質，其實等同於投射出一個重疊於現實空間的的虛擬空間，該空間需要建立的資訊刑事法規，就是本文所主張的「資訊刑法」。

不論是電腦犯罪或網路犯罪，另一爭議都會是定義的廣狹問題。從前開論述可以發現，最廣的定義方式都是與電腦（或網路）**相關**。由此出發，然後大抵可

[24] 當然，「資訊」一詞若由語意觀之，係可指涉極度廣義的「傳達思想的過程與內容」，使用電腦與網路等電子科技產品的資訊科技（information technology）僅僅只是其概念中的子集而已。本文在此為了利於敘述，將直接使用「資訊」一詞代替「資訊科技」行文，未免讀者產生混淆，謹在此先做說明。關於「資訊」一詞之定義與解說，可參蔡蕙芳，「電磁紀錄無權取得行為之刑法規範」，國立中正大學法學集刊，第 13 期，2003 年 10 月，頁 109-111。

[25] 類似見解，參蔡蕙芳，「妨害電腦使用罪章：第一講：保護法益與規範功能」，月旦法學教室，第 126 期，2013 年 4 月，頁 63。論者亦使用「空間」之概念，說明妨害電腦使用罪章之立法，係為處理發生於該空間中的廣義電腦或網路犯罪為目的而生。此一說法，與本文所述現實空間與虛擬空間並行而各自需要相對應的刑事規範，實殊途同歸。

以劃分成「使用電腦（網路）為工具或環境犯罪」和「利用電腦（網路）特質犯罪」兩大類型，前者往往是傳統刑法已有相關規範的犯罪透過電腦（網路）作犯罪手段進行，後者則屬於舊有刑法本無規範（或套用舊有規範時可能產生疑慮）的犯罪。

本文所謂的資訊犯罪亦如是。本文以為，使用資訊科技為工具或環境犯罪，例如網路詐欺、用電腦偽造文書等等，屬於舊瓶裝新酒的傳統犯罪的變形，但本質上並未改變，傳統刑法的構成要件適用上也不至於產生問題，並非本文資訊犯罪所定義的範圍。但利用資訊科技特質犯罪，例如製造散播電腦病毒、破解電腦保全程式進行入侵等等，對於此種在資訊空間中且並非傳統現實空間所存在的行為類型，傳統刑法的構成要件並不能夠全盤合身的套用上去，因此會有修法的必要性與需求性，也是本文要討論的主要重點。

## 第二節 我國修法歷程

### （一）我國刑法中與資訊犯罪相關條文之修正沿革

在民國 92 年修訂妨害電腦使用罪章之前，其實就可從修正歷程看出因應科技進步而修法的思維脈絡。[26]民國 86 年 9 月 25 日刑法修正，可以看出我國刑法首次面對新型態的網路與電腦犯罪衝擊時，選擇的解決方式是新創設電磁紀錄此一概念，並列入第 323 條**準動產**，透過將電磁紀錄作為準動產的擬制，將原本用來規範傳統財產犯罪的條文套用到電磁紀錄上：「電能、熱能及其他能量或電磁紀錄，關於本章之罪，以動產論。」

對於有文書性質的電磁紀錄，該次修法則增列**準文書**規定於第 220 條第 2 項：「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，足以為表示其用意之證明者，亦同。」目的亦是希望透過電磁紀錄作為準文書處理

[26] 本文以下所引用之條文修正沿革、內容及理由，請參見立法院法律系統，中華民國刑法修正沿革，網址：http://lis.ly.gov.tw/lgcgi/lglaw?@72:1804289383:f:NO%3DE04536*%20OR%20NO%3DB04536$$11$$$PD%2BNO（最後瀏覽時間：2013 年 6 月 1 日）。亦可參見法務部，前揭註 2，頁 405-413。

的擬制方式，將傳統關於文書的規範範圍擴及使用日益頻繁的電磁紀錄。[27]

在民國 92 年專章修訂時，也一併移除第 323 條電磁紀錄作為準動產之規定。修法理由謂：「本條係八十六年十月八日修正時，為規範部分電腦犯罪，增列電磁紀錄以動產論之規定，使電磁紀錄亦成為竊盜罪之行為客體。惟學界及實務界向認為：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成要件有所扞格。為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為完整，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為改納入新增之妨害電腦使用罪章中規範。」由上述修正理由可以看出，電磁紀錄之性質（可複製性）與傳統動產、準動產本不相同，若強以傳統刑法要件套用的結果，將勢必產生本文所謂「不合身」的窘境。[28]

另外，此次修法也將第 352 條第 2 項關於電磁紀錄可準用毀損文書罪的規定刪除，以本章第 360 條取代。[29]由此亦能得見有形的一般文書與無形的電磁紀錄所構成的文書，當同樣面對「毀損」行為時，所可能造成的結果仍有所不同，而有清楚定義後重新修正用語的必要。[30]不過，對於本章的修訂，學界評價也並非全然肯定，有論者便持負面評價，主張新科技只是新的犯罪工具，事實上並沒有產生

---

[27] 修法歷程甚多文獻均有談及，可參見如林山田，《刑法各罪論》，上冊，五版，2005 年，頁 549-550；楊智傑，《資訊法》，三版，2011 年 6 月，頁 126；柯耀程，「『電磁紀錄』規範變動之檢討」，月旦法學教室，第 72 期，2008 年 10 月，頁 117-118；廖有祿、金明燦，「電腦犯罪刑法規範之研究－以二次修正案為中心」，中央警察大學「資訊、科技與社會」學報，第 6 卷第 2 期，2006 年 12 月，頁 60。

[28] 關於舊法竊取電磁紀錄罪與新法無故取得電磁紀錄罪之比較、異同、法律適用等問題，詳參蔡蕙芳，前揭註 24，頁 99-188。

[29] 修法理由謂：「原條文第二項之『干擾』行為方式規定不夠明確，易生適用上之困擾，且本項行為之本質，與有形之毀損文書行為並不相同，為使電腦犯罪規範體系更為完整，爰將本項刪除，另增訂第三百六十條。」可參柯耀程，前揭註 27，頁 118-119。亦可參見前揭註 26。

[30] 事實上，本罪章立法過程實顯倉促，草案審議過程未見深入討論，立法院對於條文內容刪改幅度亦小，學者對此多有批評，或許也是因此才產生後續的爭議與討論。林山田，前揭註 27，頁 550；李茂生，「刑法新修妨害電腦使用罪章芻議（上）」，台灣本土法學雜誌，第 54 期，2004 年 1 月，頁 235。

新的保護法益，新的工具仍是攻擊舊的法益，故本章的修訂僅是彰顯了立法者對於此一新犯罪類型的恐懼而已。[31]

之後於 94 年刑法總則修正時，則為了統一先前分散於各罪的「電磁紀錄」概念，在第 10 條第 6 項中對電磁紀錄一詞做了定義性的規範。[32]至此，我國刑法關於妨害電腦使用罪的相關修法才算是大抵成型。[33]即便如此，例如具有財產性質的電磁紀錄在法律中的定性，立法與實務運作似乎也尚未建立較為完整而妥適的規範，以下僅舉一個判決實例說明之。

## （二）判決個案分析：臺灣高等法院 95 年度上易字第 2110 號判決

### 一、判決事實與爭點

本案事實略謂：被告某甲向自稱「吳志國」之成年大陸男子，透過 MSN 網際網路，以每筆卡號、密碼新臺幣 137 元之代價，購得其所出售智冠公司之「仙境傳說」網路遊戲 GF 月卡卡號及密碼共計 770 筆（係智冠公司下游製造商第一美卡公司遭人入侵公司電腦所失竊者）。隨後，某甲在其住處利用電腦上網之方式，在雅虎奇摩拍賣網站上， 以代號「amor857」張貼販賣前揭 GF 月卡之訊息，而以每筆卡號、密碼 200 元至 250 元之代價出售予不特定人牟利，總計售出 550 筆。嗣智冠公司之員工某乙上雅虎奇摩拍賣網站發現被告某甲販售之 GF 月卡顯低於市價（市價為 350 元）， 進而向被告某甲購買一組 GF 月卡之卡號及密碼，始發現該卡號、密碼係智冠公司交由第一美卡公司製造但未售出之卡號及密碼，乃通知第一美卡公司，並由第一美卡公司會同警方查獲被告被甲，並扣得儲存有 GF 月卡卡號、密碼之筆記型電腦一臺，因認被告甲○○涉犯刑法第 349 條第 2 項之故買贓物罪嫌。

---

[31] 鄭逸哲，「吹口哨壯膽－評刑法第三十六章增訂」，月旦法學雜誌，第 102 期，2003 年 11 月，頁 104-105。

[32] 參柯耀程，前揭註 27，頁 119。刑法第 10 條第 6 項：「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。」

[33] 當然其後仍有相關附屬刑法例如個人資料保護法等的修正，此處先不多作討論，留待後文探討法規間競合與關聯處再做說明。

換言之，本案所牽涉的「贓物」是若干組數字（卡號及密碼），事實上具有經濟價值，購買者購入後，只要進入遊戲公司網站輸入該卡號及密碼進行儲值，即可換取有價之虛擬寶物或遊戲時數等等（視不同網路遊戲商業模式有所差異）。只是這些虛擬遊戲月卡因為是透過網路購得，**並無實體卡片**，被告可能僅是透過對話紀錄、郵件或記事本軟體等方式，將對應的卡號和密碼記錄下來，並對外進行販售。也就是說，**該卡號與密碼是實際上有經濟價值但卻沒有實體物品的電磁紀錄**。因此，本案**爭點就在於判斷該電磁紀錄是否係物，是否受贓物罪之規範**。

**二、法院見解**

法院認為：「查**刑法第 349 條所稱之贓『物』，依據民法第一編總則第三章之規定**而作文義解釋，**應僅指動產及不動產之實體物品而言；至於電磁記錄、權利及財產上之利益則因非實體物品，尚非屬該條所定之贓『物』之文義所得涵攝。**又刑法第 323 條於 86 年 10 月 8 日修正公布時，增列『電磁紀錄』為該條所定之準動產，同時增訂刑法第 339 條之 3 利用電腦設備詐欺罪及刑法第 352 條第 2 項干擾他人『電磁紀錄』之處理之規定（嗣於 92 年 6 月 25 日公布修正刪除，改增訂刑法第 360 條），均可印證電磁紀錄並非刑法第 349 條所稱之贓『物』，始有特別立法加以規範之必要。況刑法第 323 條於 86 年 10 月 8 日修正公布時，雖增列『電磁紀錄』為該條所定之準動產，惟嗣已於 92 年 6 月 25 日修正公布時將電磁紀錄自準動產項目中刪除，改納入新增之妨害電腦使用罪章規範，使電磁紀錄不再成為準動產。換言之，由上開刑法第 323 條與第 339 條之 3 及第 352 條第 2 項等規定之增訂，可知『電磁紀錄』解釋為非屬刑法第 320 第 1 項所稱之『動產』或第 349 條所稱之『物』、第 352 條所稱之『文書』，及同法第 354 條所稱之『物』。從而，刑法第 349 條所稱之贓『物』，自應解釋為不包含『電磁紀錄』在內。此外，由刑法第 339 條第 1 項、第 2 項、第 339 條之 1 第 1 項、第 2 項、第 339 條之 2 第 1 項、第 2 項、第 341 條第 1 項、第 2 項，及第 346 條第 1 項、第 2 項，分別將『物』與『財產不法之利益』分列，可知上開條文所稱之『物』應不包含

『財產上之利益』在內。是刑法第 349 條所稱之贓『物』， 亦應不包含財產上之利益在內。」[34]判決被告無罪。

**三、判決簡評與討論**

簡言之，法院認為**電磁紀錄既非物，自不受以物為標的的贓物罪所規範**。[35]然而，法律論述面的角度吾人固然可以肯認法院見解，其除清楚說明立法歷程作佐證，也闡明電磁紀錄之定性與物的不同等情，對法令的解釋並未踰越其能解釋之範圍，可茲認同；但若從實然面看本案，卻會發現不合情理之處，便係此種「純」電磁紀錄直接擁有經濟上價值時，若缺乏與贓物罪類似的相關法規進行規範，是否變相允許不法取得有價電磁紀錄者轉手販賣而後手並無刑責的情況？由此觀之，亦得見我國法規修正確實缺少通盤的考量，而往往有疏漏之嫌。

## 第三節 妨害電腦使用罪章規範對象與範圍

在對於電腦犯罪、網路犯罪等用語之介紹，以及我國大致的修法脈絡後，現在回過頭來看看本文要探討的主要標的，亦即刑法第 36 章妨害電腦使用罪章。本章章名為〈妨害電腦使用罪章〉，顧名思義主要規範的行為，**應是妨害他人電腦使用權益的行為**，但乍看之下不免令人產生「要怎樣妨害他人使用電腦才構成犯罪」的疑惑。[36]若從內容觀察，本章實際上與外國立法例的資訊刑事法規相當，規範的行為態樣包括前述部分電腦犯罪與網路犯罪所定義的範圍與罪名，但卻又不盡然相同。[37]

---

[34] 臺灣高等法院 95 年度上易字第 2110 號判決。本文以下所引用之判決內容全文，請參見法源法律網，裁判書查詢，網址：http://fyjud.lawbank.com.tw/index.aspx（最後瀏覽時間：2013 年 6 月 1 日）。

[35] 實務上相同見解，參臺灣高等法院台中分院 93 年度上易字第 356 號判決。此外，有論者亦認為未建立針對具財產性電磁紀錄遭不法取得後進行移轉之規範，屬於立法的缺失。參蔡蕙芳，「妨害電腦使用罪章：第二講：本章各罪與他罪之關係」，月旦法學教室，第 129 期，2013 年 7 月，頁 71-73；蔡蕙芳，前揭註 24，頁 170-171。

[36] 舉例而言，刑法分則中類似章名如「妨害性自主」，大抵能使觀者一目了然的想見該章規範的行為態樣係侵害他人性自主權，例如強制性交等行為。反觀妨害電腦使用之章名，與其實際規範的內容間難以產生直接的聯想，究竟以何種手法才能「妨害」到他人使用電腦的權利？此種命名確有值得深思之處。

[37] 立法者認為，我國妨害電腦使用罪章係規範**「專指以電腦或網路為攻擊對象的犯罪」**，雖定義範圍與前開學界主張不盡相同，範圍與定義上也未界定是使用哪一種「電腦犯罪」或「網路犯罪」

另外，本章既然主要針對牽涉「電腦」與「網路」相關的犯罪進行規範，按理說應就主要牽涉的名詞例如電腦等等進行定義，方能明確界定規範的對象與範圍，但就此節立法者卻以科技日新月異，若對「電腦」等名詞作定義，恐有掛一漏萬之虞，因而仿照英國立法例，不對前開名詞下定義。[38]從名正而後言順的角度言之，本文對於立法者此種不作定義的立法方式持反對意見，亦對於「妨害電腦使用」此種曖昧不明的命名方式感到疑惑。

首先，從法律理論角度來看，按刑事法規所規範的內容，對人民基本權的可能侵害較民事、行政法規嚴重，故就刑事法規的立法、用語與司法解釋，都應務求慎重，避免不當侵害人民基本權，因而有所謂罪刑法定原則。[39]其次，刑法的立法與施行目的，除了對於犯罪行為的妥適評價與應報懲罰之外，亦應考量對於社會的公示教育與預防未來犯罪之功能。[40]故刑法從詞彙用語的設計與定義開始，立法者均應考量其對於一般人民是否能達成足夠的公示性，使之瞭解何種行為係刑法會予以追訴處罰的，進而達成有效的教育及預防犯罪功能。若以此一標準檢視，一般人似難免對「妨害電腦使用」此一章節的命名與其規範目的產生疑問，而對於何種「電腦」係應受規範的對象，亦不免產生疑問。

若從實務上觀察，以「妨害電腦使用」為案由對最高法院判決作檢索，可以發現有近半犯罪確實是單純的「電腦」使用犯罪，行為態樣多為刪除了他人（例如行為人剛離職的公司）的電磁紀錄、不法複製他人電腦內文件等與網路無關的

---

的定義方式，但就內容進行觀察，實與外國資訊刑事法規頗為雷同。徐振雄，前揭註 3，頁 41-44。另需注意的是，雖有學者認為，現實中僅有一台單機電腦的系統幾乎不存在，進而以解釋論說明本罪章係以「電腦及其相關設備」的用語立法，其指涉者實乃「電腦系統」或「電腦網路」之概念。參蔡蕙芳，前揭註 25，頁 63。然本文以為，立法當時網路並未如同現今普及，以現今電腦與網路幾難以分離的現況去反推過去立法時的想法，難免有過度補充且脫離當時時空背景的疑慮，可能因而將立法者當時的疏漏透過解釋方法縮小。此雖不失為一種減少問題的方式，但若就實事求是的研究評論角度而言，似無須為立法者過度解釋以圓其說之必要。

[38] 李聖傑，「使用電腦的利益」，月旦法學雜誌，第 145 期，2007 年 6 月，頁 75；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，2008 年 4 月，頁 123-125；林冠宏，「刑法妨害電腦使用罪章之研究」，刑事法雜誌，第 50 卷第 6 期，2006 年 12 月，頁 84-85。

[39] 罪刑法定原則可參林山田，《刑法通論》，上冊，增訂十版，2008 年 1 月，頁 67-87。

[40] 林山田，同前註，頁 52。

類型；[41]但也有近半係與網路連線相關，例如盜取網路寶物、製作虛假帳號供他人犯罪使用、以程式干擾他人網站運作等等。[42]從實然面觀察，則是否本罪章應以〈**妨害電腦與網路使用罪章**〉為名，使章名更為恰當而貼近現實？

縱然撇開法律理論不談，對於此種牽涉技術性質的犯罪，實務上要解釋及操作，往往需要仰賴此領域的專家作鑑定或出具相關報告。[43]然而，就本章主要規範的「電腦」和「網路」等名詞所指涉之事物，在熟習此一領域的專業人士眼中是否早有相關定義的共識，而可能與法律所認知範圍不全然相同？舉例來說，「電腦」（computer）一詞，若從英文直譯應為「計算機」，在資訊工程領域中，要介紹計算機的由來，往往會以**算盤**作為計算機的始祖，但算盤是本章要規範的對象嗎？[44]以技術角度來說，現代科技產品大量使用的嵌入式系統（embedded system），在資訊領域中確實將其列為電腦的一種，但若在法律爭訟中要由未接受過相關訓練的法官去作判斷，似乎只是徒增審判上的困擾而已。

最令人納悶的是，既然電腦、網路、電磁紀錄等名詞與本罪章主要規範的犯罪行為有高度緊密的關係，則為何電磁紀錄在刑法第 10 條第 6 項能作定義，電腦和網路卻不以相類似方式處理？[45]舉例來說，在資訊工程領域的定義中，近代電腦通常略可被理解為「能將演算法編程為數學或邏輯指令以進行計算之裝置」等等。[46]對於「網路」一詞，則通常可解釋略為「將複數電腦系統連結以傳送、分享資訊與資源之裝置」等等。[47]蓋電磁紀錄與電腦等詞彙，既然同屬本章各罪構成要件所必須，何以不能作等同處理，以杜爭議？

---

[41] 例如最高法院 100 年度台上字第 6468 號判決。

[42] 前者例如最高法院 98 年度台上字第 2908 號判決，後者例如最高法院 100 年台上字第 3411 號判決。

[43] 此種情況在實務運作多不勝數。例如最高法院 101 年度台上字第 5058 號判決所處理之案件，便係委由刑事警察局針對相關紀錄檔作鑑定。又如臺灣高等法院 98 年度上訴字第 3246 號判決中，亦有出現委託臺灣微軟公司出具之鑑識分析報告等語。

[44] J. GLENN BROOKSHEAR, COMPUTER SCIENCE: AN OVERVIEW 4-8 (8th ed. 2005).

[45] 刑法第 10 條第 6 項：「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。」

[46] *Supra* note 44.

[47] *Supra* note 44, at 136. *See generally* DOUGLAS E. COMER, COMPUTER NETWORKS AND INTERNETS (4th ed. 2004).

若對照外國立法例觀之，我國現行立法方式亦屬少見。例如美國聯邦電腦詐欺及濫用防制法（CFAA）對於電腦便定義為「得以執行邏輯、計算及儲存功能的電子、磁性、光學、電子化學或其他高速資料運算裝置，以及其他相關或是與上述高度資料運算裝置同工的資料儲存及通訊裝置。不包括自動打字機、自動機、手持計算機或其他類似的裝置。」；[48]歐洲理事會《網路犯罪公約》的第 1 條亦對於電腦系統、網路都訂有相當清楚而詳盡的定義。[49]

本章法條構成要件設計時，已經用到多次「電腦」這個詞彙；在實務運作上，本章又需要處理相當多與網路相關的犯罪行為。從前開不論是比較法的觀點，抑或是資訊工程領域的角度，均可發現要對電腦和網路等語做出普遍性的抽象定義並非不可能，也未必真的會掛一漏萬，甚至可能利於未接受過資訊相關訓練或教育的實務工作者在面對個案時做出正確判斷。因此本文以為，立法者不對電腦、網路等重要名詞做出定義，實際上已經使得本章規範範圍模糊，不但可能容有技術抗辯的空間，且與刑事法上罪刑法定原則產生較為緊張的關係，無法有效對一

[48] The Computer Fraud and Abuse Act of 1986, 18 U.S.C 1030(e)(1) ("the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;"). *See generally* CHUCK EASTTON & DET. JEFF TAYLOR, COMPUTER CRIME, INVESTIGATION, AND THE LAW 71-168 (2011). *See also* The Computer Fraud and Abuse Act of 1986, 18 U.S.C 1030(e)(1), *available at* http://www.law.cornell.edu/uscode/text/18/1030 (last visited Dec. 1, 2012).

[49] Article 1 (a) – Computer system
A **computer system** under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices "Automatic" means without direct human intervention, "processing of data" means that data in the computer system is operated by executing a computer program. A "computer program" is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A "peripheral" is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.
A **network** is an interconnection between two or more computer systems. The connections may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols. Other types of networks exist, whether or not connected to the Internet, able to communicate computer data among computer systems. Computer systems may be connected to the network as endpoints or as a means to assist in communication on the network. What is essential is that data is exchanged over the network.
Convention on Cybercrime, Nov. 23, 2001, CETS No.185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited Dec. 1, 2012).

般民眾發生公示效果、達成預防犯罪的目的，係第一個需要探討改進的問題。

## 第四節 小結：以抽象定義劃定規範對象與範圍之優勢

從前開比較法的角度我們可以發現，不論係歐洲理事會《網路犯罪公約》，或是美國聯邦刑法，事實上都有對於主要規範客體的電腦作抽象的定義。[50]此舉不但能夠清楚劃定規範對象與範圍，強化對人民的警示與犯罪預防效果，更能切合於罪刑法定原則。[51]

不管就刑法公示及預防犯罪的目的來說,抑或是從罪刑法定原則的角度而言，若不能將資訊刑法中至為重要的詞彙做出定義，不但可能造成實務運作上的困擾與爭議，更可能間接使得國家建立資訊刑事規範用以保障資訊安全的目的落空。所以本文以為，以抽象定義去劃定規範對象與範圍，是建立完善資訊刑法框架的立基點。

雖有論者認為，立法者係因徬徨於「科技中立」的考量，而不願意明確對電腦、網路等詞彙加以定義，推想應係希望透過**實務個案解釋**去應對未來的科技發展。[52]甚至有論者主張，美國聯邦電腦詐欺及濫用防制法雖有對電腦做出定義，但實務操作上卻採取寬鬆的解釋,藉此說明我國現狀下交由司法實務去解釋「電腦」，係相當彈性而妥適的立法方式。[53]

本文對前開論述所言卻持不同意見。首先，若立法者真的是因為「科技中立性」而感到徬徨，進而決定不對相關詞彙作定義，則為何在第 362 條製作電腦程式罪的要件設計卻全然看不出考量過「科技中立性」的痕跡？[54]若立法者有科技中

---

[50] The definition of "computer" in CFAA, *supra* note 48. The definition of "computer system" and "network" in Convention on Cybercrime, *see id.*

[51] 例如美國法便於電腦定義中，排除並非規範對象的打字機、計算機等等可能（資訊工程領域的）電腦定義所囊括的機器，由此可知，抽象定義確實可作為清楚界定規範範圍與對象的立法方法。

[52] 徐振雄，前揭註 3，頁 55；林冠宏，前揭註 38，頁 84。論者也批評即便立法者真是如此認知，似乎也需要做出基本的定義，以免模糊地帶的設備裝置例如 PDA、手機等判斷上出現恣意或落差。

[53] *Supra* note 48. 蔡榮耕，前揭註 38，頁 114-115、123-125。

[54] 簡言之，本文以為第 362 條所謂「損害性程式」的立法設計，根本違反了科技中立性此一原則，因為事實上並沒有任何一個程式只能作「損害性」的使用。科技本身都是中性的，立法者此種設計顯然沒有科技中立行的概念，與此處論者為立法者所作的科技中立性解釋云云顯然相左。關於

利性的思為，對於爭議更為明確的第 362 條要件設計上應有更多琢磨的空間；倘若立法者根本沒有此一概念，則以後見之明為其開脫，似亦意義不大。

其次，妥適的立法本應考量各種因素，包括實務操作者的學識、法律理論等等。一般法律實務人士普遍缺乏資訊背景訓練，加以欠缺基本的法條定義可供解釋操作時，不但立法結果與罪刑法定原則有違，此種「授權」是否過度而可能導致司法恣意或認知歧異，也是相當值得擔憂的。

反面言之，倘若能在法律中，不論仿照外國立法例或委請專業人士協助，藉此訂立**基本的、抽象的詞彙定義**，除了能先紓解與罪刑法定原則間的緊張關係，實務解釋也能因此有所依循，此舉亦不礙於司法機關針對未來新興的科技產物做出解釋。事實上，前開論者所舉的美國法例，恰好支持了本文的見解，亦即立法者先作成了抽象的定義後，再交由司法機關繼續發展實務見解，不但未有掛一漏萬之情況，更能讓司法機關在有所依循下，能謹慎按照立法意旨的脈絡去充分實現規範目的。更進一步言之，倘若司法實務確實面臨了難以套用舊有抽象定義的新科技時，其實也反映出法律本身可能已經過時而有待檢討，此時對法律進行修正自然是立法者責無旁貸的工作，又豈能因為擔心科技發展太快就逃避面對此一責任呢？

此外，在設計抽象規範的過程中，可仿照美國聯邦刑法的立法模式，明文排除立法者認為不符定義的物品，藉此清楚確定規範的對象與範圍。[55]總的言之，科技發展確然日新月異，法令的名詞用語與時俱進、檢討修正卻也是立法者無可迴避的義務。若擔憂抽象定義可能因為資訊發展而跟不上時代，大可定期檢討修正。縱然擔憂抽象定義可能造成實務操作不便，或因為缺乏相關知識而解釋困難，亦可於立法時仿照其他技術性強烈的法規，授權主管機關訂立相關的管理辦法等等配套措施，對於抽象定義作進一步的例示，以利實務操作即可。[56]

