結合型犯罪—白領、網路、組織犯罪

林東茂（東吳大學法律系專任教授）/蕭宏宜（東吳法研所博士生，中央警察大學刑事警察系兼任講師）

壹、緒論

這個題目是應法務部邀稿所訂。在「結合型犯罪」的脈絡下，依序探討白領、網路與組織犯罪的相關問題。

網路犯罪是近年來學術研究的重心。原因無他，網際網路顯然是繼機械革命後，影響人類生活最大的一項發明；現在與未來，也都將是重要的資訊與溝通媒介。然而，毫無窒礙的虛擬空間與可以快速交換資訊的獨特商業價值，卻也同時成為犯罪溫床與詐欺犯的另一個天堂[1]。對此，我們應該先釐清一個根本的疑惑：什麼樣的基礎，得以連結既有的白領犯罪與組織犯罪？網路犯罪的界線何在？

遠在 1931 年Mcboyle v. United States 案中，美國的Holmes法官即指出：「當立法者決定將某行為犯罪化時，合理的作法應該是用可以瞭解的文字，將底線與後果公諸大眾；為了讓這樣的警示公平，犯罪的要件自應盡量清楚明確。[2]」談控制現象的對策，要由對現象的瞭解出發。本文分從兩個面向討論，先談白領犯罪、網路犯罪、組織犯罪的定義與特徵，並探討這三個概念在內涵與外延上可能重疊的部分；次就國內「結合型犯罪」的現象面，談規範面的抗制手段。

貳、白領犯罪

一、定義

---

1 Bekämpfung der Kriminalität im Internet-Möglichkeiten und Grenzen.In: www.artikel5.de/artikel/bka-erlaeuterung.html ,1998, versandt im Februar 2000, 頁 3 ，「Wirtschaftskriminalität und Internetbetrug」。

2 283 U.S. 25

依蘇哲蘭（Edwin H. Sutherland）在一九四九年提出的「白領犯罪」概念，其定義為：「具有崇高社會地位的人，在其職業活動過程中的不法行為[3]。」白領犯罪對社會的危害性往往比所謂的「街頭犯罪」（例如搶劫、偷竊、傷害等）來得嚴重。白領犯罪所從事的違法行為，蘇哲蘭堅持不僅指違反刑法，還包含民法與行政法所禁止的行為[4]。此一定義提出後，雖然內涵迭有更易，所重者仍不脫三個要素：行為人的崇高社會地位、職業活動與信任的違背。

一九七０年，美國前司法部檢察官愛德賀茲（H. Edelhertz）發表對白領犯罪的修正定義：「為了避免財物的損失或支出，或是為了獲得企業或個人的利益，以非物理性的方式[5]（nonphysical means）及以隱匿或欺騙手段所實施的違法行為[6]。」他認為，白領犯罪的定義不應侷限在與職業有關的犯罪上，也不應該僅包括社會上層人士；任何透過詐騙手段所實施的財產性犯罪，都可以被認為是白領犯罪。此一定義曾經被廣泛使用；其後則因設定的研究對象過於寬泛，導致焦點模糊的原因而被捨棄。對於白領犯罪的看法，又再度將重點放回有權勢者犯罪的問題上。如Geis主張，白領犯罪雖然定義頗有爭議，但其核心「有權勢者利用可得的機會，濫用自己權力」卻是不變的[7]。

另依夏普羅（S. P. Shapiro），「信賴的違反」（the violation of trust）是白領犯罪的主要特徵與發生原因。「由於受委託之人可以獨佔或不公開資訊，

---

3 Sutherland, White Collar Crime,1949,P.9. “may be defined approximately as a crime committed by a person of respectability and high social status in the course of his occupation”該書聚焦於當時美國規模最大的七十家製造業、礦業及商業公司的違法（主要是違反公平競爭）行為。Sutherland發現，至少每家公司都有一次違反刑事法、行政法或民法的行為，平均違法記錄為十四次（其中僅不到 16%屬違反刑事法的行為）。參閱同書，頁 227。

4 主因：企業機構與社會上層人士擁有足以影響犯罪化過程的強大政經力量，白領犯罪如果限定於刑法所禁止的行為，將無法包含強勢者的犯罪行為。參考孟維德，白領犯罪—現象、理論與對策，2001，亞太圖書出版社，頁 445。

5 至少包含兩種意義：一為不是以搶劫或偷竊等方式，另一為非造成肉體傷害的方式。

6 Edelhertz, H. (1970), The Nature, Impact and Prosecution of White Collar Crime. Washington, DC: National Institute for Law Enforcement and Criminal Justice.轉引自孟維德，白領犯罪—現象、理論與對策，2001，亞太圖書出版社，頁 28，註 5。