---

第 362 條與科技中立性之討論，詳參本文第四章第四節。

[55] 參前揭註 51。

[56] 舉例而言，我國證券交易法第 157 條之 1 第 5 項及第 6 項便有「重大消息」此種事關財經專業

的名詞。主管機關為此訂定了「證券交易法第一百五十七條之一第五項及第六項重大消息範圍及其公開方式管理辦法」，以利實務操作，便係著例。

# 第三章 保護法益的爭議

## 第一節 實務與學說的爭論

本章屬於刑法分則編的一章，而我國刑法分則體系仿照德國法，係以國家、社會、個人專屬、個人非專屬法益的順序作章節編排，各章分別有其所保護的核心法益。[57]在這樣的刑法分則體系下，從學術角度論，各章間層次井然，法益輕重一目了然；而對於實務操作最具有實益的，則是可以藉由法益的判斷，對於犯罪行為中牽涉的罪名作競合，並且正確解釋構成要件，藉此妥適評價其犯罪行為。

本章從立法之初至今，持續為學界、實務所討論者，即屬本章「保護法益為何」此一問題。此一爭議係由於立法理由認為本章所保護之法益，**乃兼及於社會和個人法益**。[58]然而，此一主張向為學界所強力抨擊，論者認為刑法體系中固然有雙重法益的規定，但法益之間仍有主從之分，而非如立法理由所稱並列並重，本章修訂所採的雙法益說，堪稱自行創造了不合傳統刑法體系的新理論。[59]

為了解決本章保護法益的爭議，論者紛紛提出不同見解。有認為本章從系統解釋的角度逐條解讀後，認為貫穿本章各罪所保護之核心，係「資訊社會的安全秩序信賴」，應作社會法益解釋較為妥適。[60]通說則以體系解釋為本，認為由本章在刑法分則所排列的位置，可以推知本章應屬於個人法益。[61]甚至有論者以為，此

---

[57] 林山田，前揭註 27 書，頁 43-44；許恒達，「資訊安全的社會信賴與刑法第三五九條的保護法益－－評士林地方法院九十九年度訴字第一二二號判決」，月旦法學，第 198 期，2011 年 11 月，頁 238；林冠宏，前揭註 38，頁 86-89。

[58] 甘添貴，「虛擬遊戲與盜取寶物」，台灣法學雜誌，第 50 期，2003 年 9 月，頁 179-180；李茂生，前揭註 30，頁 239；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，2003 年 9 月，頁 122。另有學者認為，本章立法以「電腦或網路安全」為保護法益，並進一步以網路犯罪公約所謂「電腦資料與系統的私密性、完整性與可使用性」做闡釋，似有將立法者明文指出的（傳統）雙法益說投射至新法益之見解。參蔡蕙芳，前揭註 25，頁 64。本文則認為，電腦或網路安全，或是網路犯罪公約所稱「電腦資料與系統的私密性、完整性與可使用性」，固然是本章立法主要保護的標的，也確實屬於一種吾人可見、可及的利益，但以現行法架構來說，要創設新「法益」勢必要面臨刑法體系之挑戰，似仍以將此等利益按其性質，分別回歸至傳統法益分類，應為較佳的方式。

[59] 李茂生，前揭註 30，頁 239-240。

[60] 李茂生，前揭註 30，頁 239-247；許恒達，前揭註 57，頁 240-244。

[61] 林山田，前揭註 27 書，頁 549；林冠宏，前揭註 38，頁 90。值得一提者，係主張個人法益的學者中，也有別開蹊徑，主張以使用電腦為一種新型態的利益為出發點思考，導引出本章以保護

種犯罪的特性係同時為犯罪類型卻也是犯罪的方法，而牽涉的法益保護可能囊括個人、社會和國家法益，應以個案作認定，若要以刑法體系作解釋必然會遭遇相當的困難。[62]

從實務上判決意旨也能發現此一爭議的蹤影。舉例來說，臺灣高等法院臺南分院 99 年上更（一）字 10 號刑事判決，便認為本章規範實際上係維持網路電腦使用的社會信賴及社會秩序，屬於社會法益的保護，並不以具體的實際損害為成立要件，臺灣高等法院 95 年上訴字第 2674 號判決亦持類似見解。但最高法院 98 年台上字 3015 號刑事判決、100 年度台上字第 6468 號刑事判決等，卻似都認為本罪章側重保護個人法益為主，而需要對於損害作精確的認定。其中，臺灣高等法院 95 年上訴字第 2674 號判決似因採社會法益說，對於犯罪致生之損害認定論述較為模糊，因此遭最高法院指摘，以最高法院 98 年台上字 3015 號刑事判決撤銷發回。[63]由此一案例，顯可得見此一保護法益爭議除了引發學界討論外，更確實影響實務審理，確有討論空間，是為本文所認第二個值得探討解決的問題。

## 第二節 以法解釋學觀點主張本章保護社會法益之討論與缺點

有論者以法解釋學方法，略謂本章保護法益原則上為社會法益，而在與個人法益重疊的部分，係將對個人法益的侵害程度作為斷定犯罪嚴重程度的判斷標準。此時個人法益雖與社會法益重疊，但已經被社會法益所涵蓋保護，罪名部分則以競合論處理。[64]

首先應注意者，係刑法保護社會法益之罪，事實上都與個人法益保護有所重疊。舉例而言，若行為人以放火的方式從事殺人行為，此時可能同時觸犯刑法第 173 條第 1 項放火或失火燒燬現住建築物及交通工具罪，以及刑法第 271 條第 1 項殺人罪。就本例而言，刑法第 173 條第 1 項之罪，其保護的法益其實主要是保障

---

個人的「安心領域」為核心，並將現實和虛擬的「**空間**」作比較後，認本章主要處罰對於虛擬空間的領域破壞，最後推論出本章主要保護個人法益者，參李聖傑，前揭註 38，頁 70-79。

62 張紹斌，「刑法電腦專章及案例研究」，軍法專刊，第 54 卷第 4 期，2008 年 8 月，頁 90。

63 此一爭議與判決內容、評析等，詳參本文第四章第二節。

64 李茂生，前揭註 30，頁 239-247。

公共安全的社會法益，而同時重疊了個人生命法益的保護。刑法評價上係以刑法第 55 條想像競合，從一重處斷。

本文以為，前開論者說法雖不無可觀之處，可惜似乎仍有缺陷。首先，論者對於第 358 條無故入侵電腦罪的保護法益，論述上即未能圓滿的說明其保護的也是社會法益。[65]若與我國刑法結構較為相似的德國法比較，便能發現其主張恰與論者相反，而採取（相當於）本章之罪（的條文）皆**原則上屬於個人法益**的論點，分別放置於各個人法益章節。[66]

再來，刑法上各罪之所以有其保護的核心法益，其目的在於妥適評價各種不同行為可能侵害的客體，及可能造成危害的嚴重性。以前開放火罪案例而言，誠然放火罪保護核心是社會法益，也就是規範放火行為可能對於公眾的生命造成的巨大危險，在此個人法益作為附屬法益被保護。但公共危險罪的目的是防止該對公眾危險的產生，縱然最終目的係保護（複數的）個人法益，但因為此種危險若實現時所生危害可能相當嚴重，故刑法評價上並無待實害（對於個人法益的侵害）實現便介入處罰，以期提早避免實害的實現。也就是說，即便社會法益都有附屬的個人法益存在，但兩種法益間評價的重點、保護的程度、公權力介入的時點等等均有所不同，並不能一概而論。

正因為社會法益之罪有此特性，若將本章之罪皆視為社會法益時，須面臨的問題就是，當個人確實因為本章犯罪行為而有損害時，解釋上要如何說明此種個人規模的侵害足以造成社會公益層級的危險呢？其次，就算從各罪行為本質分別來看，直觀上仍然不免從個人的秘密隱私（第 358 條）、個人的財產（第 359 條）等法益作評價，若直接一律上綱為社會法益的評價方式，似不免有疏漏和無法銜接之處。

的確，在特定情況下，第 358 條入侵行為侵害的確實一望即知是侵害社會法

---

[65] 李茂生，前揭註 30，頁 242-243。論者對於第 358 條保護法益的論述，僅能看出對立法技術的批評、對立法本意的揣測等等，甚至也直言第 358 條罪質相當曖昧模糊，難以清楚定義。

[66] 葉亭巖，「德國刑法第 41 次修正－『反駭客法』之簡介」，科技法律透析，第 20 卷第 4 期，2008 年 4 月，頁 18-22。詳細討論可參考本章第三節內容。

益，例如被入侵的電腦可能是戶政機關的主機；但反過來說，一般情況下吾人顯難將入侵一般個人電腦的行為，直接與侵害社會法益間作連結。故對於性質上可能不足以（或稱未必）生公眾危險的侵害行為，一律以社會法益定性的作法，雖似乎可以為法益爭議提供一個可能的解答方向，但就整體而言並非妥善的方案，故本文尚難以全然認同。

## 第三節 比較法上德國法將資訊犯罪定性為個人法益所面對的問題

從比較法的角度觀察，法益爭議的處理或可以與我國刑法體系相近的德國法為借鏡。德國刑法並未將資訊系統犯罪成立專章。取而代之的，是將需要規範的各種行為態樣，分別按照立法者認為主要保護的核心法益，分配到保護該法益的章節中。[67]最近一次的修法則被稱為《反駭客法》，修正了妨害個人秘密罪章中關於探查、截取電磁紀錄的條文，以及毀損罪章中變更刪除電磁紀錄罪等，主要目的是為了強化資訊系統安全的保護規範，以達到歐洲理事會及歐盟法要求的規範水平。[68]

然而，本文認為，德國刑法此種作法固然在短期內似乎仍可維繫其核心刑法的體系與架構，但就長遠而言，仍然會面對不斷產生新的體系例外問題。舉例來說，德國刑法**毀損罪章**中規定了 303b 妨害電腦使用罪（computer sabotage）（行為態樣類似於我國第 359 條、第 360 條的混合體），亦即認為本條核心係屬於個人法益；然後在 303b(2)和 303b(4)中，以加重結果犯的方式規範受侵害客體為企業、公務機關和侵害規模較大的犯罪態樣，藉此解決犯罪行為態樣相似、但侵害規模卻近乎達到社會法益層級的問題。[69]

---

[67] 林山田，前揭註 27 書，頁 550。德國法相關內容亦可參見李崇偉，「美、日、德三國網路犯罪相關法制之探討」，中央警察大學法學論集，第 9 期，2004 年 3 月，頁 162-169。

[68] 葉亭巖，前揭註 66，頁 18-22。

[69] 詳細條文翻譯可參見葉亭巖，前揭註 66，頁 20-21。*See* German Criminal Code (English version), *available at* http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html (last visited Dec. 1, 2012).

從刑度來看，透過加重結果犯的方式，確實可以妥適的反映出犯罪侵害結果規模較大時所對應的罪責；但沿著此種思維往下探討，卻也可以反推出德國法應也認為這種實質上牽涉社會法益的犯罪型態的刑度應予以加重。即便承認了此種行為態樣也可能嚴重到社會法益的層級，本文推想，德國法應是為了維持刑法體系完整，修法時卻又只能將各罪分列在不同個人法益的章節中處理，再透過搭配實際上是保護社會法益的加重結果要件，該加重之罪便成為一種「實質例外」，也就是藏在個人法益罪章中的社會法益之罪。事實上，本文以為此種作法不但未解決法益不一致的問題，更可能把法益不一致的情況因而擴散到更多罪章去，形成另類如同我國妨害電腦使用罪章的情況而已。

本文可想見若未來持續產生新行為態樣的犯罪類型時，德國刑法此種「藏在個人法益中的社會法益之罪」的例外，可能會持續增加；累積到一定程度時，甚至可能造成體系崩壞的危險。因此就保護法益問題的處理，雖可部分肯定德國法的處理思維，但本文對該方案仍有疑慮，而認為並非全然妥善的解決方式。

## 第四節 小結：試論近程及遠程之法益爭議解決方案

以我國現況而言，**近程的解決方式須委諸司法判決統一見解**，透過個案侵害的輕重程度，對於構成要件解釋的寬嚴作調整，避免實際上侵害了社會法益的犯罪，因為損害難以證明而成為漏網之魚；同時，也要避免實際上僅侵害個人法益的犯罪，因為刑度的設計不當，而有刑責過度評價的情況。[70]然而遺憾的是，目前較無爭議者，僅有透過第 361 條加重的犯罪態樣已由司法判決統一見解，其餘例如本文所談及的被害者為大型私人機關的犯罪類型，仍有待司法判決見解的累積與統一。[71]

**遠程解決方案部分，則需要系統性的檢討並修正現行法令，必要的話甚至應**

[70] 但此種方式實質上可能會引致司法權侵害立法權的批評，故實務運作上須格外留意，不能過度踰越司法權範疇作出不當解釋與見解。

[71] 最高法院 97 年度台非字 285 號判決、最高法院 99 年度台上字第 6306 號判決意旨參照。詳參本文第四章第五節關於第 361 條的介紹。

**該訂立新法建構新的資訊刑事體系**。本文在此大膽提出一個可能的方向，即係在某些行為類型的罪名中，可將之分列為個人及社會兩條獨立條文的作法，藉以解決法益的爭議。舉例來說，針對變更電磁紀錄行為，可設計一條係**保護個人法益的變更電磁紀錄罪**條文，以結果犯的方式規制，須證明實際損害才受到刑事的處罰，並且保留告訴乃論的規定，減少情節過度輕微的案件大量湧入法院。在此**同時**，也並列設計另一條**保護社會法益的變更電磁紀錄罪**，構成要件部分則採用類似公共危險罪章的設計，以危險犯的方式規制，輔以未遂犯、預備犯等規定，因為行為可能損害較廣，故將刑罰權介入的階段提前，且定性為非告訴乃論之罪，由國家掌握偵查訴追的權限。[72]

本文此種主張的優點，係透過不同嚴格程度及構成要件的設計，使得相類似行為在犯罪規模不同、侵害客體不同、損害結果嚴重度不同的情況下，可以採用不同法條（搭配不同保護法益）處理，藉由訂立對應的妥適刑度，減少現行法僵硬的刑度造成評價錯誤的情況。例如同樣是變更電磁紀錄行為，若受害的客體僅係一般私人電腦，因為法條設計是結果犯，加上告訴乃論的規定，可以過濾掉情況輕微甚至並無損害可言的案件，減輕司法負擔；反之，若受害客體是重要公務電磁紀錄，或是收錄大量個人資訊的私人伺服器資料庫等情節重大的犯罪，賦予偵查機關判斷是否足生公共危險的裁量權，決定公權力是否需要介入處理此一侵害社會法益的犯罪，倘若偵查機關認為本案尚未達侵害社會法益的公共危險層級，則將是否發動（侵害個人法益的變更電磁紀錄罪）告訴的決定權交由被害人自行判斷。

透過這種個人法益與社會法益分列的法條結構，若能搭配訂立新法跳脫刑法罪章地位的拘束，現行法中妨害電腦使用罪章為人詬病、爭議不斷的法益問題便迎刃而解。刑事規範之設計必然有其核心保護法益，但是現行法將本罪章置於刑

[72] 侵害的嚴重程度是否達社會法益的層級，應由立法者進行判斷，並設定相對應的標準。事實上，現行法第 361 條將受害客體為公務機關的犯罪加重刑度，某層面上就是一種粗糙的侵害嚴重度判斷標準了。

法分則中，因為刑法分則原先就有著罪章法益的概念，竟反客為主的導致學界、實務受限於刑法舊有原則，而必須牽強的為刑法體系做出保護法益的圓滿解釋，致生後續操作與學說討論上之爭議，實非良事。故本文主張應另立資訊刑法，使資訊刑事法規得以脫離刑法分則的舊有限制，並透過個人與社會法益分列的條文設計，藉此機會重新檢視資訊刑法所規範的行為態樣所牽涉的法益為何？是否可能有造成社會資訊安全危險的可能性？又或是該行為僅設計結果犯已足？訂立新法的機會除了提供立法者一個重新審視現行規範的機會，也能藉此將過去設計上的缺失補正，並且清楚的對於某些價值評斷的問題做出釐清。

# 第四章 構成要件的檢討

本章將就現行妨害電腦使用罪章的各罪構成要件，進行逐條的討論與檢討，透過整理學界所提出的相關評論為引，接著將本文所檢索到的各罪相關實務判決進行介紹與評論，最後提出對於構成要件修正的方向。

應特別說明者，係構成要件的修法需要深入研究及討論，並且仔細思考與他罪（甚至其他法律）的競合與重疊，是一件立法大工程，實非三言兩語可以交代清楚。故本文在此僅能簡單建議大略的修正方向，而不對條文構成要件作逐條、逐字的檢討，並在本文文末以附錄方式舉例說明本文所建議的修法後條文設計。

本文認為，條文的檢討方向，大抵應以第三章第四節提及的遠程解決方案中，將**同一行為分列雙重法條設計為原則**，先檢討現行法中，何種行為態樣是可能因為犯罪規模、侵害客體的不同，而需要分別訂立個人及社會法益之罪的條文。

其次，**對於各條文中受侵害客體究竟為「電腦系統」本身，抑或是「電磁紀錄」做出明確的界定**，除能避免規範漏洞外，亦能對於構成要件作更加精準的描述。[73]事實上，在法律條文設計中，同一語意的相類似行為所能侵害的客體未必完全相同。舉例來說，若「干擾」無線網路訊號的傳遞，使得接收端因為封包漏失而產生網路擁塞，受干擾的客體其實是無線訊號，但以現行法來說應較為接近「電磁紀錄」；反之，也可能對電腦系統本身透過程式「干擾」，例如以程式佔用 CPU 資源，使「電腦系統」處理資料的速度大幅下滑等，此時受到干擾的客體應是「電腦系統」。故對於同樣的行為態樣，確實存在不同受侵害客體的不同情況，這點現行條文似未注意而漏未處理，屬於共通性應修正的標的。

## 第一節　　第 358 條

刑法第 358 條為入侵電腦或其相關設備罪：「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，

[73] 以我國現行法來說，還有「相關設備」需要作定義。

處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」立法理由為：「鑒於對無故入侵他人電腦之行為採刑事處罰已是世界立法之趨勢，且電腦系統遭惡意入侵後，系統管理者須耗費大量之時間人力檢查，始能確保電腦系統之安全性，此種行為之危害性應已達科以刑事責任之程度，為保護電腦系統之安全性，爰增訂本條。」[74]

本條最為人所批評者，係在構成要件中明定三種犯罪手法，行為人必須是以其中任一種手法進入電腦內，方該當本條所謂的入侵電腦行為。然而，從比較法角度觀察，外國立法例對於入侵行為的判斷，往往是以行為人是否有權（或獲得授權）作為是否入侵的判斷依據，藉由權限的判斷而非犯罪手法來斷定入侵，本文以為應係較佳的立法方式。

關於第 358 條的相關判決，在（二）判決實證：臺灣高等法院 101 年度上訴字第 2540 號判決中，可以看出行為人在使用非構成要件所明定的手法，卻實質上實施無權侵入電腦的行為時，現行法規的漏洞。而在（三）判決實證：臺灣高等法院 100 年度上易字第 2136 號判決中，除討論構成要件的漏洞外，也論及入侵行為既遂與未遂的判斷，以及法院對於構成要件中「無故」的見解等。

### （一）學界評論

第 358 條入侵電腦或其相關設備罪，條文設計上列舉三種犯罪手法作為構成要件，分別為「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」，藉以限縮本罪適用範圍，避免處罰過廣，屬於開放性漏洞立法方式。有論者以為，本條法條結構因設計不當，使得條文性質上又像舉動犯、又像結果犯，造成適用上的困難。[75]易言之，因為條文前段列舉了三種不同行為，

[74] 前揭註 29。

[75] 柯耀程，前揭註 58，頁 123-124、126-127；王銘勇，「侵入電腦系統罪之研究」，法令月刊，第 55 卷 3 期，2004 年 3 月，頁 29；廖宗聖、鄭心翰，「從網路犯罪公約談我國妨害電腦使用罪章的修訂」，科技法學評論，第 7 卷第 2 期，2010 年 12 月，頁 75-76。亦有學者認為，事實上本條雖確兼有行為犯與結果犯的特性，然而在行為與結果在時間與空間條件下能夠被區分時，可以視為結果犯杜此爭議。參蔡蕙芳，前揭註 25，頁 65-66。

似在暗示只要行為人進行其中任一種行為即該當本罪，無須等待結果發生，係舉動犯的性質；然而本條後段所謂「入侵」之要件，似又暗示須有入侵結果產生，構成要件才該當，應屬於結果犯，本罪性質上因而產生許多矛盾，可能造成適用上的困難。[76]這種條文的設計，在既遂與未遂的判定上往往很容易致生爭議與困難。

其次，論者有認第 358 條的問題中最嚴重者，係限縮入侵手法的立法方式，可能導致規範保護不周的問題，使得即便行為人惡意入侵，或是被入侵電腦根本未設置密碼等防護措施時，因為不符本條所列舉的構成要件手法，則不成立本罪，因而產生規範漏洞。[77]縱然認為某些入侵行為的嚴重性並不足以達到刑事處罰的程度，以此種硬性的手法侷限來限縮本條適用範圍，仍屬較為不妥的立法方式。

另有論者則批評本罪應區分所侵入電腦所儲存資訊的性質，界定其行為所侵害者究屬個人隱私、營業秘密或係國防機密等，才能正確評價其行為侵害程度與應得刑度。[78]此一論點，其實與本文第三章論及法益爭議時所討論者有關，畢竟受入侵對象不同時，其造成損害的規模亦不相同，牽涉法益自也可能產生出入，則此時自應建立相對應的判斷標準，才能正確的評價犯罪行為的嚴重性。

也有論者以為，真正更嚴重的類型並非來自外界的入侵，而係任意在網路上提供合法帳號密碼予他人從事犯罪行為的「助長不法連線罪」，才是與本罪相關但更有待規範的類型。[79]所謂助長不法連線罪，主要是處罰行為人任意的散布帳號密碼，在網路上以類似現實世界中人頭的方式，幫助欲透過人頭帳戶掩護其他犯罪的行為人作案，而對此種幫助犯之行為作正犯化的規範。

---

[76] 柯耀程，前揭註 58，頁 123-124、126-127；王銘勇，同前註；廖宗聖、鄭心翰，同前註。

[77] 柯耀程，前揭註 58，頁 123-124、126-127；蔡榮耕，前揭註 38，頁 125-128；曾淑瑜，「九十二年刑法增訂妨害電腦使用罪章前後之法律適用」，華岡法粹，第 31 期，2004 年 5 月，頁 129-130。實務工作者認為本條雖規範了三種不同的入侵方式，但實際上多數案件均屬「無故輸入他人帳號密碼」類，後兩者則使用頻率甚低，參張紹斌，前揭註 62，頁 88-89。

[78] 王銘勇，前揭註 75，頁 30。

[79] 李茂生，「刑法新修妨害電腦使用罪章芻議（中）」，台灣本土法學雜誌，第 55 期，2004 年 2 月，頁 243-252。日本法上「助長不法連線罪」之相關介紹，可參見王銘勇，前揭註 75，頁 26-28；李崇偉，前揭註 67，頁 159-161。

## （二）判決個案分析：臺灣高等法院 101 年度上訴字第 2540 號判決

### 一、判決事實、爭點與法院見解

本判決主要的系爭法條是 359 條無故取得他人電磁紀錄罪，但高等法院在本案中針對被告涉及第 358 條入侵電腦罪部分，作了不另為無罪諭知，其理由恰可說明第 358 條構成要件的問題。

本案事實略謂：被害人甲女與被告乙男為前男女朋友，而曾有同居關係。其後因乙男發現甲女疑似另結新歡，而趁著甲女將設有密碼的電腦開機後暫時離開的空檔，其時電腦尚未進入休眠密碼保護模式，而逕行使用甲女電腦內複製甲女與訴外人丙男出遊照片後，之後將該照片散播，為甲女發現後提起本件告訴。

本案之爭點在於刑法第 358 條前段限制入侵行為之手法需為「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」，倘若行為人非使用前揭任一手法進入與使用電腦，並不構成本條之罪。則本案被告之行為，似不合於前接任一手法，是否構成本條之罪？

本案中，告訴人甲女證稱從未告訴乙男其所使用電腦之密碼，平常除了長時間離開電腦前會將電腦銀幕蓋上使其休眠外，若短時間離開則通常不會使其休眠。換言之，甲女之電腦雖設有密碼，惟在短時間離開電腦期間因電腦尚未進入自動休眠，則不會進入需重新輸入密碼的認證畫面。法院由此斷定在被告乙男不知密碼的情況下，確實有可能是趁著甲女暫離期間使用其電腦，複製前開照片。法院認為：「……是揆諸上揭說明，被告既**非以輸入電腦密碼方式開啟電腦為之**，即無構成刑法第 315 條之開拆封緘之行為，亦未構成刑法第 358 條之無故輸入他人帳號密碼侵入他人電腦之行為」而對檢方起訴乙男涉犯第 358 條之部分作了不另為無罪諭知。

### 二、判決簡評與討論

從這個案例可以看出第 358 條構成要件設計的「開放性漏洞」所產生的問題。在構成要件特別規定必須符合「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」的手法時，在本案此種設有密碼但因為電腦尚未自動休眠的情況下都無法適用，更遑論未設有密碼的電腦了。但如同本案被告這種未獲授權就私自進入（使用）電腦的行為之可罰性，竟需仰賴該電腦是否設有密碼、是否啟動時會進入認證畫面等條件來判斷，與一般人民的認知似乎有所落差，在構成要件的設計上應有值得檢討的地方。

## （三）判決個案分析：臺灣高等法院 100 年度上易字第 2136 號判決[80]

### 一、判決事實與爭點

本案事實略謂：被告某甲係 NSM 公司對臺灣大哥大股份有限公司維修業務之履行輔助人，於 97 年 6 月前，負責維護台哥大公司 TA 主機系統業務。嗣 NSN 公司將維修 TA 主機系統業務交由同公司之 PS CORE 小組處理，某甲即進入處理 ICD 及 iGMLC 專案之小組，惟某甲仍協助處理維修 TA 主機系統業務。某甲明知在維護 TA 主機系統時，可採「現場維修」或「VPN 遠端網路連線」等方式進行，如認有必要採「VPN 遠端網路連線」方式進入臺灣大哥大公司管理之電腦系統時，應先申請取得授權，始得在遠端即機房以外地點，以 VPN 方式連入，進行維修工作，並於維修完畢後，由臺灣大哥大公司關閉連線，以免臺灣大哥大公司內部電腦系統直接曝露在網際網路上發生危險。惟某甲仍貪圖方便，未取得臺灣大哥大公司以 VPN 方式連線作業之授權，而在臺灣大哥大公司人員不知情下，使用臺灣大哥大公司行動電話網路卡，逕以 MMS 模式連線及輸入 TA 主機帳號密碼之方式，登入 TA 主機，迴避臺灣大哥大公司上揭 VPN 管制措施，而無故利用臺灣大哥大公司管理網路電腦系統之漏洞，入侵臺灣大哥大公司管理之上揭 TA 主機電腦及其相關設備。後以無故入侵他人電腦及相關設備罪起訴。

簡言之，本案爭點在於**委外網管人員**貪圖方便而採用**未獲授權的連線方式進行主機維護工作**，是否構成刑法第 358 條無故入侵他人電腦與相關設備罪。本案

[80] 本案歷審判決為：臺灣新北地方法院 99 年度易字第 2352 號判決、臺灣高等法院 100 年度上易字第 2136 號判決。

中，台哥大公司關於 TA 主機系統維護標準的作業程序，是先由委外網管提出連線申請後，由網管中心發給 VPN 連線密碼，委外網管透過 VPN 進行連線後，輸入 TA 系統的帳號密碼進行維護。維修完成後，網管中心會關閉權限，下次若需要再透過 VPN 進行連線時，需再次進行申請並由網管中心發給新密碼（亦即每次申請獲得的密碼都不一樣）。假若 VPN 連線方式無法使用時，則可以直接到台哥大機房所在地進行申請後，進入機房作現場維修。但某甲為了貪圖方便，在接獲需要維修的消息後，選擇以台哥大公司並不知情的 MMS 連線方式，透過手機帳號密碼連接台哥大公司內部的加值系統主機，之後再藉此建立與 TA 主機系統間的連線，以進行相關維護，免去向台哥大公司申請授權的麻煩。

**二、法院見解**

一審法院判決中提到：「……按無故**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 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金，刑法第 358 條定有明文。……其未徵得臺灣大哥大公司同意，逕利用該系統之漏洞以 MMS 模式連線進入 TA 主機，即已該當無故侵入他人電腦相關設備無誤。是核被告江金庭所為係犯刑法第 358 條之無故侵入他人電腦相關設備罪。」[81]亦即本案一審法院所認定該當的構成要件是「**利用電腦系統之漏洞**」入侵電腦及其相關設備。

而關於「**無故**」此一構成要件的論述，一審法院認為：「**所謂『無故』係指未經該電腦相關設備所有人、管理人明示或默示同意或不具有其他阻卻違法事由情形下**，而利用電腦系統之漏洞進入而言。而本案中，被告主觀上已知悉臺灣大哥大公司所同意遠端連線進入 TA 主機方式為 VPN 連線情形下，仍以臺灣大哥大公司所不知悉之 MMS 模式連線進入 TA 主機，故不論被告是否為維修 TA 主機等職務上目的進入，其未徵得臺灣大哥大公司同意，逕利用該系統之漏洞以 MMS 模

[81] 臺灣新北地方法院 99 年度易字第 2352 號判決。

式連線進入 TA 主機，即已該當無故侵入他人電腦相關設備無誤。」[82]

而二審法院則是這樣說明的：「按鑒於對無故入侵他人電腦之行為採刑事處罰已是**世界立法之趨勢**，且電腦系統遭惡意入侵後，**系統管理者須耗費大量之時間人力檢查**，始能確保電腦系統之安全性，此種行為之危害性應已達科以刑事責任之程度，為保護電腦系統之安全性而增訂刑法第 358 條之入侵他人電腦或其相關設備罪。次按**所謂「無故」，係指無正當理由之謂。而理由是否正當，應依吾人日常生活經驗法則，由客觀事實資為判斷，並應符合立法旨趣及社會演進之實狀**（最高法院 98 年度台上字第 5053 號判決參照）……堪認被告為解決吳捷建置系統時所生之問題，及回覆胡天從郵件所提之疑問，認有進入 TA 主機查看必要時，並非無進入該主機之方式，其捨台灣大哥大公司與 NSN 公司約定之途逕，逕以台灣大哥大公司所不知之 MMS 模式進入，致使台灣大哥大公司須耗費大量之時間人力始能查明。核被告以 MMS 模式進入，乃係怠為台灣大哥大公司規範之繁複申請程序，為圖一己便利而為，難謂其以該方式進入係有無正當理由。」[83]仍論以無故侵入他人電腦即相關設備罪，惟就罪數部分與一審見解不同，而撤銷改判。

## 三、判決簡評與討論

本案值得討論者有二點。首先，被告某甲在一次的連線行為中，究竟該當了幾個無故入侵電腦及其相關設備罪？其次，法院對於被告認為其並非「無故」的抗辯，又是如何論述？

從法院認定的事實中，我們可以簡單的整理出被告一次連線行為的路徑，是透過手機進行 MMS 連線，連接到台哥大公司加值系統的主機上，再透過內部網路連線到 TA 主機，輸入 TA 主機的帳號密碼後進入 TA 主機進行工作。法院在本案中認定的入侵行為，乃著眼於透過 MMS 連線到加值主機後，能在台哥大公司不知情的情況下連結到 TA 主機，亦即法院認為這種連線方式係屬**利用電腦系統的漏洞**（漏洞在照理說 MMS 連線就算能夠連到加值主機上，也不應該能夠從加值主機再

[82] 同前註。
[83] 臺灣高等法院 100 年度上易字第 2136 號判決。

連接到台哥大公司內部的任何其他主機）。本文對於法院此種認定，頗為贊同。按一般而言，若某機關擁有多台伺服器對外提供服務，使用者在連線到其中某台伺服器後，應無法接著由內部網路的連結存取其他伺服器，特別是部分伺服器可能僅提供機關內部私人網域服務，一般而言網路管理者對此多設下相關保全措施避免此種情況發生。換言之，台哥大對外提供服務的加值系統，與僅對內提供服務的 TA 主機間的連線，確實存在相關漏洞使被告某甲得以利用。

然而，我們需要思考的是，某甲在**未得到台哥大公司同意**的前提下，**輸入職務上使用的 TA 主機帳號密碼**，是否也構成了「無故輸入他人帳號密碼」的入侵行為？而進一步要問的問題則是，當某甲透過 MMS 連線到加值主機後，能夠存取台哥大公司內部網路上的任何主機時，是否在預備與 TA 主機建立連線（也就是與 TA 主機建立連線前的認證畫面，即輸入帳號密碼之前）就已經完成了一次的入侵行為？

當然，就犯罪行為的判定上，因為某甲最終的目的是要進入 TA 主機進行作業，前階段的各次（假若確實成立）入侵只是最終一次入侵的手段而已。但這也提醒了吾人一個問題，那就是入侵行為的判斷時點與既遂與否的依據為何？連續的跳板式入侵又應該如何評價？最大的問題是，因為構成要件已經設限了三種類型的手法，是否導致實務在入侵行為判斷上的困難與侷限？

本文認為，事實上本案就是典型**無權入侵**的類型。從本案中，吾人可以發現立法者所謂開放性漏洞的手段限制，拿來作為輔助判斷是否構成入侵行為的參考固然可行，但實際上真正應處罰的行為，卻仍是行為人未獲得授權而進入電腦的入侵行為，而與到底有沒有輸入帳號密碼、有沒有利用漏洞無關。在設計了前開手法限制後，只是造成了法院必須把原本是拿來幫助判斷是否算是入侵電腦的因素作構成要件的論述與檢驗而已，但是就有無此必要、是否造成判斷上面的僵化等問題，本文認為應不無影響。

其次，則是法院關於無故的見解有所不同。從前開一、二審法院的論述可以

發現，一審法院對於「無故」的認定，實際上著重於「無權進入」；而二審法院則引述了第 358 條的立法意旨，輔以過去實務建立對於「無正當理由」的相關見解去進行判斷。[84]吾人可以由此推論，一審法院之所以將無故的論述集中於無權進入的方向，主要的原因是本案的被告某甲所為並非立法者心目中**典型的惡意駭客入侵**行為，而是**未獲得授權的取巧進入行為**（但是所作的事情"似乎"又是正當目的），致使法院需以「無權進入」為軸去解釋被告的「無故」進入行為，而顯得似乎有些離題。相較之下，二審法院就無故的解釋較為妥適，透過被告確實有其他合法途徑而不為的論說，將被告確實無正當理由侵入的情況說明清楚。本文以為，二審法院的論述強度較為薄弱處，係引用立法理由試圖強化其對「無故」見解的說服力，先不論立法理由所謂「電腦系統遭惡意入侵後，系統管理者須耗費大量之時間人力檢查，始能確保電腦系統之安全性」云云是否真有足夠的說服強度，此一說法無疑將犯罪所造成的結果與客觀上的「無故」作牽強連結，實有不妥而畫蛇添足之嫌。

### （四）修法建議

第 358 條入侵電腦或其相關設備罪部分，其受害客體主要為電腦系統（及其相關設備）。首先應處理者，係「入侵」概念的釐清。論者有認為本條之入侵，與刑法第 306 條侵入住宅罪之「侵入」乃完全不同的法觀念，主要差異在於「侵入」住宅屬於不作為犯的典型，只要經命退去而不退去，其不作為可該當 306 條之罪。[85]然亦有論者似認為，入侵與侵入所指涉之行為，均與人類使用空間的排他期待有關，屬於安心領域的保護，差異僅在於兩罪係保護不同類型空間的信賴與期待而已。[86]

---

[84] 最高法院 98 年度台上字第 5053 號判決提到：「其所謂「無故」，係指無正當理由之謂。而理由是否正當，應依吾人日常生活經驗法則，由客觀事實上資為判斷，並應符合立法旨趣及社會演進之實狀。立法者將『無故』置入犯罪構成要件，顯係在評價構成要件之階段即進行判斷，而排除有正當理由之『妨害秘密』行為。」

[85] 張紹斌，前揭註 62，頁 87-88。

[86] 李聖傑，前揭註 38，頁 77-79。

從比較法的角度來看，美國法上相類似條文係以無權使用（access，或譯為存取）作構成要件，學理上則發展出「虛擬進入說」與「下達指令說」來對該入侵行為作解釋。[87]所謂虛擬進入說，解釋上類似於以現實空間概念作類比，一旦無權進入了該空間時，即構成入侵行為；反之，下達指令說則不作空間的類比，直接以行為人是否對電腦下達指令作為判斷入侵與否的依據。[88]這兩種不同學說在多數情況下判斷結果別無二致，但在某些情況下結果並不相同。舉例而言，若行為人以測試帳號密碼方式試圖進入某台電腦而未能得手時，按虛擬進入說因為尚未「進入」該電腦空間，並不該當入侵電腦罪；反之，若按照下達指令說，因為輸入帳號密碼並獲得電腦的帳號密碼回應，此時指令已經下達，故該當入侵行為。[89]

本文認為，「入侵」的概念，解釋上仍應以空間作類比較為妥當，也就是說「入侵」電腦罪與「侵入」住宅罪在空間法益的破壞上，其實是相當類似的。美國法上較為寬鬆的指令下達說，本文以為其目的主要係為處理未遂犯問題。從前開例子當中可以發現，事實上該行為若以我國現行法做評價時，僅算得上第 358 條的未遂犯而已，現行法並不處罰。[90]的確，若從資訊安全的保護來看，或許此種「試圖入侵」的行為已經足使人民感到不安，但若就行為本身的嚴重性去分析，似乎並不能將未能接觸電腦內部資訊的未遂犯，與已經成功侵入的既遂犯相提並論。倘若認為此種入侵行為的嘗試具有相當危險，應訂立未遂犯的處罰條文，較為合乎我國法的體系，而不至於混淆既遂與未遂間的分際。[91]

其次，應刪除前段以犯罪手法限制適用範圍的規範漏洞，而可從客觀不法構成要件去限縮適用範圍。透過修正客觀不法構成要件為「未獲授權及踰越權限」，

---

87 蔡榮耕，前揭註 38，頁 115-117。

88 蔡榮耕，前揭註 38，頁 115-116。論者認為採用虛擬進入說來解釋入侵，可能造成舉證困難的結果，特別是在相關紀錄檔均被刪除的情況下尤其如此。惟本文所疑惑者，是一旦相關紀錄檔均遭到刪除，不論採取虛擬進入說或下達指令說，舉證上都會遭遇相當的困難，似乎不是單純採用不同學說解釋就能解決此一問題。在資訊的世界中，倘若相關紀錄檔都遭刪除，此時要證明曾經「進入」該電腦，和證明曾經對該電腦「下達指令」，就困難度而言實無二致。

89 蔡榮耕，前揭註 38，頁 116-117。

90 蔡榮耕，前揭註 38，頁 126-129。

91 類似看法，參蔡榮耕，前揭註 38，頁 129。

事實上能夠囊括各種駭客入侵到公司員工無權（或越權）進入資料庫等行為，也無須判斷是否有設定密碼等安全設備。[92]透過此種方式，當能重構本條為不處罰過廣且補足現況漏洞的條文，也不至於再次發生如同臺灣高等法院 101 年度上訴字第 2540 號判決中，行為人取巧的利用作業系統尚未自動上鎖的機會，進行實質上的入侵電腦行為，卻無法可罰的規範漏洞。

至於論者主張應仿照日本設立「助長不法連線罪」之論點，本文則抱持保留態度，其主要原因係以資訊安全角度考量，資訊犯罪中危害最甚者，往往係熟知資訊技術者，縱然欠缺他人提供帳號密碼幫助仍能犯罪，對於減少相關犯罪幫助不大；若僅是隨意的提供帳號密碼供他人使用，考量到刑法仍有幫助犯可對後續犯罪者及幫助者進行追訴，以現況觀之，似尚無單獨將實質上屬幫助犯之行為正犯化之必要性。[93]也就是說，本文認為若行為人在網路上任意散播其帳號密碼，而為他人犯罪之用時，在該他人該當犯罪行為之正犯時，以幫助犯評價此行為人即為已足，尚無特別為此散播行為建立正犯化規範之必要性。

## 第二節　第 359 條

刑法第 359 條為無故取得、刪除或變更電磁紀錄罪：「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。」修法理由謂：「二、電腦已成為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，鑒於世界先進國家立法例對於此種行為亦有處罰之規定，爰增訂本條。」[94]

本條在學說上最招致批評者，係本條立法時將三種不同的行為態樣共用同一

[92] 柯耀程，前揭註 58，頁 123-124、127；蔡榮耕，前揭註 38，頁 127-128。

[93] 不同意見，可參王銘勇，前揭註 75，頁 30。論者以為，放任網路流竄他人帳號密碼，因無正犯存在，而無由成立幫助犯，但仍可能助長後續犯罪。惟本文以為，在我國民眾資訊安全概念不足的情況下，暫且保守的在後續犯罪產生之後，再以幫助犯論罪，或較符合我國民情，而不至於讓民眾產生過度陷人入罪之疑慮。

[94] 前揭註 29。

條文，雖屬較為精簡的條文設計方式，卻並未考慮此三種行為所造成的結果並不相似，損害程度似乎也有輕重之分，保護法益也似有所不同，而有構成要件與對應刑度設計不當之嫌。

本條為結果犯，但關於損害結果之認定與判斷，不但學界認為有所困難與疑惑，實務上也產生對於損害結果認定標準不同的分歧。本文所節錄之判決包括（二）判決實證：最高法院 97 年度台上字第 3817 號判決、（三）判決實證：最高法院 98 年度台上字第 3015 號判決、（四）判決實證：最高法院 100 年度台上字第 52 號判決、（五）判決實證：最高法院 100 年度台上字第 6468 號判決等，雖案情各稍有不同，且非主要爭點亦有所出入，但共通的主要爭點均與**損害結果之認定標準**相關。

本文整理實務相關判決，發現實務上對於損害認訂的標準大抵可以分為三大類：第一大類，係對損害認定最為寬鬆的見解，放寬第 359 條的損害認定標準，認為只要到達足生損害之程度即為已足，而無須有實際損害的結果。第二大類，則是嚴格遵守構成要件認定損害結果，認為理由和事實都要能夠清楚指出損害為何，而部分判決在損害的認定標準甚至有偏向必須有實質的經濟損害之傾向。第三大類係較為折衷的見解，認為本條係以保護電子化財產秩序為目的，其所謂具體之損害並不僅指經濟上損害，尚包括了其他類型的損害。詳細之討論將於本節第五段的判決評析處作進一步說明。

## （一）學界評論

第 359 條無故取得、刪除或變更電磁紀錄罪，在學說上主要為論者所詬病之處，係將三種不同的行為類型——「取得」、「變更」和「刪除」置於同罪，造成適用上困難。[95]論者認為，若與類似行為相比，取得和刪除的行為，與個人法益

[95] 柯耀程，前揭註 58，頁 127；廖宗聖、鄭心翰，前揭註 75，頁 79-80。須特別說明者，係於廖宗聖、鄭心翰所著「從網路犯罪公約談我國妨害電腦使用罪章的修訂」一文中，認為本罪之行為態樣有二，而將「刪除或變更」合併視作其中一種類型，與前段的「取得」作比較與區隔，本文認為此種分類方式應有誤會。

本文以為，刑法以「或」連結之前後文，本即屬不同類型，方以或字作區隔，從一般語言的

對於財產、隱私等保護的類型較為類似；但變更之行為，在我國通說將文書真實性定性為社會法益的前提下，似乎較為接近保障電磁紀錄真實性的社會法益之罪。[96]不過，亦有學者認為，從本章規範目的「電腦與網路安全」之角度出發，第 359 條的三種行為態樣，乃係用以描述資訊之私密性、完整性與可使用性在未獲授權（或超出授權範圍）下被侵害的不同攻擊方式，而非用以補充傳統刑法（在虛擬空間中）的處罰漏洞，而認為此種法條類比並不恰當。[97]

事實上，在資訊領域中取得電磁紀錄所牽涉的問題，多與電磁紀錄具可複製性有關，在被不法取得後，原先電磁紀錄並不因此受減損或消滅，性質上與傳統的動產有益，故取得行為所牽涉的保護法益究屬財產抑或僅係隱私等問題，其定性仍須仰賴個案判斷。[98]變更與刪除行為，若以技術層面角度觀察，部分變更行為可能與刪除重疊，則此時變更行為（變更電磁紀錄中人類可讀取瞭解的內容？抑或是變更電磁紀錄的邏輯紀錄？）和刪除行為的分界與定義，是仍待立法者解釋的。[99]

另外，因為「致生損害於公眾或他人」屬於結果犯要件，搭配前段對電磁紀錄所為之行為（取得、變更或刪除）結果，造成雙結果犯的奇妙結構，此時若將本罪往保護社會法益的方向解讀，則對公眾的損害舉證可能產生困難，應將「致生」改為「足生」，將之作為補強行為侵害的確認性佐證，應可有效解決目前適

---

用法去推論亦可得出此一結果。更進一步言之，若以此兩種行為態樣對電磁紀錄所發生之效果觀之，「刪除」性質上類似毀損或致令電磁紀錄無法使用（立法者並未說明應該「刪除」到怎樣地步才算得上是立法者所認為的「刪除」。究竟是要到低階格式化的程度才算刪除？或者一般刪除檔案索引檔的程度就算是刪除？此爭議非本處主要爭點，暫且撇開不談）。而「變更」可能造成的結果中，雖有部分與刪除行為類似，例如變更檔案內部編碼為亂碼使該檔案無法正常讀取；但卻也有單純的變更電磁紀錄內容，例如修改文字檔內文等。由此觀之，刪除與變更實乃兩種不同的行為，而不能合併成單一行為態樣討論，故本文以為論者之陳述應有誤會。

[96] 李茂生，前揭註 79，頁 252-256。此處之討論仍回歸到前面所論及之法益問題，可見法益問題顯屬於本章亟待解決的難題。關於刑度的問題，舉例而言，第 359 條無故取得、刪除或變更電磁紀錄罪中，包含了三種不同的行為。其中刪除電磁紀錄罪的行為，假設該電磁紀錄符合準文書之規定（刑法第 220 條第 2 項）時，行為人可能同時該當第 352 條毀損文書罪。縱然撇去法益爭議不提，採本章亦為保護個人法益之通說見解，第 359 條的刑度（五年以下）仍是遠重於第 352 條的三年以下。

[97] 參蔡蕙芳，前揭註 25，頁 66-67。

[98] 相關討論，可參見本文第二章第二節。

[99] 前揭註 95。

用混淆的困境。[100]實務上則因為此種雙結果犯的模糊性，最高法院因而作出本罪係結果犯之限縮見解，而需要就損害作證明，不能僅以損害之虞即該當本罪。[101]此舉固然避免過度擴張本罪適用範圍，但亦引起此種見解違背立法意旨，在資訊（特別是智慧財產和營業秘密）的排他控制力實際上已受損，但卻無法證明損害的情況下，因為損害舉證的困難導致無法以本罪相繩，顯然使得規範目的因而落空。[102]

換言之，本罪因為其結果犯的構成要件設計，若案件事實實以涉及社會法益層級時，對公眾的損害會因為較為抽象而舉證困難，造成判定上的困難。若嚴格認定實質損害時，對於許多接觸甚至只要得以接觸就可能造成電磁紀錄所有者侵害的案例而言，往往會因為缺乏實質上的經濟損害，而無從透過本條獲得保護。

## （二）判決個案分析：最高法院 97 年度台上字第 3817 號判決

### 一、判決事實、爭點與法院見解

本案事實略為：被告某甲與先前任職之 A 公司負責人不合而離職，自行設立與 A 公司營業內容相同之公司，並為達與 A 公司競爭客戶之目的，竟基於刪除 A 公司電腦紀錄之犯意，進入 A 公司所在之大樓辦公室內，無故刪除 A 公司所有二部電腦，內容紀錄有 A 公司之客戶資料、工廠資料、報價資料及 A 公司與客戶聯絡內容檔案等電磁紀錄，致生損害於 A 公司。

本案一審法院判決某甲有罪，處有期徒刑陸月，如易科罰金，以參佰元折算壹日。[103]告訴人認為判決過輕，請求檢察官上訴，二審法院認為：「惟查現今電腦儼然為使用者知識資料之寶庫，若資料將之除去，所造成之損害，經常難以回復，故九十二年六月二十五日公布增訂刑法，設有專章；被告丙○○前開犯行，原判決僅量處有期徒刑六月，並得易科罰金，顯然輕縱，尚有未洽。檢察官循告訴

[100] 柯耀程，前揭註 58，頁 127-128；蔡蕙芳，前揭註 25，頁 72。
[101] 林孟皇，「妨害電腦罪章的無故取得電磁紀錄──評最高法院一百年度台上字第三三七五號刑事判決」，月旦裁判時報，第 12 期，2011 年 12 月，頁 89-90。其餘相關判決解析，可參見本文以下判決實證與評析。
[102] 林孟皇，同前註，頁 90-91。關於資訊（或電磁紀錄）之控制力受損可能造成的損害與其特性、新舊法規範等討論，可詳參蔡蕙芳，前揭註 24，頁 109-120。
[103] 臺灣台北地方法院 93 年度訴字第 1106 號判決。

人之請求上訴意旨以原審量刑過輕，亦有理由。」[104]撤銷原審判決，改判有期徒刑七月。被告不服二審判決，上訴最高法院。[105]

被告認為：「……刑法第三百五十九條之無故刪除他人電腦之電磁紀錄罪，係以致生損害於公眾或他人為要件，而上訴人刪除之電腦檔案係 A 公司已經出貨完成之訂單，而該訂單或資料，依證人即 A 公司之人員某乙、某丙之證述，**均有另行歸（存）檔**，足見**上訴人之行為對於 A 公司並未產生損害**，原判決對上開證人所為之證述，未說明何以不足採，有理由不備之違法。……」

由被告上訴理由觀察，被告認為二審法院就被告所為如何致生損害乙節，以及被告於訴訟中所提出的「有備份故未造成損害」抗辯並未說明為何不採，而認為有理由不備之違法。也就是說，本案爭點就在於**損害認定的標準**。

觀察二審法院之論述，其主要著重於事實的認定，亦即該電磁紀錄確實遭到刪除、且確實為被告所為，對於被告之抗辯，二審法院僅簡單引述相關事實及證詞，並說明該電磁紀錄之重要性之後，便直接認定被告抗辯不可採而未多加說明：「由證人某乙、某丙之證詞可知，被刪除的資料係 A 公司與客戶之往返資料及產品照片，而貿易必須不斷的與客戶聯繫及處理客戶之回應，故與客戶往來之資料十分重要，一旦此類資料遭刪除，公司及缺乏與客戶聯絡之管道，即會造成客戶流失，故被告某甲辯稱遭刪除之資料，A 公司另外有存檔，對於 A 公司，並不會發生損害云云，委不足採。」

對此，三審法院認為：「……並就上訴人辯稱其刪除之 A 公司電腦檔案，係已出貨之紀錄，該公司均另有存檔，其行為不足致生損害於 A 公司等語，認不足採信，予以指駁；經核俱與卷內資料相符，原判決並無理由不備、理由矛盾之違法。」全盤支持二審法院的判決，並駁回被告上訴。

## 二、判決簡評與討論

[104] 臺灣高等法院 94 年度上訴字第 2803 號判決。

[105] 本案上訴理由實有三項主張，本文在此僅就與本文討論主題有關的主張進行討論，其餘程序論點、事實爭點等，因與本文主軸較為無關，未免離題故本文不多作說明。本文其餘判決實證作法亦同。

本案的主要爭點其實就是被告所主張的論點，亦即當被刪除的電磁紀錄有作相關備份時，是否就不足致生損害？也就是說，第 359 條無故刪除電磁紀錄罪的損害認定，究竟是採用何種標準？對於本判決的評析暫且就此打住，以下將以爭點類似的判決作比較後，再進行分析與評論。

## （三）判決個案分析：最高法院 98 年度台上字第 3015 號判決[106]

### 一、判決事實、爭點與法院見解

本案事實略謂：被告某甲先前受僱於亮泰企業股份有限公司（下稱：亮泰公司），擔任業務副總經理職務。亮泰公司給予每位公司員工一個電子信箱帳號及密碼，做為業務上與客戶通訊使用。員工之電子信箱帳號及密碼，除負責網路系統之管理人員某乙統一管理外，均由每位員工自行保管，即使負責人或各階層主管均無從取得其個人以外之屬於員工之個人信箱帳號及密碼。但該公司為監控員工之電子郵件，**對於所有傳送至公司員工電子信箱內之郵件，即自動備份至負責人某丙辦公室內的獨立備用電腦**，負責人某丙得藉由備份電腦讀取員工之電子郵件。另業務部門之員工電子郵件，亦設有自動備份至 SALESBACK-UP 信箱內，由擔任業務部門之副總經理負責監看。某甲以不詳方法，閱覽到該公司負責網路系統管理人員某乙所保管之登載亮泰公司全體員工電子信箱帳號及密碼之筆記本，並私自抄下工程部副理某丁（帳號 kevin@ltw-tech.com）、工部副總經理某戊（帳號 calvin @ltw-tec h.com）、總經理助理某己（mandy@ltw-tech. com）、業務副理某庚（帳號 joanne@ltw-tech.com）（以上所有信箱，下合稱前開員工信箱），及負責人某丙（帳號 peter 及 peter1@ltw-tech. com）之電子信箱帳號及密碼資料。旋即於非工作時間，在其住處利用其所有之電腦及網路設備，使用以其兄名義申請之 ADSL 線路（IP 位址為 218.166.74.17 ），**輸入**亮泰公司給予該公司之負責人某丙（帳號 peter 及 peter1@ltw- tech. com），及前開員工信箱之**帳號密碼**，透過網際