7 孟維德，白領犯罪的本質與意涵，中央警察大學學報第三十五期。

且有管理委託人財產的權利，在委託人與受託人利益發生衝突或對受託人的監督不足時，委託人結構上將處於容易被害的地位；此種結構性的機會促使白領犯罪發生[8]。」

目前被廣泛使用的定義，則是 1996 年 6 月，在美國「白領犯罪國家研究中心」(National White Collar Crime Center)所召開的座談會中，與會者所擬定關於白領犯罪的共識：「由個人或機構所從事之有計畫的詐騙性違法或非倫理行為，通常是社會上層或受人尊敬之人為了個人或機構利益，在合法的職業活動過程中違反信託責任或公眾信賴的行為[9]。」這個定義較蘇哲蘭來得廣且具彈性[10]。據此，可以包括利用市場遂行其犯罪活動的行為，如逃漏稅、信用卡詐欺及惡性倒閉。其他的白領犯罪，則包括利用其在商業或政府中的信用地位以進行犯罪的行為，如收取回扣、盜用公款等。另外的所謂職業上犯罪，如醫療詐欺、公勞保詐欺。

二、鄰接現象

1. 間接經濟損害

白領犯罪所造成的間接損害難以被準確測量，但仍是十分嚴重的。如較高的

8 Shapiro, S.P., (1990), “Collaring The Crime, Not the Criminal: Reconsidering the Concept of White-Collar Crime.” American Sociological Review 55: pp.407-419.

9 Helmkamp, J., Ball, R, & Townsend, K. (Eds.), (1996), Proceedings of the Academic Workshop, Definitional Dilemma, “Can and Should There Be a Universal Definition of White Collar Crime?” Morgantown, WV: National White Collar Crime Center, p.3.轉引自孟維德，白領犯罪—現象、理論與對策，2001，亞太圖書出版社，頁 11，註 31。

10 周愫嫻教授則據台灣的實證研究，提出類如上述綜合考慮行為人、手段、動作、法律特性和行為結果等五方面的特徵，值得參考：一、行為人特徵：犯罪人為社會經濟地位高者（可能包括教育程度高、收入高、職業地位高、或具有社會、政治、經濟影響力者）或公司法人。二、犯罪行為特徵：利用「合法」的職權、專業、知識、影響力（如名聲）、公司等從事之非暴力犯罪行為。三、犯罪動機：獲取個人或公司之利益或權力，或避免個人或公司在利益或權力上被剝奪。四、行為違法特徵：違反刑事法、民事法、行政法等中的特定法規。五、行為結果：在法律上，侵害其他個人、公司和國家之利益；在社會影響上，破壞大眾對個人之社會地位、或公司的公信度。氏著，白領犯罪的界定與爭議，犯罪學期刊第九期，頁 13。

稅率、商品與服務額外增加的成本，以及較高的保險費率等。投資在犯罪預防與加強保護措施上的資源，亦屬間接經濟損害。另外，要維持管制機關及司法體系對白領犯罪的回應，也需要花費很大的成本，同時違法者通常會動用較多的資源自我辯護，因此平均對每件白領犯罪回應所需要的成本高於對傳統犯罪的成本。還有因受到內線交易及其他不法操控的犯罪影響致投資者喪失信心，使得有形的股票跌價或債券利率提升和無形的侵蝕社會成員的彼此信賴等，這更是難以估計實際損害的間接經濟損害[11]。

2. 被害者

組織可能成為白領犯罪被害者[12]，如侵佔、挪用公款、員工偷竊等。然而，因白領犯罪的盤根錯節，被害者與加害者間的區分，有時顯得弔詭。如美國Revco連鎖藥局因雙重收費而遭控訴詐欺，Revco認為，之所以雙重收費，是因為政府機關醫藥費用補貼措施不公正而缺乏效率，他們才是被害者[13]。若然，在身受強大結構性壓力下，為求生存而從事違法行為，均係被害者矣。

3. 偵查實務

對於各類型白領犯罪的偵辦，警察介入的程度其實相當有限。在專業訓練以傳統犯罪為導向的前提下，執法者未必具備白領犯罪的專業知識[14]；處理白領犯

---

11 孟維德，白領犯罪—現象、理論與對策，2001，亞太圖書出版社，頁 86。

12 Smigel研究指出，人們對大型私人機構偷竊會比對小型私人或政府機構顯得較不具罪惡感。Smigel歸因企業組織的規模、匿名性、非人稱性、官僚性，大型企業的授權特性、職能分殊化及依賴複雜的科技等，都使他們較易成為被害者。參閱Smigel, E. O. (1970), “Public Attitudes toward Stealing as Related to the Size of the Victim Organization.” pp. 15-28 in E. Smigel & H. L. Ross (Eds.), Crimes against Bureaucracy. New York: Van Nostrand Reinhold.轉引自孟維德，白領犯罪—現象、理論與對策，2001，亞太圖書出版社，頁 71，註 38。

13 Vaughan, D. (1983), *Controlling Unlawful Corporate Behavior*. Chicago, IL: University of Chicago Press.轉引自孟維德，白領犯罪—現象、理論與對策，2001，亞太圖書出版社，頁 93，註 77。

14 犯罪過程隱蔽與難以偵查，導致偵查過程可能必須藉由侵害隱私權（如：監聽）才能達到目的，亦使白領犯罪偵查顯得棘手。參閱Bennett, J. Bradley, "White-Collar Crime, Blue Collar Tactics: A Defense Lawyer's Perspective (White-Collar Crime Symposium)," 28 Western State University Law Review 65 (2000).

罪案件所花費的時間可能較高又不容易破案，甚至受到政治壓力的影響和阻礙。

三、公司犯罪

化約的說，公司犯罪是指以公司企業為媒介而損及內外眾人的行為[15]。例如：公司負責人利益輸送，將公司資產賤售他人，此背信之舉損及公司股東，除處罰負責人之外，是否一併處罰公司？又例如：企業負責人不回收遭到指控的瑕疵產品，導致消費者健康受損甚至死亡，除處罰負責人之外，是否也處罰公司？

雖然前揭蘇哲蘭對於白領犯罪的原始定義，討論的是崇高地位者的犯罪，其研究對象，卻是違反工商經濟法規的集體性違反公平競爭行為，就此而言，公司犯罪，也可以看作是一種以「增進公司利益為目的」的集團性白領犯罪。因此，蘇哲蘭的定義雖指富有權勢者之犯罪行為，真意卻顯在譴責大公司的非法行為。事實上，在蘇哲蘭的觀念中，白領犯罪就是經濟犯罪[16]。其原創的將犯罪學研究的景深，成功的對焦在中上階層，在當時，很有社會批判的味道。

（一）特質

1. 行為是經由公司決策作成的，或至少在表面上有決策。由於公司決策是集體意志的表現，所以公司犯罪不可能是單獨犯，而有許多參與者。這些參與者在刑法上的關係，也許是共同正犯，也可能是幫助犯或教唆犯。例如：決議不回收有瑕疵的商品；決議將有毒的垃圾傾倒在他國或外縣市；決議降低成本而不增列防污染費用；決議賤賣公司資產給公司負責人的關係企業；決議參加圍標等等。這個特質可以排除公司內個別成員的違法行為，不把它當作公司犯罪。國票案是由營業員單獨犯下的，無關公司決策，所以不是公司犯罪。

15 Clinard, M. and R. Quinney, Criminal Behavior System. NY. Holt, Rinehart and Winston. 1973, p.188. 為公司犯罪下了一個定義：「公司成員為了公司利益所為須負刑事責任的行為，以及公司須負刑事責任的行為。」

16 換言之，所有經濟犯罪均為公司犯罪。這說法受到諸如pobl-Sichtermann與犯罪學者Kaiser的支持。參閱Schünemann, UnternehmensKriminalität und Strafrecht, 1979, S.5 註釋 18。

2. 圖謀或傷害公司的經濟利益。公司犯罪的最終目的可能為了獲利。例如，不惜污染環境與鄰為敵，目的是降低成本；不回收有瑕疵的商品，目的還是為了省錢。公司犯罪的終局結果也可能是傷害員工利益。例如，公司決策者將公司內的資金挪做私用，或做其他的利益輸送[17]。

3. 可能造成他人生命身體與財產的侵害或危險。這是第二個特質可能引發的後果。例如，不回收有瑕疵的商品，導致消費者的危險[18]，或為節省成本而違法傾倒有毒廢棄物、怠於增列污染防制費用導致環境污染，危及附近居民健康。

（二）刑法規範的介入與抗制問題

有謂：「市場供需法則下所自由決定出來的價格，就是合理的價格[19]」，道德

---

17 「指公司之控制者，將公司之利益（含公司將要取得或已取得之資產等利益），經由所設計之交易等安排，移轉至能與控制公司之經營者具有特定關係之人（含法人）或其人頭，造成公司利益受損的情形。」劉連煜，公司利益輸送之法律防制，月旦法學雜誌第四十九期，1999/6，頁90。