[106] 歷審判決依序為：臺灣台北地方法院 94 年度訴字第 1823 號判決、臺灣高等法院 95 年度上訴字第 2674 號判決、最高法院 98 年度台上字第 3015 號判決、臺灣高等法院 98 年度上更（一）字第 331 號判決。

網路連接入侵亮泰公司之電子郵件伺服器（網域名稱為：ltw-tech.com），進入上開人員之電子郵件信箱**讀取文件**。因該公司之 out-look 設有信件讀取即自動刪除之功能，致使上開信箱帳號之使用人無法收取上開期日客戶寄進來之郵件，某丙即通知某乙進行調查，始查知上情。

一審法院僅認定被告涉犯**第 358 條**無故輸入他人帳號密碼入侵電腦罪事證明確，判決被告有罪，處有期刑陸月，如易科罰金，以參佰元折算壹日。但就檢方認為被告尚涉犯第 315 條妨害書信秘密罪、第 359 條無故取得他人電磁紀錄罪部分，一審法院認定並不該當。就第 359 條無故取得他人電磁紀錄罪部分，一審法院認為：「本條犯罪之成立，除須無故而取得、刪除、變更他人電腦或相關設備之電磁紀錄外，並須其行為已對公眾或他人產生具體之損害為必要。本件被告無故輸入某丙等人之帳號、密碼讀取某丙等人之電子郵件，已如前述，但被告之行為，是否已對亮泰公司致生具體之損害非無疑問。公訴意旨未具體指明被告之無故讀取某丙等人電子郵件行為，**究對亮泰公司產生何種具體損害之結果**，且亦**未提出任何證據證明亮泰公司受有具體損害**，則自亦與上開規定之構成要件有間。」[107]除強調第 359 條屬於結果犯，以具體損害結果為必要外，亦認為檢方就此節並未充分舉證，判處被告並不該當第 359 條之罪。由此節觀之，**本案之爭點與前一案例相同，亦是關於損害認定飄準的問題**。

但二審法院卻持不同看法，認為：「按『無故取得、刪除或變更他人電腦或其他相關設備之電磁紀錄，致生損害於公眾或他人者』，構成刑法第 359 條之罪。被告未經授權自告訴人亮泰公司之伺服器以下載告訴人陳章南等人之電子郵件之電磁紀錄，所為核屬無故取得他人電腦之電磁紀錄，又本條犯罪之成立以對公眾或他人產生具體之損害為必要，**然本項法益在於維持電子化財產秩序，並不以實際經濟上之損害為限（此有立法理由可參）**，而本案被告取得他人之電子郵件電磁記錄後，因告訴人亮泰公司之 out-look 設有信件讀取即自動刪除之功能，導致上

[107] 臺灣台北地方法院 94 年度訴字第 1823 號判決。

開信箱帳號之使用人某丙等無法收取附表所示之郵件……據此，就使用人未能正常收取客戶之電子信件，**亮泰公司亦未能即時處理客戶之來信，影響公司正常運作而言，自已生損害於該等信箱帳號之使用人及告訴人亮泰公司**。」[108]撤銷一審判決，改判被告無故取得他人電腦之電磁紀錄，處有期徒刑陸月，如易科罰金，以參佰元折算壹日。

本案上訴到三審後，最高法院認為：「刑法第三百五十九條：『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……』，所規範之行為包括『取得』、『刪除』及『變更』電磁紀錄；必行為人無故『取得』、『刪除』及『變更』他人電腦或其相關設備中之電磁紀錄，且**因此對公眾或他人產生具體之損害**，始足當之。原判決以上訴人牽連犯刑法第三百五十八條無故侵入他人電腦罪及刑法第三百五十九條無故取得他人電腦之電磁紀錄罪，從較重之刑法第三百五十九條規定論處；但事實欄僅記載：上訴人私自抄錄亮泰企業股份有限公司（下稱亮泰公司）給予該公司負責人某丙及員工……（以下合稱「某丙等五人」）之電子郵件信箱帳號及密碼，使用上訴人之兄名義申請之ＡＤＳＬ線路，連續於原判決附表所載時間，無故輸入某丙等五人之電子郵件信箱帳號及密碼，透過網際網路連接亮泰公司之電子郵件伺服器，進入各該信箱以下載郵件……致生損害於亮泰公司及各該信箱之使用人（即某丙等五人）等情。對於上訴人究係取得陳章南等五人之電子郵件信箱內**何種電磁紀錄**？倘有取得電磁紀錄，對亮泰公司及陳章南等五人**造成如何具體之損害結果**？均未具體認定並記載，致事實尚欠明確，本院無從就原判決適用法則是否適當為判斷；非無可議。」[109]指摘二審法院就此節事實調查不夠明確，因而撤銷判決發回更審。本案更審法院最後以本罪係告訴乃論之罪，而某丙等五人並未就第 359 條部分提出告訴，就第 359 條部分做出不受理判決，事證明確且經提出告訴的第 358 條則

[108] 臺灣高等法院 95 年度上訴字第 2674 號判決。
[109] 最高法院 98 年度台上字第 3015 號判決。

判決有罪。[110]

**二、判決簡評與討論**

撇去本案因為不合告訴乃論之程式的部分不談，若從實體面觀察，本案二審的論述（亮泰公司亦未能即時處理客戶之來信，影響公司正常運作而言，自己生損害於該等信箱帳號之使用人及告訴人亮泰公司），是否真如三審法院所指摘「未認定具體損害結果」？若是，則所謂認定具體損害結果又該「具體」到何種程度？本文在此仍先不多作討論，將討論之篇幅留待本章第二節第五段一併說明。

## （四）判決個案分析：最高法院 100 年度台上字第 52 號判決[111]

**一、判決事實與爭點**

本案事實略謂：被告某甲任職於某乙所開設民間公證人事務所，擔任公證專員之職，試用期間屆滿後，因某甲工作期間表現欠佳，經協調處理後，雙方同意延長試用期，再行評估是否繼續聘僱；某甲於任職之初，已與某乙簽訂保密協定，明定該事務所內**所有與公證事務相關之檔案、文件、電磁紀錄等，均在保密之範圍內，不得任意取得或外流**。某甲於即將離職之前一日在事務所內，利用事務所分配使用之電腦，將儲存於該事務所區○○路內、僅限於該事務所內公務使用之檔案「四月公證案號表.xls」、「如何辦理夫妻財產制契約登記.doc 」 、「服務項目格式─空白.doc 」 、「辦理委託公證所須攜帶的證件.doc」等 4 項電磁紀錄，先以壓縮程式壓縮為檔案大小僅約 32KB 之「新資料夾 3.rar 」檔案後，再利用該事務所公證服務部帳號，透過電子郵件收發管理軟體 Outlook Express，將「新資料夾 3.rar 」壓縮檔寄至其個人使用之電子郵件信箱內，以此方式無故取得某乙電腦內之前述 4 項電磁紀錄。後為某乙所發覺後，提出告訴。

**本案主要的爭點係被告主張前開四項電磁紀錄，均屬於可從公開網站搜尋取**

[110] 臺灣高等法院 98 年度上更（一）字第 331 號判決。

[111] 歷審判決依序為：臺灣新北地方法院 95 年度易字第 88 號判決、臺灣高等法院 96 年度上訴字第 1142 號判決、最高法院 96 年度台上字第 6981 號判決、臺灣高等法院 96 年度上更（一）字第 949 號判決、最高法院 100 年度台上字第 52 號判決。

**得，且與某乙事務所保密事務無關，並未造成某乙任何的損害，與刑法第 359 條無故取得他人電磁紀錄罪構成要件不符。**

**二、法院見解**

一審法院就此節表示：「惟查，無論前述『四月公證案號表.xls 』等電子紀錄，是否確均可於其他公開網站上尋得，或是否確均與證人某乙業務上之當事人機密無關，上開電磁紀錄既均存在於證人某乙之事務所內部電腦系統內，並僅供事務所內部使用，自均屬證人某乙之電磁紀錄無疑，無論被告係基於何等動機及目的而取得上開電磁紀錄，或上開電磁紀錄對於被告究具有何等之用途，均無影響於被告無故取得他人電磁紀錄行為之成立，而被告於任職於證人某乙事務所之初所簽訂之保密協定，亦特將**『聘用方之業務處理內容、資料檔案』均列入保密之範圍**內，顯見證人丁○○對於其事務所內部之所有檔案資料，均有嚴格之保密管理機制，被告無故取得上開電磁紀錄，顯然**足生損害**於證人某乙對於其事務所內**檔案、文件、電磁紀錄管理之正確性及機密性**；從而，被告上開所辯，亦無非卸責之詞，不足採信。」[112]因而判處被告某甲有期徒刑肆月，如易科罰金，以參佰元折算壹日。二審法院亦贊同一審法院見解，駁回被告之上訴。[113]

然而，本案上訴至最高法院後，卻出現了逆轉。最高法院認為：「按刑法第三百五十九條所謂『致生損害於公眾或他人』，須以行為人無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，以**對公眾或他人產生具體之損害**為必要，**如僅有發生損害之虞，即與犯罪構成要件不符**。原判決認定上訴人之行為『足生損害於詹孟龍對於其事務所內檔案、文件、電磁紀錄管理之正確性及機密性』等語，僅記載上訴人之行為『足生損害』，已與本罪之犯罪構成要件不符；且上訴人於原審抗辯：大多數檔案均可在公開網站上尋得，無關詹孟龍業務上之當事人機密，並未造成詹孟龍任何損害云云。原判決僅以該等資料均係屬雙方簽訂保密協定之範圍，而證人詹孟龍對於其事務所內部之資料均有嚴格之保密管理機制，

[112] 臺灣新北地方法院 95 年度易字第 88 號判決。
[113] 臺灣高等法院 96 年度上訴字第 1142 號判決。

被告無故取得上開電磁紀錄，顯然足生損害於證人詹孟龍對於其事務所內檔案、文件、電磁紀錄管理之正確性及機密性，而認被告之辯解不足採信，並未敘明被告無故取得上開電磁紀錄，對於詹孟龍有產生何具體之損害，即有判決不備理由之違法。」[114]將本案發回高等法院更審。

更審法院認同最高法院見解，認為：「告訴人指稱被告寄送的『四月公證案號表』、『如何辦理夫妻財產制契約登記』、『服務項目格式空白』、『辦理委託公證所須攜帶的證件』等 4 項電磁紀錄檔案（偵卷 74-95），其內容或為法律問題的 Q&A ，或為辦理公証程序法定要件的說明，且於告訴人網頁或台灣台北地方法院網站上均可查得，顯屬公開的資訊，於**客觀上已難認屬告訴人營業上的秘密**。再依告訴人與被告所簽訂的保密協定內容，被告雖對於『服務期間所知悉一切公證上業務內容，有絕對保密義務。』但僅限定被告『不得將客戶資料與公證書攜出事務所』（偵卷 16）；而前述 4 項電磁紀錄並不屬於協定範圍內的『客戶資料與公證書』，縱使被告確有將前述電磁紀錄以電子郵件方式攜出事務所，也不能認定違反保密協定。**則上述 4 項電磁紀錄既非告訴人營業上秘密，且縱然攜出也不違反保密協定，即不足以認定對於告訴人已致生損害。**」[115]也就是說，更審法院以前開電磁紀錄是否屬於保密協定所規範的營業上秘密，作為判斷是否致生損害的依據，而認為被告複製該電磁紀錄的行為因為與營業上秘密無關，亦不違反保密協定，判決被告無罪。

檢方不服更審判決，認為不論前開四項檔案是否可從公開管道取得，或是與該事務所營業秘密有無關聯，均不妨礙被告該當無故取得他人電磁紀錄之罪行。況且該保密協定中將「聘用方之業務處理內容、資料檔案」列入保密範圍，被告無故取得在保密範圍內的資料檔案，「**顯然足生損害於某乙對於其事務所內檔案、文件、電磁紀錄管理之正確性及機密性**」。而且被告轉寄前開檔案之行為，顯然侵害了某乙對於前開檔案事實上之管領支配力，故「原判決似認刑法第三百五十

[114] 最高法院 96 年度台上字第 6981 號判決。
[115] 臺灣高等法院 96 年度上更（一）字第 949 號判決。

九條之**保護客體限於『營業秘密』或『保密協定』範圍內之電磁紀錄**，有適用刑法第三百五十九條不當之違背法令。」[116]對於檢方之主張，最高法院維持其前審見解，重申本罪屬於結果犯，需以致生具體損害為必要，若僅係有損害之虞尚不足以構成本罪，維持更審無罪判決，駁回檢方上訴。[117]

**三、判決簡評與討論**

從本案中可以發現，**法院對於構成要件中具體損害結果的要求甚為嚴格，似以實質上造成經濟或其他顯而易見的損失為標準**，而不採檢方主張的有損害之虞，認定該見解偏離構成要件解釋範圍。但值得吾人深思的是，本案中固然被告所取得的檔案多屬其他合法途徑亦能取得的檔案，從財產損失的角度來說，固然對於告訴人方不生影響，但若從資訊安全的角度來說，檢方認為被告之行為有害及檔案、文件、電磁紀錄管理之正確性及機密性之虞實不無道理，則此時是否應回頭檢視本條的立法目的所欲保障的標的為何？用嚴格的結果犯去規範是否可能是一種立法疏失？

## （五）判決個案分析：最高法院 100 年度台上字第 6468 號判決[118]

**一、判決事實與爭點**[119]

本案事實略謂：被告某甲，設立汶皇國際貿易股份有限公司（下稱汶皇公司）並自任負責人，另受僱於朝能興業有限公司（下稱朝能公司），擔任國外業務專員一職，並使用亦於同址辦公之關係企業即保證責任屏東縣長慶果菜運銷合作社（下稱長慶合作社）配置之電腦，從事規劃、設計參展所需文件，及以電子郵件聯繫國外客戶等農產品推展、外銷工作，後以另有生涯規劃為由自行申請離職。

---

[116] 最高法院 100 年度台上字第 52 號判決。

[117] 其論述內容與用語與最高法院 96 年度台上字第 6981 號判決、臺灣高等法院 96 年度上更(一)字第 949 號判決一字不差，相當於該二判決文字敘述之組合而已，並無不同的論述方式與見解，在此便不重複引述其文字。

[118] 本案歷審判決為：臺灣高雄地方法院 98 年度訴字第 988 號判決、臺灣高等法院高雄分院 99 年度上訴字第 1139 號判決、最高法院 100 年度台上字第 6468 號判決、臺灣高等法院高雄分院 100 年度上更（一）字第 121 號判決。

[119] 另可參見林志潔、古旻書，「無故刪除他人電腦之電磁紀錄罪之實害結果應如何判斷？／最高院 100 台上 6468 判決」，台灣法學雜誌，第 204 期，2012 年 7 月，頁 248-252。

某甲利用返回辦公室辦理職務交接之機會，於較少員工走動之午休時段，無故擅予刪除長慶合作社電腦內儲存於「我的文件」夾中「韓國首爾國際食品展」、「莫斯科農產品展示會」電磁紀錄（內容為參展相關之文字、圖片檔案），及 outlook 系統中以 export@fruitseafood.com.tw 電郵地址與國外客戶往來之全數電子郵件電磁紀錄（下合稱前開電磁紀錄）。

本案主要爭點即被告刪除前開電磁紀錄後，**嗣後歸還備份檔**，是否仍造成被害人之損害，而該當刑法第 359 條之罪？

**二、法院見解**

一審法院認定被告某甲之行為，「**使接手國外農產品推銷工作之長慶合作社員工某乙，不能立刻查考、追蹤長慶合作社之參展成效，復無法即時與國外固有客戶聯繫，而致生損害長慶合作社**。」[120]雖被告提出誤刪抗辯，且事後已經將刪除的檔案備份交還長慶合作社，故長慶合作社未受損害等主張，但一審法院針對該電磁紀錄內容之重要性及貿易聯繫時效之急迫性等情作說明，認為：「經被告刪除之電磁紀錄，包括原存於『我的文件』夾中『韓國首爾國際食品展』、『莫斯科農產品展示會』等文字、圖片檔案，及 outlook 中以 export@fruitseafood.com.tw 電郵地址與國外客戶往來之全數電子郵件電磁紀錄，已如前述。而廠商參與政府機構主辦之國外展示會，要非僅意在取得主辦單位之參展補助，接觸進而開發更多外籍客戶，方為主要之目的，然該主要目的之達成，非賴詳予紀錄完整之參展經過及所接觸外籍客戶詳細聯繫方式，並妥為留存，俾日後持續查考、追蹤不可；又使用電子郵件等現代通訊方式，取代買賣雙方互派業務員會面議定交易內容，本屬更為便捷、有效率之方式，尤在跨國性之貿易中，因買賣雙方相隔甚遠，對於現代通訊方式之依賴，往往更甚於國內貿易，**苟逸失交易對象之電郵地址等通訊方式，非僅無法該固有客戶進行立即聯繫，甚恐有致雙方從此失聯之虞**；再者，現今商業競爭頻繁且變化迅速，可能**因一時怠於或疏於與客戶進行聯繫，即蒙受**

[120] 臺灣高雄地方法院 98 年度訴字第 988 號判決。

**商機損失，或至少有蒙受損失之虞**，俱為從事國外貿易之人所週知之事，被告對此自無由諉為不知，其徒以事後曾將手邊留存之前開電磁紀錄備分提供予後手某乙一節，遽予推論長慶合作社並無損害，顯無足取。末參諸被告就自己持有之前開電磁紀錄備分留而不刪，卻利用因辦理職務交接而得返回辦公室之機會，在毫無正當理由之情況下，執意進行無助職務交接之擅刪電磁紀錄舉動，更堪認被告非僅明知，並有意經由刪除電磁紀錄之舉，使接手其職務之某乙，**不能立刻查考、追蹤長慶合作社之參展成效，且無法即時與國外固有客戶聯繫，顯已致生損害於長慶合作社甚明**。」一審法院雖不採信交還備份抗辯，惟仍以被告某甲對於客觀行為（有刪除電磁紀錄）坦承，且在提出告訴前確實已經交還備份等情，最終僅判決被告處有期徒刑陸月，如易科罰金，以新臺幣壹仟元折算壹日。

二審就此節支持一審法院見解，駁回被告上訴。[121]但最高法院卻有不同看法，認為：「刑法第三百五十九條所規定『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』罪，屬於結果犯，必須該行為已致生損害於公眾或他人之結果，始構成本罪。否則，縱有無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄行為，**倘未致生損害於公眾或他人之結果者，因該罪無處罰未遂犯明文，自不成立該罪**。換言之，刑法第三百五十九條之罪，以『致生損害』於公眾或他人為構成要件，屬於結果犯，此與僅以『足以生損害』於公眾或他人為構成要件者，例如刑法第二百十條之偽造私文書罪，以有足生損害於公眾或他人之危險，即行成立者，迥然不同。**是此項『致生損害於公眾或他人』之構成犯罪事實，不僅事實欄應明白認定，且須於理由內說明其所憑之依據，方足資以論罪科刑。**」[122]認為按照前審卷證，若被告確實歸還前開電磁紀錄備份，則「倘若無訛，依其情形，自無從證明上訴人之行為，已『致生損害』於長慶合作社之結果。原判決理由欄未予說明如何認定上訴人上揭之行為，已致生損害於

[121] 臺灣高等法院高雄分院 99 年度上訴字第 1139 號判決。本案被告另涉犯偽造文書等罪名，二審撤銷一審判決等，因與本案無關，不多作討論。
[122] 最高法院 100 年度台上字第 6468 號判決。

長慶合作社之理由，洵有判決不備理由之違法。」而將案件發回更審。

更審法院見解與最高法院相同，並未多加說明，僅交代「然被告事後曾將手邊留存之前開電磁紀錄備分提供予後手某乙一節，已據證人某乙於原審時結證屬實，已詳前所述，**被告刪除電磁紀錄之行為既未致生損害於長慶合作社**，可見被告之行為尚與刑法第 359 條之無故刪除電磁紀錄罪之構成要件不合，自不成立該罪。」[123]另外以本案相同事實所提起請求損害賠償之民事訴訟敗訴作佐證，加強被告刪除前開電磁紀錄確實沒有造成損害之說明，判決被告無罪。

## 三、判決簡評與討論

本案中，撇去法院論述似有指摘檢方舉證不足之意思，對於損害的判斷方式，三審和更審法院令人意外的似偏向採信被告「歸還備份故並未造成損害」抗辯，認為在該電磁紀錄確實已經歸還的前提下，無法證明致生何種損害，而不採檢方所主張的「使接手其職務之某乙，不能立刻查考、追蹤長慶合作社之參展成效，且無法即時與國外固有客戶聯繫，顯已致生損害於長慶合作社」。

本文以為，本案單純從判決內容觀察，固然不能排除檢方舉證不足的可能性，但若在檢方此種主張輔以明確證據的前提下，法院認為無致生損害的見解實無道理。電磁紀錄本身具有**可複製性**，故在面對類似於傳統動產的犯罪行為（例如毀損、竊盜等等）所對應到電磁紀錄領域的行為（例如刪除、取得電磁紀錄）時，損害的認定思維並不能用**純粹的經濟損害**去一概而論。舉例來說，在取得電磁紀錄的行為發生時，舊有電磁紀錄事實上並不因此消失或無法存取，對於圓本所有人來說，根本不生任何實際上的經濟損害；竊盜行為完成後，標的物的實體控制便隨之移轉給犯罪行為人，對於原所有人來說當然遭受了該標的物所具有的經濟價值損害。也就是說，傳統動產在此是排他而唯一的，經濟損害的計算相當明確，但電磁紀錄卻可能因為取得的行為而產生「副本」的共存現象，而讓原所有人未受（或無感）實質經濟損害。

[123] 臺灣高等法院高雄分院 100 年度上更（一）字第 121 號判決。

如本案中，被告確然歸還了「相同」的電磁紀錄（事實上以物理角度觀察並非當初被刪除掉的那一份），從電磁紀錄的外觀來看當然是相同的，若單純從該電磁紀錄所表彰的經濟損害來看，似乎在完璧歸趙後根本沒有損害可言。但是進一步來看，本文認為檢方對損害的認定方式才是正視了電磁紀錄的特性，從後手某乙接手工作後不能立刻使用該電磁紀錄所記載之資訊這點來看，確實產生的隱晦的時效上損害。此種損害在本案這種公司行號的經營中，還可能勉強用電磁紀錄中記載的資訊，與其相關的交易、契約或聯繫時效等等方面，找出一個實質經濟損害的數字，但若在被害人是一般私人時，似乎就註定無法以相類似的方式處理。法院此種認知，實有誤會電磁紀錄可能表彰的經濟損害之外的其他價值之嫌。

包括本案在內，事實上本文所節選關於第 359 條的實證案例都圍繞在一個問題打轉，亦即**損害認定的標準**。從前開論述可知，各級法院採用的見解大抵可分三大類。**第一大類，係對損害認定最為寬鬆的見解，放寬第 359 條的損害認定標準，認為只要到達足生損害之程度即為已足，而無須有實際損害的結果**，例如臺灣新北地方法院 95 年度易字第 88 號判決、臺灣高等法院 96 年度上訴字第 1142 號判決等便採用此一標準。然此一標準令人詬病者，係其偏離第 359 條後段「致生損害於公眾或他人者」之結果犯要件，而似將本條解讀為危險犯。此種見解屬於少數說，大多被上級法院指摘對構成要件的解釋有誤，而遭到撤銷。

**第二大類，則是嚴格遵守構成要件認定損害結果，認為理由和事實都要能夠清楚指出損害為何，而部分判決在損害的認定標準甚至有偏向必須有實質的經濟損害之傾向**，例如最高法院 98 年度台上字第 3015 號判決、最高法院 96 年度台上字第 6981 號判決、臺灣高等法院 96 年度上更（一）字第 949 號判決、最高法院 100 年度台上字第 52 號判決、最高法院 100 年度台上字第 6468 號判決、臺灣高等法院高雄分院 100 年度上更（一）字第 121 號判決等等，應係實務多數見解。這類判決對於損害結果認定嚴格，恪守構成要件之規範，頗值贊同，但部分見解過度重視實質經濟損害已如前述，恐有無法落實本條立法目的之嫌，則是較為值得

檢討的問題。

**第三大類係較為折衷的見解，大多由重申本條為結果犯開始，進而論述本條係以保護電子化財產秩序為目的，其所謂具體之損害並不僅指經濟上損害，尚包括了其他類型的損害**，但可惜並未再做進一步的論說。[124]例如臺灣高等法院 95 年度上訴字第 2674 號判決、臺灣高等法院台南分院 99 年度上更（一）字第 10 號判決等。[125]此種見解對於損害的認定較第二大類寬鬆，本文認為也是較合乎立法目的與現實情況的類型。電磁紀錄之經濟價值損害與傳統動產不同已如前述，倘若不正視電磁紀錄受不法取得、變更或刪除行為侵犯時可能造成的其他類型損害，例如隱私、電子化財產秩序等等，則可能造成本條立法目的落空，而成為適用範圍狹隘而形同具文的規範。

## （六）修法建議

本罪主要保護的客體是「電磁紀錄」，所禁止的行為是無故取得、變更與刪除。本文以為，應將三種不同行為分別規範，明確界定三種行為態樣的差異與分界，重新思考禁止該行為之目的與保護法益為何，並且檢討各自對應的應有刑度。[126]

其次，對於本條所規範之行為態樣，若能加以說明或定義為佳。舉例來說，本文認為「刪除」此一要件，技術面來觀察便可能產生爭議。[127]事實上，本罪的三種行為態樣間，有許多彼此重疊的部分。例如刪除電磁紀錄，實際上必然伴隨

---

[124] 判決論述謂：「本條犯罪之成立以對公眾或他人產生具體之損害為必要，然本項法益在於維持電子化財產秩序，並不以實際經濟上之損害為限（此有立法理由可參）。」參臺灣高等法院 95 年度上訴字第 2674 號判決。

[125] 臺灣高等法院台南分院 99 年度上更（一）字第 10 號判決因性質雷同，並未列入本文實證所引判決之內。其論述為：「按『無故取得、刪除或變更他人電腦或其他相關設備之電磁紀錄，致生損害於公眾或他人者』，構成刑法第三百五十九條之罪。而電腦已成為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（此參照該條之立法理由），足認本條犯罪之成立雖以對公眾或他人產生具體之損害為必要，然**本項法益既係在於維持電子化財產秩序，故並不以實際上對公眾或他人造成經濟上之損害為限**。」

[126] 參前揭註 96。

[127] 參前揭註 95。其實要「刪除」到何種程度才算是刪除，屬於立法者價值評斷的問題，若能清楚表明其看法，自然可以減少相關的爭議。

（或同時該當）變更電磁紀錄之行為。則此時立法者心目中究竟何謂「變更」，似乎就有必須說明清楚之必要。因此，在各行為態樣間的設計與說明上，需要特別注意重疊與競合的問題，方能減少適用上的困難與爭議。

再者，「致生損害於公眾或他人」的構成要件，應以前開同一行為分列雙重法條設計的方式取代，透過確立保護法益不同時，對應實害犯或危險犯的寬嚴不同條文設計，以期妥適評價犯罪者行為的嚴重性，同時能杜絕損害判斷標準不一的問題。[128]

在個人法益的保護上，或可採用「足以生損害於他人」的要件取代，藉此將損害結果從構成要件內容轉換為判斷侵害強度的佐證，除了可以消除前開學界所謂雙結果犯的疑慮外，讓本條合於規範目的，也修正原先雙結果犯的要件設計，減少難以舉證損害結果而無法該當本罪的情況。[129]在社會法益的保護上，則以前開行為態樣，搭配「致生資訊安全之公共危險」的公共危險犯要件設計，將較為嚴重的取得、變更或刪除電磁紀錄行為，提前到危險犯的層級，以利公權力提早介入處理。並且就對社會資訊安全信賴侵害較為嚴重的社會法益之罪，可設計未遂犯作為銜接，避免此種強烈提高社會危險的行為因為未遂而無法處理的漏洞。如此一來，因為統一了對於損害認定的標準，也可以有效解決實務上寬嚴不一的損害標準問題。

## 第三節　第 360 條

刑法第 360 條干擾電腦或其相關設備罪：「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。」立法理由認為：「鑒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

[128] 詳參本文第三章第四節遠程解決方案部分之論述。
[129] 林孟皇，前揭註 101，頁 89-91。

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。」[130]

本罪主要的評論多集中於構成要件中「干擾」一詞的定義不清，立法者雖有於立法理由中舉例說明，惟仍未直接明確的做出定義。此一評論，與本文第二章所論及應以抽象定義方式釐清本罪章各關鍵用語之主張可說是遙相呼應。另外，所謂的「電腦程式或其他電磁方式」之干擾手法規定，也令人費解。

本文在此所節錄之判決，（二）判決實證：最高法院 101 年度台上字第 739 號判決中係典型 DDoS 攻擊手法，該當本條干擾行為並無疑問，但值得討論者係何種程度達到干擾損害結果的程度？（三）判決實證：臺灣高等法院高雄分院 95 年度矚上訴字第 4 號判決中，則主要討論本條所謂干擾手法規範模糊可能衍生的問題。

## （一）學界評論

第 360 條干擾電腦或其相關設備罪中所謂「干擾」，學說上認為係指未達毀損之程度，但卻得使電腦於受干擾期間暫時使用不能或效能大幅下滑，在排除干擾後仍可恢復正常運作之暫時性阻礙行為而言。[131]立法理由中亦有舉例作說明。[132]即便如此，論者仍有認立法理由對干擾定義似有做出說明，但仍未直接對於究竟是何種行為係「干擾」下明確定義，直接沿用修法前第 352 條第 2 項就未加以定義的干擾一詞，除了沒有解決舊法的問題外，仍然可能持續造成適用上的恣意或困難。[133]

---

[130] 前揭註 29。

[131] 林山田，前揭註 27 書，頁 558；曾淑瑜，前揭註 77，頁 132；林冠宏，前揭註 38，頁 96-97。

[132] 本條立法理由二提及分散式阻斷攻擊（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，便係著例。參前揭註 26。

[133] 李茂生，「刑法新修妨害電腦使用罪章芻議（下）」，台灣本土法學雜誌，第 56 期，2004 年 3 月，頁 207-209；鄭逸哲，前揭註 31，頁 111；廖宗聖、鄭心翰，前揭註 75，頁 81-82。本文以為，論者的主張與本文認為應「名正而後言順」去定義「電腦」等詞彙的用意相近，多有認為若不對

舉例來說，在「干擾」一詞定義不清的情況下，若某電信業者透過基地台發送強力訊號方式進行「蓋台」，此種看似單純發送訊號的合法行為，卻致使鄰近的它台業者客戶訊號微弱甚至收不到訊號時，是否構成本條所稱「干擾」行為？

此外，亦有論者認為，除了干擾一詞外，立法者用以限制干擾手法的「電腦程式」和「電磁方式」，對於缺乏資訊相關訓練的法律從業人員而言也相當難以認知。[134]本文則認為相較於外國立法例，本條對於干擾手法的定義確實過於模糊，且客體部分也僅規範了電腦及相關設備，並不及於電磁紀錄本身，而有改進的空間。

## （二）判決個案分析：最高法院 101 年度台上字第 739 號判決[135]

### 一、判決事實、爭點與法院見解

本案事實略謂：被告某甲為「聖僑資訊事業股份有限公司」（下稱聖僑公司）之負責人；被告某乙係聖僑公司資訊部門技研組組長，負責程式設計；某丙則原任聖僑公司之業務經理，於民國 96 年 7 月 31 日離職後，以其妻某丁名義，另設立與聖僑公司業務經營項目相近、具商業競爭關係之薪僑資訊整合有限公司（下稱薪僑公司），且薪僑公司所有之「www.plas-rubber-machine.com」、「www.prm-video.com」、「www.prm-catalog.com」、「www.prm-mail.com」網址等網站，均委由某戊擔任負責人之達文西數位科技有限公司（下稱達文西公司，上揭網址所在 IP 位址係 61.56.212.51）代為管理。緣某甲因見薪僑公司之廣告宣稱可提供客戶「高畫質網路影像線上即時瀏覽動態影片技術」，致聖僑公司流失客戶，故指示某乙對薪僑公司網站進行干擾，某乙乃與某甲基於無故以電腦程式干擾他人電腦與相關設備，及製作專供上開犯罪之電腦程式等共同犯意之聯絡，由某乙自在上址聖僑公司辦公室內，密集接續地**以網路下載之電腦程式**，或**以自己**

何謂「干擾」做出定義，構成要件的模糊性與罪刑法定原則會因此產生衝突，適用上亦有流於恣意或產生困難的風險，實間接支持了本文第二章的論證。

[134] 張紹斌，前揭註 62，頁 97；廖宗聖、鄭心翰，前揭註 75，頁 82。

[135] 本案歷審判決為臺灣台中地方法院 97 年度訴字第 1494 號判決、臺灣高等法院台中分院 98 年度上訴字第 1992 號判決、最高法院 101 年度台上字第 739 號判決。

**撰寫專供上述干擾薪僑公司電腦及相關設備等犯罪之 Httptestor.exe 電腦程式**，透過聖僑公司所申請之上網線路及聖僑公司以外之多個網路 IP 位址對外連線，針對薪僑公司網站首頁，**多次重複持續寄出大量請求封包以佔用網站服務資源之方式，對上揭薪僑公司之網站進行干擾**（即藉 DDoS 阻斷式攻擊之方式，佔用系統分享資源，使薪僑公司網站提供服務之資源被佔用，達到干擾薪僑公司正常網路連線系統運作之目的），造成薪僑公司網站及其他亦由達文西公司代管而位於同一 IP 位址 61.56.212.51 之數十家公司網站服務功能均無法正常運作，因而使薪僑公司之客戶無法順利登入薪僑公司網站收發國際貿易往來之電子郵件、達文西公司所代管網站之其他客戶網站無法連結、電子郵件無法正常收發，致生損害於薪僑公司、達文西公司。事經達文西公司負責人某戊發現其公司所有 IP 位址 61.56.212.51 之網路伺服器流量異常，而以防火牆流量監控程式得知干擾來源之 IP 位址係 61.225.5.223 及 61.225.2.8，即報警處理，某戊並將薪僑公司上開網址移至 IP 位址為 211.20.64.154 之基隆機房，**上揭網站服務功能干擾行為旋隨同薪僑公司之網址轉移**；後再以 wireshark 軟體程式（用以截錄封包使用之程式）進行封包截取分析後，發現來自泰國、墨西哥、中國大陸、印度等代理伺服器主機之不同來源封包中，**有相同之 IP 位址 122.127.211.102 及 220.140.113.30**，經再以 Tracert 診斷工具（係一用以追蹤封包所走路徑之指令）追查此 IP 位址來源，發現皆為透過 h33.s152.ts.hinet.net 所提供之浮動 IP，而肯定此二 IP 位址皆為發動干擾行為之來源。嗣經台中縣警察局霧峰分局會同內政部警政署刑事警察局，向 ISP（即網路服務供應商）中華電信公司調閱相關 IP 紀錄，查知 IP 位址 61.225.5.223 及 61.225.2.8 為聖僑公司申請使用，並前往聖僑公司資訊部門執行搜索，經比對聖僑公司之連線紀錄，發現上開源自 IP 位址 122.127.211.102 及 220.140.113.30 之封包，皆係由聖僑公司所發送，並當場查扣聖僑公司所有之電腦主機 14 臺及 NAS（網路硬碟）主機 1 臺。[136]

[136] 臺灣台中地方法院 97 年度訴字第 1494 號判決。

本案主要牽涉的法條包括第 360 條干擾電腦及其相關設備罪，以及第 362 條製作損害性電腦程式罪。就第 360 條部分，事證明確，一二審法院見解相同，均認為被告所為 DDoS 阻斷式攻擊確實干擾了被害人主機之運作，除引用多分專業鑑識報告外，也透過被干擾伺服器服務確實遭到癱瘓之結果，去說明被告所主張「流量測試」、「測試競爭對手是否確實能提供多國連線服務」等抗辯，認為被告所為衡諸常理已經遠超過合理測試的範圍。

而損害認定部分，二審法院則認為：「告訴人薪僑公司及達文西公司之網路系統，確實因被告上揭佔用大量網路資源之干擾，致使薪僑公司網站及其他亦由達文西公司代管而位於同一 IP 位址 61.56.212.51 之數十家公司網站連結功能均無法正常運作，因而使薪僑公司之客戶無法順利登入薪僑公司網站收發國際貿易往來之電子郵件、達文西公司所代管網站之其他客戶網站無法連結、電子郵件無法正常收發，致生損害於薪僑公司、達文西公司等事實……復有達文西公司之網站因遭被告上開攻擊行為而癱瘓，致須租用虛擬主機之發票、支付超出頻寬費用之收據等附卷可證（見原審卷第 187 至 190 頁），故被告無故以電腦程式干擾他人電腦及其相關設備，致生損害於告訴人等之事實，甚為明確。」[137]認定被告之行為該當第 360 條干擾電腦及其相關設備罪。

較具爭議者，係被告是否確實製作了 Httptestor.exe 電腦程式作為 DDoS 阻斷式攻擊使用。一審法院除了引用相關證人的證言、被告抗辯該程式未完成無法使用外，主要以內政部刑事警察局鑑定報告中指稱：「1、…**被告所使用之程式原始碼，無法認定係自行撰寫或係網路上下載取得，因電磁紀錄有易修改特性，即使程式碼係由網路上下載取得，亦有可能取得後修改程式碼內容，故無法認定係自行撰寫或係自網路上下載取得**，2、經查找所有扣案電腦，除證物編號 000000000-0 因無法將硬碟重組且開機時發生錯誤，無法鑑驗外，其餘電腦主機並無搜尋出與貴院所提供之原始碼相同之檔案。」等理由，認為積極證據不足以認定被告確實

[137] 臺灣高等法院台中分院 98 年度上訴字第 1992 號判決。

有製作該損害性程式，就此一部分判決被告無罪。

但二審法院認定卻有所不同。二審法院先提出被告承認自行撰寫 DDoS 阻斷式攻擊程式，之後才利用搜尋去找相類似軟體等語作基礎，其次說明程式碼與執行檔之不同，指摘被告主張該 Httptestor.exe 電腦程式未完成等抗辯不可採，且針對一審主要依據的鑑識報告，補充一段說明：「惟該項鑑識報告之後段亦同時說明『**電腦中若存放有該原始碼編譯後之執行檔，縱未有原始碼亦可執行該程式，然該執行檔檔名未知，本局無法得知係由何幾部電腦主機對薪僑公司寄出封包**』等語，復觀諸該鑑識報告之相關記載（見原審卷第 263 至 264 頁），可知刑事警察局對上開電腦進行鑑識時，係因未能知悉該執行檔檔名，故以副檔名".pas"對扣案主機進行原始檔之檔案搜尋，致未搜尋出原始檔，非指未能尋獲可供執行 DDoS 攻擊之執行檔」認為一審法院誤會了鑑識報告的意思，而有錯誤的見解，推翻一審法院判決，認定被告就製作損害性電腦程式部分有罪。

罪名競合部分，二審法院認為：「核被告所為，均係犯刑法第 360 條之無故以電腦程式干擾他人電腦與其相關設備罪，及同法第 362 條之製作專供犯罪之電腦程式罪。……又被告等為達干擾告訴人公司電腦及其相關設備之目的，而製作專供此項犯罪之電腦程式，乃以一行為而同時觸犯上述 2 項罪名，構成**異種想像競合**犯，應依刑法第 55 條之規定，從一重依刑法第 362 條之製作專供犯罪之電腦程式罪處斷。」被告不服上訴三審，最高法院則除支持二審見解外，亦補充一審時證人對 Httptestor.exe 電腦程式作為 DDoS 阻斷式攻擊使用的證詞加強判決說服力，駁回被告上訴。

## 二、判決簡評與討論

本案關於干擾電腦罪部分之所以較無疑義，主因是其損害結果明確，攻擊手法又是普遍（且立法理由早已明文提及的）DDoS 阻斷式攻擊，干擾行為成立與否的判斷問題不大。即便如此，二審法院在判決中提及：「……可見該局在無法得知係由何幾部電腦主機對薪僑公司寄出封包之情形下，僅可提供以『程式執行時

執行緒參數、執行時間長短與對方網站頻寬大小及是否影響其提供正常服務』等項，作為判斷『究係合理測試範圍進行測試或係針對電腦及網路設備產生重大影響之故意干擾行為』之參佐標準……」可以得見若非本案損害結果較為嚴重，一旦干擾行為相關扣案的電腦軟硬體證據不足時，在重度依賴專業鑑定報告的前提下，法院對於何種行為構成「干擾」與否的判定恐怕易生問題。

其次，從被告之「合理測試」抗辯，亦可得見科技中立性與本罪章各罪間的緊張關係。撇去本案嚴重的損害結果不談，究竟何種程度的「流量測試」才不構成 DDoS 阻斷式攻擊的干擾行為？又，本案中被告雖然未對 Httptestor.exe 電腦程式作科技中立性抗辯，但從被告執著於程式的可運作性抗辯，以及鑑定單位所稱電磁紀錄的易修改性等角度觀察，要如何確認某個損害性程式確實是單純為了損害目的而製作、該程式確實足以造成損害以及確實是由被告所製作等節，恐怕也是相當困難。

## （三）判決個案分析：臺灣高等法院高雄分院 95 年度矚上訴字第 4 號判決[138]

### 一、判決事實與爭點

本案主要之事實與本文主旨無關，特將本案列入個案分析之理由，乃係因本案二審法院論及**強制罪與干擾電腦或其相關設備罪之關係**，頗有值得參考的部分，合先敘明。本案中與干擾電腦與其相關設備罪有關之事實略謂：被告某甲因某乙欲與其分手，拒絕與某甲見面，引起某甲不滿，為迫使某乙出面與其復合，某甲於兩個月內大量撥打某乙原任職公司、新任職公司以至某乙父母手機等號碼，次數均多達近百次甚至百次以上，使某乙及其親友不堪其擾，需更換門號等情，檢方認為涉犯強制罪併案起訴。

### 二、法院見解

[138] 本案歷審判決為臺灣高雄地方法院 95 年度矚訴字第 1 號判決、臺灣高等法院高雄分院 95 年度矚上訴字第 4 號判決、最高法院 97 年度台上字第 2174 號判決。

二審法院對此表示：「按刑法第 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。』；而刑法第 304 條第 1 項係規定：『以強暴、脅迫使人行無義務之事或妨害人行使權利者，處三年以下有期徒刑、拘役或三百元以下罰金。』，**該二規定之最高法定刑均為 3 年以下有期徒刑**。則刑法既就干擾他人使用電腦另設特別規定，並與刑法第 304 條強制罪之最高法定刑度相同，**足見立法者係認此等對於干擾他人電腦設備，致妨害正常使用之行為，非屬刑法第 304 條之強制罪**。而被告以連續撥打上開證人及公司之電話，干擾他人使用電話，因刑法並無處罰規定，依刑法第 1 條所定之罪刑法定原則，自不得依擴張或類推解釋，對被告論以刑法第 304 條第 1 項之強制罪。故被告上開所為干擾他人使用電話之所為，應屬社會秩序維護法第 68 條：『藉端滋擾住戶、工廠、公司行號者，處三日以下拘留或新台幣一萬二千元以下罰鍰』規定之處罰範圍。」

**三、判決簡評與討論**

從本案法院的判決脈絡，可以推想法院認為被告連續撥打電話之騷擾行為，除不具有強暴脅迫之性質外，也不包括在干擾電腦及其相關設備罪的適用範圍內。但若由此發想，倘今日某一行為人以網路電話程式大量撥打電話，佔用警消線路時，是否構成以電腦程式干擾之罪？若某一行為人以手機手動大量撥打電話，佔用警消線路時，是否構成以其他電磁方式干擾之罪？若某一行為人以無線電發射器佔用警消頻道，使警消無法溝通，是否構成以其他電磁方式干擾之罪？雖然從判決中，吾人無法直接看出第 360 條所潛在的問題，但若從前開延伸疑問觀之，本罪除了受干擾的客體「電腦及其相關設備」定義不清而無法確認範圍（電話、無線電是否屬於電腦及其相關設備？）外，所謂的「電腦程式或其他電磁方式」也令人費解而頗有模糊之嫌。

## （四）修法建議

第 360 條干擾電腦或其相關設備罪之修法方向，可先對「干擾」一詞作抽象

定義，例如學界所稱未達毀損之程度，但卻得使電腦於受干擾期間暫時使用不能或效能下滑，在排除干擾後仍可恢復正常運作之暫時性阻礙行為，即為可參考的定義範例。

另外，可仿照歐盟理事會《打擊資訊系統犯罪框架決策》，分別建立對於干擾「電腦系統」及「電磁紀錄」的兩種不同客體的相對應規範，補足現行法漏未規範的資料干擾行為。[139]本文認為應參考該決策對於干擾方式的描述，取代現行較為模糊的「電腦程式或其他電磁方式」構成要件，作較為詳盡的要件規範。[140]該決策中，係將干擾電腦系統的方式明定為「藉由輸入指令、傳輸資訊、損害、刪除、效能減損、變更、阻礙、使之難以存取等方式干擾」，而對於干擾電磁紀錄的部分則定為「藉由刪除、損害、效能減損、變更、阻礙、使之難以存取等方式干擾」，可說是相當詳盡。透過較為抽象定義之後加以較為詳盡的說明，不論要將該詳盡說明置於立法理由，或是訂立相關的管理辦法等等，均能提供實務工作者在解釋法令時不至於逸脫立法者原意，又能較為正確的理解本條所規範的行為態樣。

## 第四節　第 362 條

第 362 條製作損害性電腦程式罪：「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。」立法理由謂：「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。」[141]

---

[139] 葉亭巖，前揭註 66，頁 17。歐盟理事會《打擊資訊系統犯罪框架決策》中，Article 3 規範針對電腦系統（system）所為的干擾行為，Article 4 則是關於資料（data）的干擾行為。

[140] 決策內容詳參葉亭巖，前揭註 66，頁 17。

[141] 前揭註 29。

學界對於本條的定位，有認為是本章他罪的實質預備犯，然而在程式製作者與實際使用者非同一人的情況下，可能有評價矛盾與混亂的問題產生。此外，本罪設計「專供犯本章之罪」的要件，似期望透過此種方式彰顯行為人的惡意，卻造成認定與判斷的困難，更與科技中立性原則有違，似亦非妥適的立法方式。

本條在實務判決中甚少使用，推想應是因為程式碼易於修改之特性，致使檢方往往難有證據證明該程式確實為被告所製作，更遑論該程式是否真的專供犯本章之罪之證明亦有相當困難，因此僅以被告坦承製作盜錄刷卡資訊軟體的（二）判決實證：臺灣高等法院台中分院 98 年度上更（一）字第 35 號判決為例。此外，亦可參酌本章第三節第二段之判決亦與本案有關，主要爭點即是程式損害性、可運作性以及是否確實為被告所製作，應可略見本條在實務操作上的困難。[142]

## （一）學界評論

本條所謂損害性電腦程式，係指諸如電腦病毒、木馬程式等，可能對於電腦、電磁紀錄產生損害的程式而言，立法理由訂有明文。[143]有論者認為本條係本章他罪的實質預備犯，在他罪並未處罰未遂犯的前提下，此一設計違反罪刑法定原則；在競合論的操作下，例如病毒製作者與用以干擾他人電腦者為同一人時，製作病毒行為被干擾行為吸收，反而造成罪責減輕、評價錯誤的詭異現象。[144]

其次，也有論者以為，從條文結構來看，行為人需要同時滿足（一）製作專供犯本章之罪之電腦程式、（二）供自己或他人犯本章之罪且（三）致生損害於公眾或他人三個要件才該當本罪，屬於過度嚴格的規範方式。[145]在製作與使用該損害性程式者非同一人的情況下，製作者是否該當於本罪的判斷，乃取決於該他人是否使用該損害性程式犯本章之罪，此時已經讓處罰的範圍擴散，使本罪的判

[142] 詳參本文第四章第三節（二）判決實證：最高法院 101 年度台上字第 739 號判決。
[143] 前揭註 29。
[144] 李茂生，前揭註 133，頁 212；鄭逸哲，前揭註 31，頁 113-115；盧映潔，「電腦小子鑄大錯」，月旦法學教室，第 57 期，2007 年 7 月，頁 18-19。
[145] 柯耀程，前揭註 58，頁 128；廖宗聖、鄭心翰，前揭註 75，頁 84。

斷陷於不確定的狀態。[146]論者批評，若認為有害程式對於資訊安全確實有危險性，則性質上類似公共危險，應提前針對製作與散布行為加以處罰，而不應以後續的使用行為來決定是否處罰。事實上，若確實使用該程式犯本章他罪，則論以該罪之刑責即可；反之，若提供他人使用者，可以其參與程度與犯罪支配等條件，論以共同正犯、幫助犯或教唆犯即可。[147]

此外，本條構成要件中的「專供」一詞，雖然論者認為立法者係希望藉此表達行為人的「惡意」，惟操作上卻可能因為認定不易，而致生不必要的困擾，似應修正。[148]甚至有論者直言，若該程式必須是「專供」犯「本章之罪」所用，則被告就所涉犯行應該作「無恥答辯」，主張自己要以該程式「兼」犯他章之罪，此時因為該損害性程式並非用於「專供犯本章之罪」，會產生不該當本罪的弔詭情況。[149]

本文則認為，若以科技中立性角度觀察，事實上多數所謂「損害性」程式均能用於正當用途，例如用以測試作業系統是否有安全漏洞，或是防火牆和防毒軟體是否能辨識、阻絕可能有害的程序（process）與連線，甚至進行連線壓力測試等等，實難純以該程式的「存在」本身即能證明製作者的「目的」。[150]此時本條的操作與設計目的上，無疑是處罰「使用」而非「製作」有害程式的行為，當產生此種實際上為了處罰使用有害程式的目的，而反過來去規範製作之行為時，對於刑罰權發動的目的實有模糊不清之處，而可能肇生實務操作上的爭議。

## （二）判決個案分析：臺灣高等法院台中分院 98 年度上更（一）字

[146] 柯耀程，前揭註 58，頁 128；廖宗聖、鄭心翰，前揭註 75，頁 84。
[147] 蔡蕙芳，前揭註 25，頁 68-70。
[148] 李茂生，前揭註 133，頁 213；鄭逸哲，前揭註 31，頁 114。
[149] 張紹斌，前揭註 62，頁 99。
[150] 類似見解以為，許多監控電腦系統軟體雖可用於入侵電腦使用，但仍可用於監控電腦資源分配等正當用途，則不應該當本罪，參林山田，前揭註 27 書，頁 560-561。另有論者則主張，「專供」要件的解釋應以「主要用於」或「實質上用於」來限縮並確定其範圍，但本文認為即便採用此種解釋方式，對於解決爭議似仍幫助有限。參蔡蕙芳，前揭註 25，頁 69。

## 第 35 號判決[151]

### 一、判決事實與法院見解

本案事實略謂：被告某甲因經濟狀況不佳，計畫偽造他人之金融卡，以便盜領他人存款，在其住處開始製作專供側錄他人網路資料之惡意程式，以便截獲他人（或公司）在網路銀行所設帳戶之帳號、密碼（即金融卡四位數字密碼及晶片六位數字密碼）、及使用者電腦名稱、以及身分證號碼或公司統一編號等相關資料；其間並另購入空白內容之磁條卡，以供日後偽造金融卡使用。其後**製作完成專供其自己盜取他人網路銀行帳號及密碼，名為「smart.exe」之電腦惡意驅動程式**，並透過電子信箱寄送購物廣告之方式，將惡意程式隱藏在電子郵件中，透過引導使用者安裝該程式進行網路購物轉帳時，側錄用戶網路銀行之相關資訊，以供偽造金融卡之用。

本案中，被告所製作之電腦驅動程式，應屬於個人電腦使用之讀卡機驅動程式，並加上側錄之功能，能將插入讀卡機中的卡片資訊進行拷貝，並傳送回被告處，透過不知情用戶之安裝與使用，可達成竊取卡片資訊之目的，進而讓被告利用該資訊製作偽卡使用。

本案事實明確，**被告針對製作該「smart.exe」程式乙節坦承不諱**，並未多作抗辯，法院依法判決被告有罪，論述中並未較有討論價值之部分，故本文不多作引述。

### 二、判決簡評與討論

事實上，本文在實證過程中曾試過與本條相關的多種關鍵字查詢，但實務上用到本條的案件卻相當稀少，亦惜未有較為精彩的論述，僅有前開最高法院 101 年度台上字第 739 號判決乙案中花費較多篇幅討論而已。[152]但本案事實中，若被

[151] 本案歷審判決為：臺灣台中地方法院 94 年度訴字第 2810 號判決、臺灣高等法院台中分院 94 年度上訴字第 2679 號判決、最高法院 98 年度台上字第 232 號判決、臺灣高等法院台中分院 98 年度上更（一）字第 35 號判決。本案主要罪名係偽造有價證券，但被告為達偽造之目的，自行製作側錄程式，亦涉犯第 362 條之罪。

[152] 參本文第四章第四節第二段，即（二）判決實證：最高法院 101 年度台上字第 739 號判決。

告主張其用以犯罪的「smart.exe」程式**並非自己所製作**時，在程式碼易於修改的前提下，又應如何證明與處置？這仍是值得吾人深思的問題。

## （三）修法建議

第 362 條製作損害性電腦程式罪部分，在現行法的設計下，因為需要同時滿足（一）製作專供犯本章之罪之電腦程式、（二）供自己或他人犯本章之罪且（三）致生損害於公眾或他人三個要件才該當本罪，且「專供」犯本章之罪本難以界定，在製作人與使用人非同一人的情況下，處罰的範圍擴散，相當難以操作。考量本條的規範目的，實際上是為了避免電腦程式被用以進行犯罪行為，而肇生後續損害與資訊安全的危險，實頗有公共危險罪的性質。

本條的修正方向部分，慮及「專供犯本章之罪」的構成要件定義易生爭議，而不利實務操作，加以科技中立性原則的考量，應予以刪除。再者，「供自己或他人犯本章之罪」，雖係立法者為限縮本條處罰範圍而訂，操作上卻可能導致困難，也非妥善的立法方式。

本文認為，既然本條規範目的偏向公共危險性質，「製作」損害性程式本身係一種提高網路資訊安全潛在風險的行為，故構成要件設計上可仿照公共危險罪章模式，強化「損害性程式」製作者「保管」該等程式使之不外洩的義務，在因製作者的故意或過失致使該可能有害程式流出造成公眾資訊安全上的危害時，才對之發動刑事處罰。如此一來，便無須去考量製作程式者到底是否是為了「專供犯本章之罪」才製作與否的問題，而係以客觀上該程式是否具有資訊安全的危險性，決定製作者是否需要負擔相對應的監管責任，在該程式外流而確實用於進行犯罪時，便對製作者予以究責，應較為妥適。

至於非製作者散播有害程式的行為，則應端視立法者是否認為此舉是否係已嚴重到須特別立法規範的行為，否則以現況來說，本文則傾向在犯罪發生（例如干擾或變更、刪除電磁紀錄而造成損害等）而有相對應的正犯時，再以共同正犯或幫助犯等相繩，便為已足，似無須提前以刑事處罰去規範此種行為。

## 第五節　　第 361 條及第 363 條

刑法第 361 條係對公務電腦及其相關設備犯本章之罪的加重規定：「對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。」立法理由謂：「二、由於公務機關之電腦系統如被入侵往往造成國家機密外洩，有危及國家安全之虞，因此對入侵公務機關電腦或其相關設備之犯行加重刑度，以適當保護公務機關之資訊安全，並與國際立法接軌。三、本條所稱公務機關，係指電腦處理個人資料保護法第三條所定之公務機關。」[153]

而刑法第 363 條則是告訴乃論規定：「第三百五十八條至第三百六十條之罪，須告訴乃論。」立法理由謂：「二、刑罰並非萬能，即使將所有狹義電腦犯罪行為均規定為非告訴乃論，未必就能有效遏止電腦犯罪行為，尤其對於個人電腦之侵害行為，態樣不一，輕重有別，如受害人無告訴意願，並配合偵查，實際上亦難達到偵查成效，故採告訴乃論，有助於紛爭解決及疏解訟源，並可將國家有限之偵查及司法資源集中於較嚴重之電腦犯罪，有效從事偵查，爰增訂本條。三、至於第三百六十一條之罪，因公務機關之電腦系統往往與國家安全或社會重大利益密切關聯，實有加強保護之必要，故採非告訴乃論以嚇阻不法。第三百六十二條之罪則因該行為可能造成社會重大損失，惡性較第三百五十八條至第三百六十條之罪為重大，而個別被害人往往因證據已經滅失，或不願出庭作證，以致發生被害人數雖然眾多，但卻無被害人願意提出告訴之窘境（台灣 CIH 病毒案例即無被害人願意提出告訴），影響檢察官對此類犯行之追訴，故採非告訴乃論，以有效懲處不法。」[154]

由於第 363 條規定本罪章第 358 條到第 360 條之罪原則均為告訴乃論，因此實務與學說有所討論者，係第 358 到第 360 條之罪若經第 361 條加重後，是否仍屬告訴乃論。此一問題，最高法院已有穩固見解，認為經第 361 條加重後，其涉

[153] 前揭註 29。
[154] 前揭註 29。

犯之罪已非原始（未加重）之罪，而屬於另一獨立罪名，非告訴乃論之罪，本文將於（二）判決實證：本章之罪引用第 361 條加重後是否仍須告訴乃論進行介紹。

此外，另一關於第 361 條之問題，則是草率的僅規定對於公務機關電腦犯本罪章之罪才予以加重，則在電腦屬於私人、但電磁紀錄屬於公務機關時，適用上便有疑義。再者，資訊時代中大型私人機關電腦一旦受本罪章之罪所侵害，其損害的規模與範圍未必亞於公務機關，現行法卻僅能在公務機關的案件中作刑度加重，已有不合時宜之疑慮。

至於第 363 條告訴乃論規定，雖能減少訟源，但在電腦所有人與使用人不同，或是電磁紀錄所有人與關係人不同等情況時，容易肇生告訴權爭議。本文在（三）判決實證：最高法院 101 年台上字第 5295 號判決中，便以陶氏公司資料庫案為例，可得見告訴權爭議對實務運作之影響。

### （一）學界評論

第 361 條係對公務電腦及其相關設備犯本章之罪的分則加重規定，學說與本條相關的討論，主要係本條是否為非告訴乃論之爭議。[155]然實務上對此似有定論，認為本條屬於刑法分則加重規定，故本條以及合於本條要件的各罪，性質上與原先罪名屬於告訴乃論不同，應屬於非告訴乃論之罪。[156]舉例來說，若被告甲涉犯第 359 條取得變更或刪除電磁紀錄罪，而受害客體為公務機關電腦時，此時因為合於第 361 條分則刑度加重規定，此時無待告訴，檢察官可自行偵查並進行追訴。

另外，有論者擔憂本條限制在「公務機關之電腦及相關設備」，但若受侵害的電腦是私人電腦，但裡面存放公務電磁紀錄時，處理上即生疑義。且若受侵害電腦雖非公務機關，卻處理相當程度的公務事務時，是否適用本條亦有疑問。[157]本文則認為本條以「公務機關之電腦」、而非受侵害的電磁紀錄本身性質作判斷基

[155] 曾淑瑜，前揭註 77，頁 133-134；張紹斌，前揭註 62，頁 98。
[156] 最高法院 97 年度台非字 285 號判決、最高法院 99 年度台上字第 6306 號判決意旨參照。詳細內容與評論，參見本文第四章第五節第二段。
[157] 王銘勇，前揭註 75，頁 30-31；張紹斌，前揭註 62，頁 98-99。

準未必恰當，特別是在操作第 359 條無故取得、變更、刪除電磁紀錄罪時，若受侵害的電磁紀錄屬於私人卻存放於公務機關電腦時，是否有本條加重之適用，亦生疑義。再者，網路世界中擁有大量電磁紀錄並不是各國政府的專利，事實上在網路世界裡面，大型網路服務提供者、企業、金融業等等，往往擁有更大量而高價值的電磁紀錄，不論是營業秘密或是客戶個資文件等等，在現行法下若受到侵害，卻無法透過刑責加重妥適評價其犯罪嚴重性，從這點可以凸顯出我國法就此似乎已有過時的跡象。[158]

第 363 條告訴乃論規定係許多主張本章保護個人法益的佐證之一。[159]立法者主張對於第 358 到第 360 條之罪，情狀各異輕重有別，若受害人無意追訴時往往造成偵查困難，故為集中資源在較為重大的犯罪上，將該三條列為告訴乃論之罪，透過此一訴訟上限制有助於紛爭解決及疏解訟源。[160]

但有論者批評是否能達成偵查實效此一理由，並非決定告訴乃論與否應考量之因素，且外國立法例就類似條文均採非告訴乃論。再者，電腦之使用與所有者可能並非同一人，於案件發生時便產生被害人與告訴權的爭議等缺點。[161]亦有論者認為一般告訴乃論的規定理由，多係犯罪輕微，或追訴可能違反被害人意願增

---

158 類似見解見王銘勇，前揭註 75，頁 31。該篇文章已經警覺例如證交所之類的非公務機關，雖所處事務與政府高度相關，但因性質上似不合於第 361 條之要件，故受侵害時依現行法是否得適用本條加重即有疑義。本文則進一步認為，縱然所處理的事務可能與公權力無甚關聯，只要該私人機關握有足夠大量或高價值的資訊時（特別是與公眾資訊相關者），一旦被入侵甚至盜拷電磁紀錄等，其嚴重性實不亞於、甚至可能高於同種犯行發生在公務機關的情況。

159 林冠宏，前揭註 38，頁 107-108。

160 刑法第 363 條立法理由：「二、刑罰並非萬能，即使將所有狹義電腦犯罪行為均規定為非告訴乃論，未必就能有效遏止電腦犯罪行為，尤其對於個人電腦之侵害行為，態樣不一，輕重有別，如受害人無告訴意願，並配合偵查，實際上亦難達到偵查成效，故採告訴乃論，有助於紛爭解決及疏解訟源，並可將國家有限之偵查及司法資源集中於較嚴重之電腦犯罪，有效從事偵查，爰增訂本條。

三、至於第三百六十一條之罪，因公務機關之電腦系統往往與國家安全或社會重大利益密切關聯，實有加強保護之必要，故採非告訴乃論以嚇阻不法。第三百六十二條之罪則因該行為可能造成社會重大損失，惡性較第三百五十八條至第三百六十條之罪為重大，而個別被害人往往因證據已經滅失，或不願出庭作證，以致發生被害人數雖然眾多，但卻無被害人願意提出告訴之窘境（台灣 CIH 病毒案例即無被害人願意提出告訴），影響檢察官對此類犯行之追訴，故採非告訴乃論，以有效懲處不法。」認為本條目的在於尊重被害人意願，且集中國家司法資源等。參前揭註 29。

161 王銘勇，前揭註 75，頁 31。

加其痛苦兩大類。惟本章之罪整體而言刑度非輕，且在使用者與所有者並非同一人的情況下，往往實際受害人雖是使用者，但電腦（或受害電磁紀錄）所有權人可能透過隱瞞或是私下填補損害的方式處理受害問題，此時尊重被害人意願的用意亦被扭曲。[162]

本文則以為，對於某一犯罪行為是否應告訴乃論的決定，其實與其保護法益息息相關，若認定該犯罪可能侵害社會法益時，就不應硬性規定告訴乃論，否則可能造成公益受損卻無人提出告訴的結果。[163]相關的修改建議與方向已如本文第三章所討論，在此就不多作贅述。

## （二）判決個案分析：本章之罪引用第 361 條加重後是否仍須告訴乃論

### 一、少數說：仍須告訴乃論

實務對於本章之罪（例如第 358 條）若以第 361 條加重後，是否仍屬於告訴乃論之罪此一問題，**少數見解認為仍須告訴乃論**。例如臺灣台中地方法院 97 年度訴字第 574 號判決以體系解釋之方法，並引用最高法院判例，認為在維持體系一貫性的角度來看，仍須告訴乃論：「1.就刑法第 361 條是否須告訴乃論部分：(1)按法律解釋應以文義解釋為先，有複數解釋之可能性時，則繼以論理解釋或社會學之解釋，就法條文義上可能之意義加以限定之操作，論理解釋或社會學之解釋結果，與文義解釋結果相抵觸時，如不超過文義或立法旨趣之預測可能性時，仍從論理解釋或社會學之解釋結果；而體系解釋、法意解釋、比較解釋、目的解釋及合意解釋，合稱為論理解釋。又所謂「體系解釋」係指以法律條文在法律體系上之地位，即依其編章節條項款之前後關連位置，或相關法條之法意，闡明規範意旨之解釋方法。此項解釋方法能維護整個法律體系之一貫及概念用語之一致，

[162] 李茂生，前揭註 133，頁 216-217。

[163] 論者亦認為告訴乃論在刑法上通常以侵害較為輕微的個人法益為主，社會及國家法益不在其範圍內。參蔡蕙芳，前揭註 35，頁 65。

在法解釋上確具價值，蓋每一法律規範係屬一整體，其條文之解釋，自亦應本諸論理之作用，就整個體系構造加以闡釋，以維護各個法條之連鎖關係，合先敘明。

(2)觀諸刑法第 36 章妨害電腦使用罪章係自第 358 條起至第 363 條，其中第 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。』同法第 361 條規定：『對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。』同法第 363 條則規定：『第三百五十八條至第三百六十條之罪，須告訴乃論。』上開條文之編排方式，核與刑法第 23 章傷害罪章中，刑法第 277 條規定：『傷害人之身體或健康者，處三年以下有期徒刑、拘役或一千元以下罰金。犯前項之罪因而致人於死者，處無期徒刑或七年以上有期徒刑；致重傷者，處三年以上十年以下有期徒刑。』同法第 280 條：『對於直系血親尊親屬，犯第二百七十七條或第二百七十八條之罪者，加重其刑至二分之一。』及同法第 287 條規定：『第二百七十七條第一項、第二百八十一條、第二百八十四條及第二百八十五條之罪，須告訴乃論。但公務員於執行職務時，犯第二百七十七條第一項之罪者，不在此限。』相仿。而徵諸**最高法院 19 年上字第 1962 號判例意旨**：『本案原審及第一審判決均認上訴人毆傷某氏，係犯刑法第二百九十三條第一項之罪，依同法第三百零二條規定，該罪須告訴乃論，雖某氏係上訴人之直系尊親屬，應依同法第二百九十八條規定加重其刑，然該條既明定為對於直系尊親屬犯第二百九十三條第一項之罪者，加重本刑二分之一，是加重者其刑，而所犯者仍係第二百九十三條第一項之罪，第三百零二條復明定為第二百九十三條之罪，須告訴乃論，又係以罪而不以刑，**則對於直系尊親屬犯第二百九十三條第一項之罪者，自在告訴乃論之列**』（最高法院 80 年度台上字第 3149 號、88 年度訴字第 804 號判決亦同此意旨），顯認刑法第 280 條係加重其刑之規定，至是否屬告訴乃論之罪，仍應以其所犯之罪名（傷害罪）為斷。準此，由妨害電腦使用罪章條文編排之方式觀之，**為維護法律體系解釋之一貫性，堪認被告被訴之刑法第 361**

**條、同法第 359 條罪嫌，仍應屬告訴乃論之罪。**(3)至艾菲科技公司之告訴代理人雖提出立法院司法委員會函及其附件「中華民國刑法部分條文修正草案」案審查報告（含條文對照表），並以其附件之審查會通過條文、行政院、司法院提案條文及現行條文對照表中，第 363 條部分說明欄記載：『... 三至於第 361 條之罪，因公務機關之電腦系統往往與國家安全或社會重大利益密切關聯，實有加強保護之必要，故採非告訴乃論以嚇阻不法。...』，主張刑法第 361 條應屬非告訴乃論之罪。然查，立法院公報第 92 卷第 29 期院會紀錄中刑法部分修正條文草案總說明十增訂第 36 章部分條文告訴乃論之規定部分，則僅記載：『刑罰並非萬能，即使將所有狹義電腦犯罪行為均規定為非告訴乃論，未必就能有效遏止電腦犯罪行為。尤其對於告訴人電腦之侵害行為態樣不一，輕重有別，如受害人無告訴意願並配合偵查，實際上亦難達到偵查成效，故為將國家有限之偵查及司法資源集中於較嚴重之電腦犯罪，有效從事偵查，爰增訂第 363 條，規定本章部分條文需告訴乃論。』而已將前揭條文對照表中說明欄三部分予以刪除；且嗣經立法院三讀通過之刑法第 363 條之立法理由亦不復見該部分之文字，是由立法解釋而論，尚難僅憑前揭未經定案之修正條文對照表之說明，即認立法者於增訂刑法第 363 條時，有意將同法第 361 條之規定，排除在告訴乃論之罪之外。 (4)綜上所述，**公訴人起訴被告犯刑法第 359 條、第 361 條之罪，依同法第 363 條之規定，應須告訴乃論；若未經合法告訴，公訴人即遽予起訴，依刑事訴訟法第 303 條第 3 款之規定，法院自應諭知不受理之判決。**」[164]臺灣高等法院 96 年度上訴字第 1313 號判決同此見解。

**二、多數說：無須告訴乃論**

**多數見解則認為本條無須告訴乃論**。最高法院 99 年度台上字第 6306 號判決中對此有詳盡的說理，除從刑法法條之立法方式說明外，也引述相關立法歷程資訊，支持其見解：「查刑法分則所列各罪，其須告訴乃論者，以法律有明文規定

[164] 臺灣台中地方法院 97 年度訴字第 574 號判決。

者為限；犯罪類型中有無採取告訴乃論之必要，屬於立法政策之形成。刑法第三百六十一條：『對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。』（下稱本條）之規定，**屬於借罪借刑雙層式簡略立法之一種**，係以借犯第三百五十八條至第三百六十條各條之原罪，再加上對於公務機關之電腦或其相關設備為行為客體犯罪之構成條件而成，並借原罪之基準刑以加重其刑至二分之一為其法定本刑。此與單層式借刑之立法例，如刑法第三百二十條第二項、第三百三十九條第二項等規定，均屬於獨立之犯罪類型。**故於借罪後，因其罪之構成條件已具備，而與原罪脫離，並為獨立之另一罪名，僅因其條文本身並無刑罰之規定，仍須併引其罰出刑由之法條依據而已。**同法第三百六十三條明定：「第三百五十八條至第三百六十條之罪，須告訴乃論。」依文義解釋，自不包括屬於別一罪名之本條之罪。關於本條於九十二年四月二十四日立法院第五屆第三會期司法委員會第十六次全體委員會議討論時，固有立法委員認應採告訴乃論之意見，然嗣經當時之法務部顏大和次長說明：『之所以第三百六十一條及第三百六十二條不採告訴乃論，是因為第三百六十一條的刑度已經有加重，所以不應該再適用告訴乃論』等語，並表明希望維持原來非告訴乃論之罪之規定後，並未再有爭議。嗣經二、三讀程序，均未再作文字之修正或增刪。參諸『中華民國刑法部分條文修正草案（電腦網路犯罪部分）審查會通過行政院、司法院提案現行法條文對照表』（下稱對照表）第三百六十三條說明欄第三點所載：『至於第三百六十一條之罪，因公務機關之電腦系統往往與國家安全或社會重大利益密切關聯，實有加強保護之必要，故採非告訴乃論以嚇阻不法。.....審查會：照案通過。』（見立法院公報第九二卷第二六期第一三七頁，第二九期第一四八、一四九頁，第三三期第一八0頁），足見立法院制定通過之本條，並未將之列為告訴乃論之罪。上揭刑法部分修正條文草案總說明（下稱草案總說明）(十)增訂第三十六章部分條文告訴乃論之規定（修正條文第三百六十三條）部分，雖僅記載：『刑罰並非萬能，即使將所有狹義電腦犯罪行為均規定為非告訴乃論，未必就能有效遏止電腦犯罪

行為。尤其對於個人電腦之侵害行為態樣不一，輕重有別，如受害人無告訴意願並不配合偵查，實際上亦難達到偵查成效，故為將國家有限之偵查及司法資源集中於較嚴重之電腦犯罪，爰增訂第三百六十三條，規定本章部分條文須告訴乃論。』等語，而未登載前揭對照表第三點之說明（見立法院公報第九二卷第二九期第一三0頁），實係因草案總說明(十)，僅在說明為將國家有限之偵查及司法資源集中於較嚴重之電腦犯罪，以有效從事偵查，所以增訂第三百六十三條，將較不嚴重之第三百五十八條至第三百六十條之罪，規定為須告訴乃論之立法目的而已，至於不在告訴乃論之列之本條及第三百六十二條等規定，當無於第三百六十三條草案總說明為贅載之必要，殊難據此即謂對照表說明欄第三點之記載已予刪除，並因此得以推論立法者就本條規定，係採告訴乃論之罪之立法。而刑法分則之加重，係就犯罪類型變更之個別犯罪行為予以加重，成為獨立之罪名，此為本院晚近所持之見解。**本條之罪係就對象為公務機關之妨害電腦使用罪所訂之加重處罰規定，屬刑法分則加重之獨立罪名，其是否屬告訴乃論之罪，自應以法律有無明文規定為判斷之基準。刑法第三百六十三條既未明定本條之罪須告訴乃論，其非屬告訴乃論之罪，乃屬當然。**」[165]本案二審判決臺灣高等法院台中分院 97 年度上訴字第 3108 號判決，以及另案臺灣高等法院 100 年度上訴字第 2288 號判決、最高法院 97 年度台非字第 285 號判決均同此見解，認為第 361 條既未被明文涵括在第 363 條告訴乃論規定中，雖有借用告訴乃論之罪名的立法方式，但借罪後之罪名本屬獨立，仍不得論其為告訴乃論之罪。[166]

簡言之，實務現況就此一問題，最高法院從最高法院 97 年度台非字第 285 號判決之後，均保持穩定見解，認為本章之罪搭配第 361 條加重規定後，屬於獨立罪名，無須告訴乃論。

---

[165] 最高法院 99 年度台上字第 6306 號判決，此即前開少數見解臺灣台中地方法院 97 年度訴字第 574 號判決的三審判決。

[166] 其中最高法院 97 年度台非字第 285 號判決亦推翻少數見解中的臺灣高等法院 96 年度上訴字第 1313 號判決，認為其判決違背法令予以撤銷。

## （三）判決個案分析：最高法院 101 年台上字第 5295 號判決[167]

### 一、判決事實與爭點

本案事實略謂：緣美商陶氏化學公司（The Dow Chemical Company，下稱美商陶氏公司）在世界各地廣設子公司，組成跨國之陶氏集團。被告某甲原受僱於美商陶氏公司在我國投資設立，持有百分之百股份的臺灣陶氏化學股份有限公司（下稱臺灣陶氏公司），而為陶氏集團員工之一，原任聚胺基甲酸乙酯的技術服務工程師職務，於 92 年間則擔任陶氏集團亞太研究發展中心技術總監（R&D technical leader）之職務，從事包含亞太地區關於聚胺酯技術研發及技術服務，並負責全球軟質聚胺酯泡棉產品的研發。陶氏集團每年投入資金、人力從事相關產品之研究發展，而將各項研發成果報告匯集為「中央報告系統」（Central Report Index，簡稱 CRI） 報告，**以電磁紀錄形式存放於陶氏集團位於美國密西根州密特蘭市（Midland） 總部電腦之伺服主機內**，而被告某甲雖經授權得以其員工編號登入後，下載並瀏覽此等 CRI 報告，但被告某甲依其簽立之僱傭契約約定，仍應基於為陶氏集團之利益，為該集團業務或經核可之目的，方得下載取得此等電磁紀錄；又上開 CRI 報告並均為美商陶氏公司或陶氏集團各子公司享有著作財產權之著作，依著作權法第 4 條第 2 款及世界貿易組織（WTO） 「與貿易有關之智慧財產權協定」之約定，受我國著作權法所保護，未經該等著作財產權人之許可不得擅自重製。被告某甲知陶氏集團以「Imperial」為計畫名稱，投入大量資金研發以天然種子（例如大豆油）作為生產軟質聚胺酯原料之技術，而陶氏集團員工為此計畫而製作之 CRI 報告或草稿、電子郵件、簡報投影片等未公開發表之文件，以及陶氏集團員工為此計畫所蒐集公眾可得知之專利、市場、同業資訊、科學期刊、新聞稿等，**皆以電磁紀錄形式匯整於名為「Imperial」之資料夾內，存放於陶**

[167] 本案歷審判決為：臺灣台北地方法院 94 年度訴字第 1561 號判決、智慧財產法院 98 年度刑智上訴字第 2 號判決、最高法院 99 年度台上字第 4363 號判決、智慧財產法院 99 年度刑智上更(一)字第 23 號判決、最高法院 100 年台上字第 3375 號判決、智慧財產法院 100 年度刑智上更（二）字第 11 號判決、最高法院 101 年台上字第 5295 號判決。

氏集團位於美國德州自由港（Freeport）電腦之伺服主機內，而此等電磁紀錄亦應基於為為陶氏集團之利益，為該集團業務或經核可之目的，方得下載；又此等「Imperial」之資料夾內如附表二編號 2 所示之部分文件，則為美商陶氏公司或陶氏集團各子公司享有著作財產權之著作，依著作權法第 4 條第 2 款及世界貿易組織（WTO）「與貿易有關之智慧財產權協定」之約定，受我國著作權法所保護，未經該等著作財產權人之許可不得擅自重製。

被告某甲以身體健康問題為由，向其主管表達辭意，並經臺灣陶氏公司通知被告某甲准以停職方式離開職務。惟被告某甲於離職前即已經積極與訴外人某乙洽談其離開臺灣陶氏公司職務後，共組創見控股有限公司（Innoholding Company ，下稱創見公司）事宜，後創見公司於香港設立。期間被告某甲並未獲指示再從事任何需要查詢 CRI 資料庫之工作，且被告某甲已無離職後再行向臺灣陶氏公司申請復職之意願，為擴充其離職後可以繼續參閱之資料庫，以其員工編號登入陶氏集團 CRI 系統，非基於為陶氏集團之利益，且非為陶氏集團業務或經核可之目的，而連續下載 CRI 報告之電磁紀錄，到臺灣陶氏公司發予被告某甲使用之筆記型電腦內，以此方式無故取得該等電磁紀錄，致生損害於陶氏集團（包括臺灣陶氏公司在內）所管領該等電磁紀錄之財產價值與安全祕密性。

其次，被告某甲並非陶氏集團「Imperial」計畫之成員，其得知「Imperial」資料夾內之電磁紀錄具有相當之經濟價值，為供其離職後可以繼續參閱，以電話向「Imperial」計畫之主持人，稱其對於「Imperial」計畫有興趣，希望能夠多學習此部分之技術等語，但刻意隱瞞其即將離職之事，而使該主持人誤認為被告某甲係為陶氏集團之利益，方欲取得「Imperial」資料夾內之電磁紀錄，而將被告某甲列入「Imperial」資料夾之讀取名單內，其後被告某甲即以其員工編號登入陶氏集團之伺服主機，將「Imperial」資料夾內之電磁紀錄，下載到臺灣陶氏公司發予被告某甲使用之筆記型電腦內，以此方式無故取得該等電磁紀錄，致生損害於陶氏集團（包括臺灣陶氏公司在內）所管領該等電磁紀錄之財產價值與安全祕密性。

本案中，檢方認為被告涉犯刑法第 359 條無故取得電磁紀錄等罪。[168]案件實體事實與證據都相當明確，之所以能纏訟多個審級不斷來回的主要原因，係**程序爭點即第 363 條告訴乃論規定所衍生的告訴權爭議**。

**二、法院見解**

一審法院首先說明刑事訴訟法第 332 條所稱犯罪被害人，係指因犯罪行為之直接被害人而言，但若所侵害者係財產法益時，對該財產有事實上管領力者（例如民法上之**準占有**），參照最高法院 32 年非字第 68 號判例、95 年度台非字第 275 號判決意旨，仍得提出告訴。

其次，一審法院就第 359 條告訴權爭議，認為：「**按刑法第 359 條所保護之法益，主要係電磁紀錄使用之安全，其內容兼及個人之財產、祕密及公共信用之安全。**告訴人臺灣陶氏公司為美商陶氏公司持有百分之百股有之子公司，為陶氏集團設在我國的分公司……電磁紀錄固然係存放於陶氏集團位於美國密西根州 Midland 市總部電腦及美國德州自由港（Freeport）電腦之伺服主機內，但在我國法域內，僅告訴人臺灣陶氏公司之特定員工（包括經陶氏集團指派到告訴人臺灣陶氏公司任職的員工），可經過授權後，透過員工編號下載並瀏覽，並且應為臺灣陶氏公司業務或經授權之目的，方得使用此等電磁紀錄，而該等員工基於此等電磁紀錄所創造的經濟利益，亦直接歸屬於告訴人臺灣陶氏公司。**又告訴人臺灣陶氏公司之員工，基於對於告訴人臺灣陶氏公司之忠實義務，並負有保護及不得無故取得上開電磁紀錄祕密之義務，且應接受告訴人臺灣陶氏公司之監督**，此觀被告簽立之僱傭契約書第 1 條……甚明，另於告訴人臺灣陶氏公司之員工離職時，告訴人臺灣陶氏公司亦有權限回收此等與公司業務相關的電磁紀錄……故如附表一所示之電磁紀錄，**其使用權限、財產價值及祕密性之法益，在我國法域內係受告訴人臺灣陶氏公司所管領，應可認定，亦即依一般交易或社會概念，有足使人認識告訴人臺灣陶氏公司事實上支配該等財產法益之客觀情事存在**。更何況，告

[168] 檢方認為被告另涉犯 92 年 7 月 9 日修正公布之著作權法第 91 條第 2 項之以重製方法侵害他人著作財產權罪，因非本文討論主軸，故謹此附帶說明之。

訴人臺灣陶氏公司作為陶氏集團的一部，其業務之榮枯、公司的發展，與陶氏集團之相關祕密資訊（包含以電磁紀錄形式存放之祕密資訊）不得遭無故取得有密切關係，是以在我國法域內，**告訴人臺灣陶氏公司對於無故取得存放於陶氏集團位於美國電腦之伺服主機內的電磁紀錄之行為，顯然不能謂係單純『利用權益』受到影響，亦不得謂係『間接或附帶』受害之人，而應認為係直接受有損害之人，得為告訴。**」[169]不採被告抗辯，判決被告涉犯第 359 條有罪。二審法院就此一部分認同一審法院見解，予以維持。[170]

然而，本案上訴到最高法院後，就此爭點並未進行指摘，於告訴乃論爭議部分，僅表示臺灣陶氏公司在刑事陳報書狀所為之陳述，似乎尚不足以認定其有提起告訴之意等，加以其他最高法院認為前審判決理由不備之爭點（例如第 359 條的損害認定等），撤銷原判決發回更審。[171]更（一）審法院就告訴乃論爭點並未做出新見解，維持一、二審看法，補強最高法院所指摘其他部分後，仍判決被告有罪。[172]

本案再次上訴到最高法院後，最高法院認為：「……刑事訴訟法第二百三十二條規定，犯罪之被害人得為告訴，所謂被害人，指因犯罪行為直接受害之人而言，至其他因犯罪間接或附帶受害之人，在民事上雖不失為有請求賠償損害之權，但既非因犯罪直接受其侵害，即不得認為該條之被害人。就財產犯罪言，固不限於所有權人，即對於該財產有事實上管領力之人，因他人之犯罪行為而其管領權受有侵害者，亦不失為直接被害人，而得合法提出告訴……原判決雖以台灣陶氏化學股份有限公司（下稱台灣陶氏公司）為美商陶氏化學公司（The Dow Chemical Company，下稱美商陶氏公司）在我國投資設立，屬美商陶氏公司之子公司，就存放在美商陶氏公司位美國密西根州密特蘭市（Midland ）總部電腦伺服主機內之中央報告系統（Central Report Index，簡稱 CRI）電磁紀錄，為**準占有人**，故得以其

[169] 臺灣台北地方法院 94 年度訴字第 1561 號判決。
[170] 智慧財產法院 98 年度刑智上訴字第 2 號判決。
[171] 最高法院 99 年度台上字第 4363 號判決。
[172] 智慧財產法院 99 年度刑智上更（一）字第 23 號判決。

管領權受侵害之客觀情事，認係直接受有法律上利益之損害，而得為告訴。然民法第九百六十六條規定：『財產權，不因物之占有而成立者，行使其財產權之人，為準占有人』，**亦即『準占有人』，必須是『行使其財產權』之人。**依原判決理由之記載，台灣陶氏公司員工申請下載並瀏覽 CRI 之查閱權，須由該公司將申請表格送至美商陶氏公司位於密西根州之 CRI 中心，經該中心將申請查閱者之員工編號登錄於『准許閱覽名單』後，該員工始可進入 CRI 資料庫查詢資料……被告指稱『查閱 CRI 資料庫電子申請單』明白記載美商陶氏公司之 Business Intelligence Center 有權隨時終止員工查閱 CRI 資料庫之權限。如果無訛，台灣陶氏公司人員得以其員工編號登入下載並瀏覽 CRI 資料，似係經美商陶氏公司准予列入閱覽名單後，始經授權而得查閱該項資料，既非因台灣陶氏公司之核准即取得瀏覽、下載之權，且經授權而取得查閱權，仍可由美商陶氏公司片面終止，**則能否謂台灣陶氏公司即係在我國法域內行使 CRI 電磁紀錄財產權之人？**實非無疑。而台灣陶氏公司員工經授權使用上開電磁紀錄所創造之經濟利益，**僅係結合 CRI 資料所衍生之間接商業收益**，既為台灣陶氏公司之營業所得，此一經濟利益自歸屬其所有，**亦非可執此遽謂台灣陶氏公司係行使 CRI 電磁紀錄財產權利之人。**又台灣陶氏公司為美商陶氏公司投資設立之子公司，是否為美商陶氏公司在台灣地區之**代理人**？其就美商陶氏公司之利益在我國法域內遭受侵害，是否曾獲**授權得代理該公司為訴訟行為**？除台灣陶氏公司係美商陶氏公司百分之百投資設立，而為其子公司外，兩公司間之關係究係為何？原判決並未進一步說明，此部分自屬未臻明瞭，本院尚無從為原審此部分適用法律正確與否之判斷。」[173]質疑更（一）審法院就臺灣陶氏公司以準占有人地位取得告訴權之論點不當，似已認定本案告訴權應歸屬於美商陶氏公司而非臺灣陶氏公司，因而撤銷原判決。

更（二）審法院之見解同於最高法院，指出本案臺灣陶氏公司並非合法告訴權人，而美商陶氏公司雖有派代表參與訴訟，惟按照卷證不能認其在時效內有提

[173] 最高法院 100 年台上字第 3375 號判決。

出告訴之意思。另外，更（二）審法院也從臺灣子公司無權代表其他所有美商陶氏企業下轄之子公司提起訴訟（本案系爭電磁紀錄中部分為其他子公司所有），以及相關授權合約、保密契約等均無從說明臺灣陶氏公司得代理美商陶氏公司為訴訟行為等角訴，認定本案告訴不合法，而為不受理判決。[174]檢方不服上訴到最高法院，雖爭執更（二）審法院對契約認定有誤，且美商代表所為陳述已足表達告訴之意思，另按照第 359 條立法理由解釋，其法益保護與資訊安全信賴有關，若斷定僅所有權人才有告訴權時將有違立法目的等抗辯，最高法院仍重申更（二）審見解，駁回上訴，本案至此判決確定。[175]

**三、判決簡評與討論**

最高法院對於告訴乃論之認定與相關論證嚴謹，可茲贊同。但從本案也可以發現，在資訊技術發達、跨國商業交流與拓展蓬勃的現今，許多電磁紀錄透過於雲端資料庫與網路技術進行儲存和處理，則在可預見的將來，恐怕需要透過更多實務見解的累積，才能較為清楚的釐清告訴權在跨國時代可能面臨的諸多難題。否則類似本案犯罪事實明確的案子，卻因為程序爭點造成受害人權益無從保障，恐非吾人樂見之事。

## （四）修法建議

第 361 條加重規定部分，則應視立法討論是否繼續保持公務機關的獨特性而作加重規範設計。[176]本文認為可參考德國刑法第 303b(2)和 303b(4)的加重要件，或美國聯邦刑法等等外國法例，對於不同情節而有其獨特保護必要性者，在刑度上作更精細的設計，會遠比粗糙的以公務機關電腦加重規定來的妥當。[177]例如本文

[174] 智慧財產法院 100 年度刑智上更（二）字第 11 號判決。
[175] 最高法院 101 年台上字第 5295 號判決。
[176] 有學者即批評對於公務機關電腦的加重規定事實上並無合理依據，對於公務機關須保護的獨特性缺乏合理論述，參李茂生，前揭註 30，頁 210-212。類似看法，參王銘勇，前揭註 75，頁 30-31；張紹斌，前揭註 62，頁 98-99。
[177] 例如美國法 18 USC § 1030(c) 便有對於不同情節的犯罪類型給予不同刑度的規定。*See generally* Chuck Eastton & Det. Jeff Taylo, *supra* note 48. 德國刑法 303b(2)和 303b(4)亦有類似規定，惟較美國法為簡單。可參葉亭巖，前揭註 66，頁 18-21。

前面所提及的大型網路服務供應者、企業、金融機構等等，因該等機關電腦中往往握有大量敏感資訊例如個人資料等等，倘若成為入侵行為的受害對象，甚至因而使其電磁紀錄遭到盜取時，因為該等機關的用戶數量龐大，其影響和受害範圍絕不僅只是該機關的個人法益而已。故此時要如何設計相對應的加重要件以及刑度，在在考驗著立法者的智慧與見解

至於第 363 條告訴乃論的規定，本文認為哪些罪名要維持告訴乃論之問題，仍應回歸保護法益的目的去作思考，不能僅因偵查困難、資源不足等現實理由，而使部分犯罪行為在可能牽涉複數被害人,且被害人中有直接與間接受侵害者時，因為直接被害人的怠於行使權利而使間接被害人受害。此種情況，特別是在牽涉電磁紀錄化的個人資料時特別是如此。故適當的將潛在被害人數量較多、可能涉及公共資訊安全等級的社會、國家法益之罪，將之設定為非告訴乃論，將追訴責任交給國家，或較能在資訊社會下提供真正有效的保護，也可以有效減少因為告訴權爭議造成犯行因程序要件而無法追訴的情形。

# 第五章 資訊刑法之定位與修法必要性

## 第一節 立法整合之缺失與資訊刑法之定位

本罪章所可能保護的法益事實上相當多元，從立法理由所主張的雙法益並重論，試圖藉此使多元保護法益兼容並蓄於一章，便可略窺一二。[178]概略言之，本章所可能保護的法益，實包括個人法益中的隱私秘密、財產利益，以及社會法益中社會對於資訊安全、個人隱私的合理信賴期待，甚至可能是國家安全的國家法益等等。[179]換言之，雖有論者提出本罪章不合刑法分則體系等批評，或認為新的工具與科技既然未產生新的法益，則應以過去舊有法規作解釋與涵攝為已足等負面評價。[180]

但本文卻認為，法律制度設計的初衷，本係為了解決人類社會生活所面臨的問題，當新的事務產生並伴隨了相對應的秩序破壞問題時，若舊有法令確實不能直接解決，則以新訂的法令去特別規制這新興的事務乃理所應然。透過這樣的方式，在解決新興問題的同時，其背後所代表的正是法益的維護。因此，本文以為前開諸多法益的共同交集，便是新興資訊平台（或稱虛擬世界等）的存在，為維護該平台的秩序，本罪章甚至本文所主張的資訊刑法，應是必須而必要的存在。

此外，在各類資訊的處理多已電子化的現代，事實上許多其他法律亦有針對電磁紀錄加以規範。[181]故許多本罪章所規範的不法行為，也可能同時觸犯其他法令，所以當本罪章之罪與其他法律間產生關聯與競合時，最關鍵的問題仍屬確定該罪名所保護的法益為何，才能妥善判斷法條間應如何競合，並讓該行為以正確的罪名妥適評價。[182]在現行法法益有所爭議的前提下，顯然在此種與其他附屬刑

---

178 參前揭註 58。

179 張紹斌，前揭註 62，頁 90。

180 鄭逸哲，前揭註 31，頁 105-108。

181 例如 2012 年 10 月 1 日起甫開始施行的個人資料保護法便係一例，由第二條規範用詞顯已經將電磁紀錄的收集、處理等等納入考量。

182 類似見解可參林孟皇，前揭註 101，頁 91-92。該篇文章主要提到本章之罪與著作權、營業秘密保護等法規產生關聯時，要能正確適用法規的前提仍係先釐清法益問題。

法重疊的情況下，有不利於競合判斷的因素，而有待修法或立法改進。

再者，刑法對於犯罪行為與罪責的評價，係可透過相對應的刑度作反映的，此即罪刑相當原則。[183]也就是說，刑度設計是否能恰當反應犯罪行為的嚴重性，對於刑法的運作而言實事關重大。本章各罪立法時，雖有許多行為態樣與刑法原有罪名類似，但刑度設計上似乎因為立法考慮不周，抑或是法益定義不明等原因，造成刑度設計不盡合理。[184]在許多附屬刑法相繼修法或訂定的現今，妨害電腦使用罪章修法近十年後卻未有相對應的修正，顯然也是需要檢討的問題。

本文所期許的資訊刑法，是透過修訂新法的方式，將現行妨害電腦使用罪章修正後移出刑法分則，除能避免破壞刑法分則體系外，也透過建構資訊平台刑事專法的方式，將各種與資訊平台相關、法益各有不同的基本刑事法規納入其中。在與其他法令競合的問題，則係將資訊刑法作為所有牽涉資訊平台的刑事基本法，其他法規（例如：個人資料保護法等）則作為特別法，清楚劃分其分際。此種普通法與特別法間層次分明的界定，能透過基本法作為資訊平台的基礎刑事規範，特別法則強調其特別保護的目的與法益。修訂此新法的同時，也能同時檢討相關的刑度設計，妥適給予正確刑度規定來評價不同嚴重程度的犯行。

時至修法後近十年的今日，我國妨害電腦使用罪章已顯得陳舊而有待檢討，前開各項缺陷，都在在凸顯了修法改革的迫切必要，本文則進一步認為，若能趁機建立起屬於我國資訊刑事法規的嶄新完整架構，必能化眼前危機為絕佳轉機。

本章次節，將透過所搜尋到妨害電腦使用罪章與其他法令有關的判決，來觀察實務所面臨的問題。

[183] 林山田，前揭註 39 書，頁 92-93。
[184] 刑度的例子可參考前揭註 96。

## 第二節 與其他法律相關之判決[185]

### （一）判決個案分析：與個人資料保護法相關判決

#### 一、判決事實與爭點

實務上與個人資料保護法（舊法名稱：電腦處理個人資料保護法）有關的判決，主要係與本章第 361 條公務機關加重規定，以及第 363 條告訴乃論規定有關。本文搜尋到的兩件案件，均屬被告對學校犯第 358 條無故入侵他人電腦罪（其中一件尚涉犯第 359 條無故取得電磁紀錄罪），檢方按照第 361 條對公務機關犯本章之罪起訴。在實務認為本章之罪經第 361 條加重後屬另一罪名，無須告訴乃論之見解下，**法院引述第 361 條立法理由為佐證，認定當被害者係學校時，因其不合於公務機關之範圍，無法適用第 361 條，仍須按照第 363 條告訴乃論規定處理，若未合法提起告訴，法院將依法為不受理諭知。**[186]

#### 二、法院見解

臺灣高等法院高雄分院 101 年度上訴字第 529 號判決中，法院認為：「至於刑法第 361 條：『對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一』之罪，固非屬告訴乃論之罪。唯刑法第 361 條之立法理由已載明『**本條所稱公務機關，係指電腦處理個人資料保護法第三條所定之公務機關。**』，酌以電腦處理個人資料保護法第 3 條第 6 款：『公務機關：指依法行使公權力之中央或地方機關』、第七款：『非公務機關：、、(二)、醫院、學校、、、』規定，則公立學校顯非刑法第 361 條之「公務機關」。」[187]亦即法院認為，第 361 條公務機關的判斷準則，按照立法理由所述，應參酌《電腦處理個人資料保護法》（亦即《個人資料保護法》）中對於公務機關與非公務機關的定義。

---

[185] 至於本章與刑法其他罪章之競合與重疊，可詳參蔡蕙芳，前揭註 35，頁 66-78。

[186] 本章之罪經第 361 條加重後，屬於非告訴乃論之罪的實務見解，可參本文第四章第五節。

[187] 臺灣高等法院高雄分院 101 年度上訴字第 529 號判決。臺灣高等法院高雄分院 95 年度上易字第 872 號判決有類似見解。需注意者，係此二判決所引用條文皆為舊法，新法《個人資料保護法》第 2 條：「本法用詞，定義如下：……七、公務機關：指依法行使公權力之中央或地方機關或行政法人。八、非公務機關：指前款以外之自然人、法人或其他團體。」其中已將舊法例示指明學校為非公務機關之規定移除。

其次，法院在判決中說明《電腦處理個人資料保護法》第 33 條之罪屬於告訴乃論，而《刑法》第 358、359 條亦同。鑑於刑法妨害電腦使用罪章的立法理由說明，就告訴權歸屬問題，法院認為：「……應認**電腦之使用人才是上開二條文之直接被害人**。是以本案入侵附表三之(一)至(十二)所示學校之電腦，取得電腦內有關學生資料之電磁紀錄，遭入侵之學校固為刑法第 358 條、第 359 條之直接被害人，而為有告訴權人。但各該遭入侵之電腦既未供學生使用，學生自非遭入侵之學校電腦的使用人，因此本案之學生顯非刑法第 358 條、第 359 條之罪的行為客體及立法理由所欲保障之人，而非屬刑法第 358 條、359 條規定之直接被害人，亦即並非有告訴權人。**至於涉及電腦處理個人資料保護法第 33 條部分，則應認學校及學生均為有告訴權人無訛。**」[188]似認為第 358、359 條從立法理由觀察，其立法目的以**保障使用人所使用之電腦系統安全性**為主，因此告訴權歸屬於電腦使用人；反之，電腦處理個人資料保護法之規範，**重在電子化個人資訊的保護**，因此一旦被入侵及不法取得後，受害者當然是被入侵電腦之所有者，以及被不法取得資訊者，此時學生（資訊被不法取得的被害人）自然也有告訴權。最後，法院排除了按照上述見解未合法告訴的部分，將被告所涉犯刑法第 358、359 條及電腦處理個人資料保護法第 33 條三罪，依想像競合從一重處斷予以判決。

## 三、判決簡評與討論

從本案法院的思考脈絡中可以發現，不同法規所主要規範的目的本不一致，但有時一行為卻可能同時該當不同法律中的犯罪，此時若牽涉被害人的判斷以至告訴權的歸屬等問題時，自然應依該不同法律所規範的主要目的為斷，去篩選出該法律訂立時主要保護的對象，以作成正確的判斷。此一思考脈絡，本文相當贊同。

但是，本案法院之思路，似乎在第 359 條的認定上有所盲點。第 359 條確實與使用電腦之資訊安全相關，但直接受到犯罪行為所攻擊者確非抽象的資訊安全，

[188] 臺灣高等法院高雄分院 101 年度上訴字第 529 號判決。

而是電磁紀錄。如同本案之事實中，因被告所取得之電磁紀錄實與個人資料有關，此時被竊取個人資料既然是學生，則從該被竊取之電磁紀錄的實體內容判斷，這些學生似仍不無同時被判定為直接受害者的空間？畢竟第 359 條所攻擊的客體並非「電腦」而係「電磁紀錄」，則此時直接受害者的判斷上，本文以為似乎仍要參酌該電磁紀錄的內容去斷定，較能全面的保障國民，否則至少在個人資料被盜取的問題上，若保存電磁紀錄的機關怠於追訴時，對於個人資料被盜取的被害人而言，保障實有不周。

本文所主張的資訊刑法，其主要的規範目的，便係作為以資訊空間作為生活平台的刑事基本法規，在發生不同法規競合時，其他有特殊目的（例如保護個人資料等）之法規可依特別法優先於普通法之概念適用，如此一來可透過資訊刑法將一般性資訊平台的刑事問題作基本規範，再按照個案是否同時涉及其他特殊目的（法益）去作適當的競合，應較能組織出完整的刑事法規網絡。

## （二）判決個案分析：與營業秘密法相關判決[189]

### 一、判決事實與爭點

本案事實略謂：被告某甲原任職晨星半導體股份有限公司，後轉任職於聯發科技股份有限公司，與聯發科公司簽有聘僱契約書，依約負有保守因業務所知悉或持有工商秘密之義務。然其利用職權，將所得接觸之電磁紀錄資訊，即 MT8201A 型號生產時程表透過電子信箱寄送給已離職轉至競爭對手公司工作的前同事。其後，被告某甲從聯發科離職，仍儲存與其職務相關之晶片工商秘密電磁紀錄，供其後工作使用，並將其於聯發科任職期間所獲取關於大陸市場發展之相關報告檔案洩漏於其後工作之公司。被告尚將聯發科任職期間獲取之聯發科公司晶片之線路設計圖及搭配電路板含料成本洩漏給其後任職公司等。檢方以被告涉犯洩漏工商秘密罪、背信罪、無故取得他人電磁紀錄等罪起訴。

從前開事實可以得知，**本案主要牽涉的是洩漏工商秘密罪**，而法院在判決中，

[189] 臺灣台北地方法院 97 年度易字第 500 號判決。

特別花了相當篇幅**說明我國法有關營業秘密之定義與保護規範、營業秘密與刑法上工商秘密之異同、刑法第 359 條無權取得電磁紀錄罪之規範意旨與法律適用等問題**。

**二、法院見解**

首先，法院由營業秘密之定義出發，認為：「按營業秘密價值乃在其秘密性，營業秘密一旦被揭露，其經濟價值即將銳減甚至消失，此即所謂『一旦喪失就永遠喪失』（once lost,is lost forever ），故營業秘密所有人如有保密之意圖，且已採取合理之保密措施，以維護其秘密性，而將營業秘密『合理揭露』提供予特定之他人，不論係基於事業活動之信賴關係或僱傭、銷售等契約中之保密條款，仍不失其秘密性，顯見**營業秘密之秘密性，係屬相對，而非絕對**。」但各國要採用民事責任、刑事責任或兼採兩者以保護營業秘密，係屬立法政策，並非絕對。而我國法就此一問題，係將行政及刑事責任規範於刑法、公平交易法中，營業秘密法則採民事責任之立法方式，屬於民法之特別法。

然而，刑法中所謂「工商秘密」，由其立法背景觀察，當時似並無營業秘密之概念，所謂工商秘密「應係指工業或商業上之發明或經營計劃具有不公開之性質者，均屬之，舉凡工業上之製造秘密、專利品之製造方法、商業之營運計畫、企業之資產負債情況及客戶名錄等，就工商營運利益如屬不能公開之資料，均屬本罪所應加以保護之工商秘密」。換言之，**工商秘密與營業秘密兩者在概念上並不完全重疊**。

再者，法院從電磁紀錄概念之流變，引出第 359 條無故取得他人電磁紀錄罪，其實是考量電磁紀錄的可複製性等與傳統動產不同之特性，而設計來用以取代舊刑法第 323 條竊取電磁紀錄罪。法院接著指出：「而營業秘密法所保護之營業秘密，其實即為『資訊』，因此營業秘密法第 2 條有關『營業秘密』之定義，即為：『方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊。』**如電磁紀錄上承載著受著作權或營業秘密法所保護之資訊，則未獲同意無權複製**

**他人電磁紀錄之行為，即會侵害電磁紀錄所呈現出無體資訊之『資訊之專屬性或排他性使用』（the exclusive of informatiom），此種財產上利益侵害即為舊刑法第 323 條電磁紀錄竊盜罪所要規範者。**」而論及刑法妨害電腦使用罪章修正時，並不因電磁紀錄本身是否具有財產價值為斷，對於電磁紀錄的保護作一致性的規範，避免與電磁紀錄相關的法益（包括財產或其他類型）受到不法侵害。法院認為，新法所保護法益與舊法（竊取電磁紀錄罪）目的與保護法益並不完全重疊，此種立法政策，法院認為其妥適性頗有疑義。

最後，法院重申第 359 條無故取得他人電磁紀錄罪，「係以無權侵入系統為前提，由此而接觸、刺探到未獲授權存取之電磁紀錄，並將電磁紀錄予以複製而言。」**若係原有權限接觸該電磁紀錄者，取得後做權限目的外使用，並不在本罪規範範圍內**。法院藉此說明，就保護與營業秘密有關之電磁紀錄的角度來說，刑法條文（洩漏工商秘密罪、無故取得他人電磁紀錄罪等）並不能提供完整的保護，較佳的方式係按照著作權法的立法方式，針對營業秘密的性質設計相對應的刑事規範，方稱妥適。就結論而言，法院認為被告某甲之行為並不該當第 359 條無故取得他人電磁紀錄罪。

**三、判決簡評與討論**

本案中，法院對於營業秘密、工商秘密與無故取得他人電磁紀錄罪，有著體系化的清楚論述。特別是法院認為關於第 359 之適用上，「若係原有權限接觸該電磁紀錄者，取得後做權限目的外使用，並不在本罪規範範圍內」，清楚點出 359 條之無故取得他人電磁紀錄罪之判斷，係以行為人**是否具有合法權限**取得該電磁紀錄而言，而與其取得電磁紀錄後之行為無涉，論理可茲贊同。因此，若欲以第 359 條保護營業秘密不致外洩，僅能規制本無權限接觸（取得）該營業秘密者，而不及本有合法權限接觸該營業秘密卻進行洩漏等損害公司作為者，保護效果不足。因此，本文在此同意法院見解，認為若立法者認為需以刑事罰規制洩漏營業秘密之行為，則應量身打造相關法令方能有效進行規範。

我國刑法第 359 條之規定，實質上針對的無非是「無權」取得、變更或刪除他人電磁紀錄的行為，撇去實害認定的爭議不談，從本文第四章第二節各實證案例，即可得見其實務運作效果。第 359 條適用在商業經營領域時，大多是離職員工或競爭對手以損害公司為目的取得、變更或刪除電磁紀錄。在電磁紀錄的保護上，刑法係以「無權」作為核心進行規範，以本案來說，若行為人係公司低級員工，在離職前透過某些方式取得有關營業秘密的電磁紀錄，其後進行洩漏，此時因為該職員本無合法權限取得該電磁紀錄，則可能得以適用無故取得他人電磁紀錄罪進行規制；相反地，在行為人本有權存取該電磁紀錄的前提下，單純的取得行為原則上是合法的，要處罰的重點是洩漏出去的行為，此時就不在無故取得電磁紀錄罪的射程範圍內了。

在本文的認知中，**資訊刑法所扮演的角色，便係建立典型、核心的普遍性資訊保護規範，作為所有資訊平台行為的基礎刑事法典。**以取得電磁紀錄的行為來說，「無權」便是典型而核心的類型，所著眼的保護標的是高位的資訊安全，其範圍可能囊括了隱私、營業秘密、財產等等不同法益，但並不側重於其中任一法益，而係透過資訊安全作為交集建立的普遍性規範。此時，若吾人將保護標的縮小到保障營業秘密的範疇時，資訊刑法所規制到的範圍僅及於典型、核心的「無權取得」營業秘密之犯行，倘若立法者認為保護範圍過於狹窄，應就保護營業秘密為目的的法規（營業秘密法）設計相對應的刑事規範，例如洩漏營業秘密罪等，透過在對於營業秘密的特化保障，將原本在資訊刑法中被歸類為非典型的行為態樣加入規範。透過此種特別刑事法規（營業秘密法）架構在普通刑事法規（資訊刑法）的架構，就能建立出層次井然、輕重分明的刑事規範，這也是本文的願景。

## （三）判決個案分析：與電信法相關判決[190]

### 一、判決事實與爭點

[190] 本案歷審判決為：臺灣板橋地方法院 91 年度訴字第 1028 號判決、臺灣高等法源 93 年度上訴字第 1882 號判決、最高法院 98 年度台上字第 2702 號判決、臺灣高等法院 98 年度上更（一）字第 312 號判決、最高法院 98 年度台上字第 6731 號判決。

本案事實略謂：被告某甲與其弟某乙為稹捷實業股份有限公司（下稱稹捷公司）之股東，某甲並兼任董事及工程部經理，與名義負責人某丙均為該公司之實際負責人。稹捷公司設置**專供本身業務使用之郵件伺服器**（主機名稱為caster.com.tw，ＩＰ位址為 210.64.71.131 ）之專用電信設備，以供公司員工與客戶間商業往來、公司內部公文等業務往來電子郵件之傳輸。某甲離職後，為取得稹捷公司之營業祕密，竟與某乙共同策劃，由某乙依據某甲於擔任稹捷公司之董事時所持有該公司員工之電子郵件信箱帳號及密碼表，分別由某乙在**民國 90 年 5 月到 6 月間**於多個不同時地，以電腦連結網路上網，進入稹捷公司郵件伺服器內欲登錄閱讀電子郵件信箱內之電子郵件，而以非法之方法連續侵犯稹捷公司通信祕密行為，但均未能成功而不遂。

首先應注意者，係本案犯罪時間係在妨害電腦使用罪章修正之前，檢方似因未有其他條文可供運用，而以被告共同連續違反專用電信處理之通信，即不得以非法之方法侵犯他人通信祕密未遂罪起訴。因此本案爭點相當單純，即被告之行為是否該當電信法不得以非法之方法侵犯他人通信祕密未遂罪？對此，一、二審法院均判決被告有罪。

**二、法院見解**

然而，本案上訴三審後，最高法院認為：「電信法所稱之**電信**，依該法第二條第一款之定義為：**指利用有線、無線，以光、電磁系統或其他科技產品發送、傳輸或接收符號、信號、文字、影像、聲音或其他性質之訊息。**而所謂**專用電信**，依同法條第六款（九十一年修正前為第五款）之定義為：**指公私機構、團體或國民所設置，專供其本身業務使用之電信。**交通部依電信法第四十七條第三項訂定之『專用電信設置使用及連接公共電信系統管理辦法』第三條規定：專用電信依其申請設置系統或目的分類如下：一、專用有線電信。(一)有線載波電台。(二)光纖傳輸電台。(三)專設有線電台。二、專用無線電信。(一)船舶無線電台。(二)航空器無線電台。(三)計程車無線電台。(四)學術試驗無線電台。(五)業餘無線電台。

(六)漁業、電力、警察、消防、鐵路、公路、捷運、醫療、水利、氣象及其他專供設置者本身業務需要而設立之專用無線電台。由上開規定以觀，**電信法規範之電信，簡言之，指有線電信或無線電信。**至於**電子伺服器，則屬與網際網路相連，供電子郵件存取之『電腦資訊處理設備』，而非屬電信法規範之客體，入侵他人之電子郵件伺服器，就現行法，屬刑法分則第三十六章所定妨害電腦使用罪章中第三百五十八條之無故入侵電腦罪之範圍。**……而法務部部長於修法提案報告中除說明上開立法理由外，並稱：對於無故入侵使用電腦之行為，我國現行刑法未有相關處罰之規定，因此年（九十二年）三月二十八日建中學生入侵總統府網站事件，現行法並無處罰依據，成為電腦網路犯罪規範上的一大漏洞，此又再度突顯本草案之重要性等語可知(以上見立法院公報第九十二卷第二十九期第一三0、一三九、一四0頁）。另依卷內交通部電信總局九十三年十月十二日電信公字第0九三0五0八一七八0號函稱:『電信法第六條係為落實秘密通訊自由之保障，特明定他人不得以盜接、盜錄或以其他非法之方法取得電信事業及專用電信所設置電信機線設備或電信設備傳輸之通信內容。**一般民間或企業自行假設用以存取電子郵件存取之電腦資訊處理設備，如非屬電信機線設備或電信設備，則其內之電子郵件自非電信法第六條第一項所規範之客體。**』等語，則入侵他人之電腦之行為，是否屬電信法規範之犯罪行為？攸關法律之適用，自應予釐清。原審對此未詳查究明，僅於判決理由謂：告訴人稹捷公司所設置之電子郵件伺服器係專供該公司本身業務使用之電信，自屬電信法第二條第六款所規定之專用電信云云(原判決第十三頁第九至十七行，第二十三頁第一行以下），據以論處上訴人等二人以電信法第五十六條之一罪，能否謂為適法，饒堪研求。」[191]

最高法院在前開論述中，認為本案被告所為侵入電子郵件伺服器之行為，按照（當時）現行法規應屬於妨害電腦使用罪章的規範範圍，且引用立法理由、相關函釋等，說明電信法規範客體並不及於電子郵件伺服器，因而撤銷前審判決，

[191] 最高法院 98 年度台上字第 2702 號判決。

發回更審。更審法院全盤引用最高法院論述，判決被告無罪。[192]檢方雖不服上訴，最高法院仍維持前次判決見解，認為本案被告之行為應依妨害電腦使用罪章之罪名處斷，但因犯案時間早於該章修訂之前而無法適用，駁回檢方上訴。[193]

**三、判決簡評與討論**

本判決中，最高法院認為被告入侵他人電子郵件伺服伺服器之行為，並不該當電信法妨害專用電信通信秘密之罪，無非是以電信法第 2 條第 1 款電信之定義、主管機關交通部所訂定之相關管理辦法、函釋等為依據，認為私人電子郵件服務不屬於電信法規範之範圍，該電子郵件伺服器亦非電信設備。事實上，本文以為檢方之所以會以電信法為依據起訴，誠乃當時我國法律落後尚未有入侵電腦罪之條文，無從處罰其入侵郵件伺服器之行為。惟令人疑問者，係當時刑法第 323 條準動產之規定尚將電磁紀錄納入其中，被告未能成功取得電子郵件內容之行為，應有成立竊取電磁紀錄未遂罪之空間，則為何檢方未按此處理，反罕見的引用電信法條文，實令人費解。

其次，按電信法第 6 條第 1 項：「**電信事業**及**專用電信**處理之通信，他人不得**盜接**、**盜錄**或以**其他非法之方法**侵犯其秘密。」又該條罰則訂於同法第 56-1 條：「違反第六條第一項規定侵犯他人通信秘密者，處五年以下有期徒刑，得併科新台幣一百五十萬元以下罰金。」其保護客體係電信事業或專用電信所處理之通信。本案被侵入之郵件伺服器屬於私人公司所有，並非電信事業；而觀察電信法第 47 條第 1 項：「專用電信須經交通部核准發給執照，始得設置使用。」及第 2 項前段：「專用電信不得連接**公共通信系統**或供設置目的以外之用。」由該私人電子郵件伺服器除提供公司內進行信息交換外，公司內部亦可透過該郵件伺服器連接網際網路與外部進行通信，應非屬專用電信之範疇。由此觀之，最高法院說明篇幅雖少，且僅只於對電信法中所謂電信定義作解釋，但就結論而言仍屬正確。

由這個案例也可以發現，當社會與科技隨著時代進步時，立法者本應注意時

[192] 臺灣高等法院 98 年度上更（一）字第 312 號判決。
[193] 最高法院 98 年度台上字第 6731 號判決。

代的變遷，使相關法令得以與時俱進；縱然未能領先社會變遷，先行建立相對應的法律規範，在司法判決揭露現行法之不足後，仍應即時反應，否則必然造成規範上的空窗期，讓投機人士有機可趁，非國民之福。

## 第三節 小結：修訂資訊刑法之展望

從前開判決個案分析中可以發現一個共通問題，亦即諸多法律保護核心與目的可能各不相同，但在資訊科技作為人類社會活動所必須的工具時，**縱然各法律規範目的與核心互有歧異，最終仍會因為人類活動中均使用資訊科技進行相關運作，而必須在「資訊安全」此一概念下匯流，不得不面對與刑法妨害電腦使用罪章發生競合與關聯的情況。**不同法規間因為修訂時間各異，草擬之機關不同，考量重點有所差異，故範圍之重合與銜接往往容易肇生問題，而有待立法者修法填補。

舉例來說，妨害電腦使用罪章中第 361 條「公務機關」的判斷，便借用了電腦處理個人資料保護法之規定，而不獨立做出定義，其初始目的推測應係避免不同法規間定義出現落差，而產生法規適用的灰色或空白地帶。但是，在個人資料保護法修正後，對於公務機關的定義有所更動，雖然實務上目前尚未出現與本章第二節第一段判決論述相類似的問題，卻難保在妨害電腦使用罪章久未修正的前提下未來不會致生相關爭議。故本文以為，在某一法律修正時，與其相關的法規本應一併修正檢討，避免出現法規間銜接產生漏洞或模糊地方，乃係當然之理。

其次，另一與前開論及法律保護核心與目的不同有關者，乃係**相關罪名的刑度檢討**。舉例來說，現行個人資料保護法第 42 條：「意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。」與刑法妨害電腦使用罪章第 359 條：「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。」不僅規定

相仿，行為人在一行為中同時觸犯前開兩罪之情況亦非屬少見，但刑度上除併科罰金額度之加重外，個人資料保護法第 42 條之刑度與刑法第 359 條實別無二致。然而，若將個人資料保護法第 42 條之性質定性為刑法第 359 條之特別規定，則此時其刑度差異似無法彰顯個人資料保護法之特定目的，難以反映特別目的之刑事規範所欲保護法益之特殊性，是否合於罪刑相當性乙節實令人存疑。

再者，資訊相關的刑事法令所針對的受害客體，均不脫「電腦」與「電磁紀錄」兩者，但所要保護的核心與法益其實各有不同，兼以法令設計時可能為了集中司法資源、尊重被害人自主決定等考量，而有告訴乃論之規定。此時，**各法律保護核心各異，又兼有告訴乃論與告訴權歸屬等議題交互參雜**時，就容易產生如同本章第二節第一段的案例中，受害學生僅可以電腦處理個人資料保護法第 33 條提起告訴，卻無刑法第 359 條之告訴權，在未能考量受害電磁紀錄之內容歸屬之思維下，可能有保護不周的問題。雖電腦處理個人資料保護法與刑法妨害電腦使用罪章規範目的有所差異，但是就電磁紀錄保護與受害人判斷等攸關告訴權歸屬之問題，似仍有斟酌空間，由此可得見現行妨害電腦使用罪章立法時的思維已顯有過時的跡象，若再加上與其它保護目的不同的法規間競合牽扯，問題只會更加複雜難解，而有待檢討。

立法的整合是牽連甚廣的大工程，然而資訊時代的來臨，讓各種法規與資訊刑法間，必然有所重疊與競合，則此時縱然立法整合牽連甚廣而艱難，仍係當局應正視並妥善解決的難題。本文認為，現行刑法妨害電腦使用罪章引致諸多學界及實務批評，由前開討論也確實可以發現立法技術與法規制度落後等問題，而有修法的必要，不如將此危機化為轉機，一舉訂立資訊刑法。

資訊刑法的優勢，可使資訊系統犯罪（包括電腦及網路犯罪）現有的條文作系統性檢討。透過特別法的修法，可以擺脫刑法分則罪章必須有共通法益的限制，維持刑法體系的完整性。除了能重新界定規範對象與範圍之外，還能同時確立各罪各自的保護法益與對應的構成要件，並且檢討應有的刑度。**此種以資訊安全為**

**核心的特別刑法，以所有資訊相關刑事規定交集的「資訊安全」為主軸，使相關的附屬刑法均能奠基於其上，清楚宣示與其他法規的關聯性與重疊關係**。

在刑度的設計上，立法時可重新檢視刑法與其他附屬刑法中相關的刑度規定，分層劃定不同行為態樣與嚴重程度之犯罪所對應的刑度，落實罪刑相當原則，應是可以進行的方向。特別是在同一受害客體（例如內容為個人資料的電磁紀錄遭到不法刪除），但不同法令保護重心不一的狀況（例如刑法第 359 條與個人資料保護法第 42 條）時，尤應特別考慮各法令的位階與保護法益的高低，才能透過良好的刑度設計正確的評價該犯罪行為。因此，**本文以為刑度的通盤檢討，會是支持本文資訊刑法立法主張的另一優勢**。

此外，值得順道一提的是，本文認為相關配套措施也能藉此機會檢討與建構，諸如檢討行政法上對於掌握他人電磁紀錄的公私機關，是否應該課予相對應的強化資訊保全責任；廣參各國相關法規與公約等，除了前開實體法的檢討外，亦可同時檢討程序法、司法互助等法令，在網路無國界的時代，才能真正落實資訊安全的完整保障。[194]簡言之，**資訊刑法立法的第三個優勢，便是關於資訊安全的程序法、行政管制與司法互助之規定，亦可同時進行討論與規劃**。此節因超出本文所討論之主軸，僅能在此簡單點出而無法多作討論。

總的來說，本文的構想是將資訊刑法作為整合性的基礎刑事法令，建構與現實社會刑事法平行的規範。[195]對於刑法來說，它是針對資訊領域特別設計的刑事特別法；但對於其他牽涉資訊平台的法令，例如個人資料保護法、智慧財產權相關法令等而言，它則是最基本的刑事法規。[196]換言之，若某一個案同時涉犯個人

---

[194] 事實上，本章修法研修會議時，便有實務工作者認為程序法問題嚴重性並不亞於實體法，惟至今似乎未有相對應的修法。參法務部，前揭註 2，頁 5。此一部分已經遠遠超出本文研究範圍，惟為了論述的完整性，特別在此提出，期許未來學界能就此作更深入的研究與探討，為我國建立完整資訊法規架構貢獻心力。例如歐州理事會《網路犯罪公約》中，便按照實體法、程序法、司法互助之順序，對網路犯罪法規做出層次分明的架構模型。《網路犯罪公約》介紹可詳參馮震宇，前揭註 21，頁 124-136；馮震宇，「網路犯罪與網路犯罪公約（下）」，月旦法學教室，第 5 期，2003 年 3 月，頁 115-124；廖宗聖、鄭心翰，前揭註 75，頁 61-66 等。

[195] 理想上資訊刑法尚應考量資訊刑事案件性質，去設計相關的程序法以至司法互助等制度，方能真正完整的建構出資訊刑事法規範。

[196] 我國與電腦犯罪相關的法規甚多，此處僅聊舉數例，體系與法規可詳參黃宏全，「電子商務之

資料保護法與資訊刑法的刑事規範時，例如個人資料保護法第 42 條與無故變更電磁紀錄罪，應依特別法優先與普通法的原則，優先適用個人資料保護法；反之，在非個人資料保護法範圍的案件，則適用資訊刑法處理。[197]此種設計的目的，係希望透過資訊刑法先架構出最基礎的資訊領域刑事規範，而將有特別規範目的或保護標的的法規建構在其上，將規範所及囊括整個資訊社會，構築完善的刑事架構與保護。



刑事侵權－妨礙秘密罪與電腦犯罪」，法務部，刑事政策與犯罪研究論文集（14），頁 107-108；蔡蕙芳，前揭註 24，頁 176-185。

[197] 個人資料保護法第 42 條：「意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。」

# 第六章 結論

電腦與網路的發明時間雖短，卻已經迅速深入了人類社會的各個角落，這些年來已然形成了一個存在虛擬空間，也就是本文所稱的資訊平台。與真實社會緊密連結的網路世界發展蓬勃，更已跨越國際的地理限制，聯繫了全球各地的許多資訊平台，人類的生活型態短時間內勢必難以脫離電腦與網路而生存。然而，此種與現實社會緊密相關，卻又並非全然重合的社會結構若要能持續發展並保持安定，勢必要妥善解決新興資訊犯罪帶來的問題。基此，規範資訊犯罪的刑事法令，確實有其存在的必要與價值。

我國基於此種世界潮流所趨，在 2003 年進行了大規模的刑法〈妨害電腦使用罪章〉修訂，可說是跨出了建立刑法系統規範正確的第一步。[198]然而，從學說上的論述外、國法例的比較與討論，到實務運作結果中，吾人都可以發現本章的不足之處；不論從規範對象與範圍、保護法益、構成要件，以至立法技術與整合立法等層面，都仍有相當大的改進與檢討空間。由此觀之，我國距離建立完善的資訊刑法體系，還有待各界集思廣益，才能順利走過整合立法的漫漫長路。

本文第二章「從定義談起」，先介紹了學界對於電腦犯罪與網路犯罪定義的眾說紛紜，並提出本文所主張之「資訊犯罪」，其核心係指利用**資訊科技特質**進行犯罪者而言。其次，本文本於鑑往知來的想法，介紹了我國刑法關於資訊犯罪的相關修法歷程，並且提出相關判決個案進行討論。接著針對我國妨害電腦使用罪章並未清楚定義其法條結構中所使用到的重要詞彙作利弊解析，而得出應以抽象定義劃定規範目的與範圍之結論。

第三章「保護法益的爭議」，則從立法者、學說以及實務等眾家見解談起，介紹本罪章從立法之初便引起熱烈討論的保護法益爭議。接著本文就針對學者以法解釋學方法主張本罪章保護社會法益之見解，以及德國法將相當於本罪章各罪

[198] 有論者以為，該次修法結果事實上多屬政策性條文，本文對此相當認同，也因此才具有相當大的討論與改進之價值。參曾淑瑜，前揭註 77，頁 167。

散置在個人法益各章中之個人法益見解，做出相對應的討論與評析，並嘗試以法院依個案情節解釋做為法益爭議的近程解決方案，以及修法的遠程解決方案。

第四章「構成要件的檢討」，係以逐條討論之方式，除介紹學說上所認為的法條設計缺陷外，分別挑選了與各條相對應的實務判決解析作為佐證，並以本文所主張修法的個人、社會法益雙重並列法條結構為原則，提出各條文可能的修正方向。

第五章「資訊刑法之定位與修法必要性」，則是將視角從刑法妨害電腦使用罪章提高到刑法與其他附屬刑法的關聯層級，分析出現行法令主要的缺失在於立法的整合性不足、法規設計過時、各法令關聯與競合易生爭議以及刑度設計有不符罪責相當原則之虞等問題，最終提出本文所期望的整合性資訊刑法，作為所有資訊平台刑事法令的基礎，建立清楚的分層架構，方能妥適保護我國資訊安全。

最後，本文在此再次強調，本文以為我國應透過資訊刑法的立法，解決現行資訊系統犯罪的規範與刑法原有體系的緊張關係，也可同時達成條文結構的檢討、構成要件的修正、通盤檢討刑度的高低、界定各法律間的關係等等；並且透過相關配套措施，例如行政法上強化以持有電磁紀錄之公私機關的資訊保全義務，檢討資訊系統犯罪的程序法、司法互助等法規，全面性強化我國對於資訊系統犯罪的規範，與世界各國法規接軌，共同打擊全球化框架下的資訊系統犯罪，應不失為可能的解決方案。

# 附錄：本章條文修正方向建議

| 現行條號 | 現行法構成要件 | 建議修法構成要件<br>（以個人法益的構成要件為例，第362條部分則係社會法益之條文） |
|---|---|---|
| 358 | 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。 | **未獲授權**或**逾越授權範圍**而入侵他人電腦系統或其相關設備者 |
| 359 | 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 | 無故**取得**他人電腦系統或其相關設備之電磁紀錄，**足以**生損害於他人 |
| | | 無故**刪除**他人電腦系統或其相關設備之電磁紀錄，**足以**生損害於他人 |
| | | 無故**變更**他人電腦系統或其相關設備之電磁紀錄，**足以**生損害於他人 |
| 360 | 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 | 無故藉由輸入指令、傳輸資訊、損害、刪除、效能減損、變更、阻礙、使之難以存取或其他相類之方式干擾**他人電腦系統或其相關設備** |
| | | 無故藉由輸入指令、傳輸資訊、損害、刪除、效能減損、變更、阻礙、使之難以存取或其他相類之方式干擾**他人電磁紀錄** |
| 361 | 對於公務機關之電腦或其相關設備犯前三條之罪者 | 對於公務上使用之電腦系統或其相關設備犯……之罪者 |
| | | 對於公務上使用之電磁紀錄犯……之罪者 |
| | | *（針對**私人企業、網路服務供應商**等劃定階級標準，達某一標準後給予相對應加重刑度）* |
| 362 | 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 | 因故意或過失使自己製作之有害電腦程式散播，**致生資訊安全之公共危險者** |
| 363 | 第三百五十八條至第三百六十條之罪，須告訴乃論 | *（個人法益之罪部分維持告訴乃論）* |

# 參考文獻


**中文書籍**

林山田，《刑法各罪論》，上冊，五版，2005 年，台北。

林山田，《刑法通論》，上冊，增訂十版，2008 年 1 月，台北。

法務部，《刑法有關電腦（網路）犯罪研修資料彙編》，2002 年 12 月。

楊智傑，《資訊法》，三版，五南，2011 年 6 月，台北。

**中文期刊**

王銘勇，「侵入電腦系統罪之研究」，法令月刊，第 55 卷 3 期，2004 年 3 月，頁 23-31。

甘添貴，「虛擬遊戲與盜取寶物」，台灣法學雜誌，第 50 期，2003 年 9 月，頁 179-187。

李茂生，「刑法新修妨害電腦使用罪章芻議（上）」，台灣本土法學雜誌，第 54 期，2004 年 1 月，頁 235-247。

李茂生，「刑法新修妨害電腦使用罪章芻議（下）」，台灣本土法學雜誌，第 56 期，2004 年 3 月，頁 207-220。

李茂生，「刑法新修妨害電腦使用罪章芻議（中）」，台灣本土法學雜誌，第 55 期，2004 年 2 月，頁 243-256。

李崇偉，「美、日、德三國網路犯罪相關法制之探討」，中央警察大學法學論集，第 9 期，2004 年 3 月，頁 137-170。

李聖傑，「使用電腦的利益」，月旦法學雜誌，第 145 期，2007 年 6 月，頁 70-79。

林三元，「從經濟分析的觀點探討網路不法行為之預防－－以線上遊戲「竊取」寶物之紛爭為中心」，科技法學評論，第 2 卷第 2 期，2005 年 10 月，頁 173-213。

林志潔、古旻書，「無故刪除他人電腦之電磁紀錄罪之實害結果應如何判斷？／最高院 100 台上 6468 判決」，台灣法學雜誌，第 204 期，2012 年 7 月，頁 248-252

林孟皇，「妨害電腦罪章的無故取得電磁紀錄──評最高法院一百年度台上字第三三七五號刑事判決」，月旦裁判時報，第 12 期，2011 年 12 月，頁 83-192。

林冠宏，「刑法妨害電腦使用罪章之研究」，刑事法雜誌，第 50 卷第 6 期，2006 年 12 月，頁 82-118。

柯耀程，「『電磁紀錄』規範變動之檢討」，月旦法學教室，第 72 期，2008 年 10 月，頁 117-127。

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，2003 年 9 月，頁 117-129。

徐振雄，「網路犯罪與刑法『妨害電腦使用罪章』中的法律語詞及相關議題探討」，國會月刊，第 38 卷第 1 期，2010 年 1 月，頁 40-64。

張紹斌，「刑法電腦專章及案例研究」，軍法專刊，第 54 卷第 4 期，2008 年 8 月，頁 86-100。
許恒達，「資訊安全的社會信賴與刑法第三五九條的保護法益－－評士林地方法院九十九年度訴字第一二二號判決」，月旦法學，第 198 期，2011 年 11 月，頁 233-249。
曾淑瑜，「九十二年刑法增訂妨害電腦使用罪章前後之法律適用」，華岡法粹，第 31 期，2004 年 5 月，頁 123-167。
馮震宇，「網路犯罪與網路犯罪公約（上）」，月旦法學教室，第 4 期，2003 年 2 月，頁 124-136。
馮震宇，「網路犯罪與網路犯罪公約（下）」，月旦法學教室，第 5 期，2003 年 3 月，頁 115-124。
葉亭巖，「德國刑法第 41 次修正－『反駭客法』之簡介」，科技法律透析，第 20 卷第 4 期，2008 年 4 月，頁 15-22。
廖有祿、金明燦，「電腦犯罪刑法規範之研究－以二次修正案為中心」，中央警察大學「資訊、科技與社會」學報，第 6 卷第 2 期，2006 年 12 月，頁 55-75。
廖宗聖、鄭心翰，「從網路犯罪公約談我國妨害電腦使用罪章的修訂」，科技法學評論，第 7 卷第 2 期，2010 年 12 月，頁 57-91。
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，2008 年 4 月，頁 103-134。
蔡蕙芳，「妨害電腦使用罪章：第一講：保護法益與規範功能」，月旦法學教室，第 126 期，2013 年 4 月，頁 62-72。
蔡蕙芳，「妨害電腦使用罪章：第二講：本章各罪與他罪之關係」，月旦法學教室，第 129 期，2013 年 7 月，頁 64-78。
蔡蕙芳，「電磁紀錄無權取得行為之刑法規範」，國立中正大學法學集刊，第 13 期，2003 年 10 月，頁 97-196。
鄭逸哲，「吹口哨壯膽－評刑法第三十六章」，月旦法學雜誌，第 102 期，2003 年 11 月，頁 104-115。
盧映潔，「電腦小子鑄大錯」，月旦法學教室，第 57 期，2007 年 7 月，頁 18-19。

**中文論文集**

黃宏全，「電子商務之刑事侵權－妨礙秘密罪與電腦犯罪」，法務部，刑事政策與犯罪研究論文集（14），頁 93-118。

**其他中文參考文獻**

「CIH 病毒作者 陳盈豪今接受約談」，中國時報，1999 年 4 月 30 日，新聞連結：http://ago.gcaa.org.tw/env_news/199904/88043003.htm
立法院法律系統，中華民國刑法修正沿革，網址：http://lis.ly.gov.tw/lgcgi/lglaw?@72:1804289383:f:NO%3DE04536*%20OR%20NO%

3DB04536$$11$$$PD%2BNO
法源法律網，裁判書查詢，網址：http://fyjud.lawbank.com.tw/index.aspx

## 英文書籍

BRENNER, SUSAN W., CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE (2010).
BROOKSHEAR, J. GLENN, COMPUTER SCIENCE: AN OVERVIEW (8th ed. 2005).
CASEY, EOGHAN, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET (3rd ed., 2011).
COMER, DOUGLAS E., COMPUTER NETWORKS AND INTERNETS (4th ed. 2004).
EASTTON, CHUCK ET AL., COMPUTER CRIME, INVESTIGATION, AND THE LAW (2011).
MOORE, ROBERT, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME (2nd ed., 2011).

## 其他英文參考文獻

Convention on Cybercrime, Nov. 23, 2001, CETS No.185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
German Criminal Code (English version), *available at* http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html
The Computer Fraud and Abuse Act of 1986, 18 U.S.C 1030(e)(1), available at http://www.law.cornell.edu/uscode/text/18/1030