18 德國聯邦最高法院於 1990 年做出的皮革噴霧器案(Lederspray Urteil)判決（BGHSt 37, 106.）對此即有觸及。值得注意的是：該判決一方面肯認產品製造人的回收義務，來自於「前行為保證人地位」：法律禁止對任何人的健康加以危害，德國憲法第 2 條第 2 項第 1 款有明文規定。他方面卻同時認為「客觀義務的違反並不以主觀的違反注意義務為前提」，換言之，前行為不以過失行為為必要。據此，被告對於產品的危險性是否認知並不重要（不會影響先前的行為是否被判斷為違反客觀義務），也因此，是否違反客觀義務，不會取決於消費者的損害通知。如果皮革噴劑是依照商品製造規則而生產，未使用有害人體健康的化學物質，那麼，在公司未被告知有消費者健康受損之前，公司負責人何以須承擔保證人地位？法秩序無法要求商品製造人的商品絕無瑕疵；而且，現代商業的競爭激烈，殊難想像公司刻意製造有害人體的產品行銷於市，自毀商譽。當然，如果公司為降低成本，以劣質原料生產商品，並因而違反生產技術成規，則又別論。據此，本文認為應從生產的商品有危險開始，亦即，銷售的產品已經形成消費者的損害。從此刻起，商品製造人始有保證人地位。當公司被告知，有消費者因使用皮革噴劑而健康受損，表示該產品已經是一個危險來源，公司負責人必須負責監控此一危險源，不讓損害繼續發生。所以，公司負責人不回收已經發生問題的舊產品，任其繼續行銷，應承擔消費者健康受損之責。參閱林東茂，刑法綜覽，頁 124。

19 加拿大政治理論三大學者之一的馬克佛森（另兩位是泰勒與柯罕），曾提及他反對海耶克所形容的「資本主義市場經濟是一種不可取代的經濟秩序」的看法，或許可以給我們一些啟發：「在既定的資源及所得分配的條件下，自由市場的運作確實可能是一種最有效的機制，但問題在於，在這之前必須先去證成既定的資源及所得的分配是公正的。換句話說，市場經濟是在一個接收歷史所累積的不公平分配的基礎上去進行所謂『自由』的競爭。」參閱許國賢，馬克佛森，世

或法律不應該是一個使「人類的本能」無法實現的準則，人之追求經濟利益，可能為了解決財務困境，可能是不願過儉樸的生活，也可能是為了累積更大的財富，要怎樣應對與解決，人可以自主[20]。有什麼堅強的理由，必須要依賴刑罰，來解決人與人之間關於財富取得或分配的問題？如同D. R. Cressey所言，「我們必須面對一個根本性的矛盾，如果我們為了要降低白領犯罪的機會，而去抑制商業關係中的信託擴張，那麼我們將會嚴重損及合法的商業關係以及許多其他人際間的交易行為」[21]。如何在交易雙方之外，建立有效的監督機制或可信的代理人，使個別的消費者不必直接去承擔網路交易的風險，是將來思索的方向。

在刑事實體法，公司犯罪尚須正面回應法人是否有犯罪能力與承擔刑事責任能力的嚴肅問題。英美法系國家視為理所當然者[22]，在歐路法系卻顯得謹慎[23]。何謂犯罪行為？若堅持須以社會倫理非難性為基礎，只有具自由意志的自然人才有社會倫理道德的判斷力，法人自然不能成為適格的犯罪行為人；可成為犯罪主體的是自然人，是公司的決策者或某部門主管。

參、網路犯罪

對於日益嚴重的網路犯罪，現有的研究大致立基於兩個面向：一是從安全技術的科技層面，研究如何預防與防堵，另一則是從法律層面，探討如何追訴處罰行為人。就後者而言，不能跳開規範的闡釋與設計問題。這個疑難，植基於方法二元論的分析法學，尤其是「為了對犯罪進行有效的威懾，必須使犯罪活動的成

界哲學家叢書，東大圖書公司，頁 185。

20 林東茂，經濟犯罪的幾個現象面思考，一個知識論上的刑法學思考，九十年七月增訂二版，頁 309。

21 Cressey, D. R., (1980), “Management Fraud, Controls, and Criminological Theory. ” pp. 117-147 in R.K. Elliott and J. T. Willingham, (Eds), Management Fraud: Detection and Deterrence. New York: Petrocelli.

22 美國學者William Chambliss即認為，無視白領階層、大型公司與犯罪集團的犯罪事實而得出來的犯罪概念，嚴重扭曲犯罪現實。參閱氏著，Toward a Radical Criminology, in The Politics of Law: A progressive Critique, 1982, P.231.

23 以德國法為例，僅秩序違反法（Ordnungswidrigkeitengesetz, 簡稱OWiG）第 30 條有針對法人與非法人團體處以罰鍰（Geldbuße）的規定。

本大於這種活動的價值」的所謂經濟分析法學[24]，可能無用武之地[25]。針對傳統犯罪型態，類如竊盜、侵占、詐欺等行為的描述與對應原則，雖然承審法官有更易、構成要件間的模糊也一直存在，百年來的變化自有其脈絡可尋；網路犯罪的型態相對繁複多變，可預見的未來，除非網路型態或法規範的對應起根本的變化，否則，就犯罪事實的掌握而言，一個可以預見的終點，恐怕很難存在[26]。

一、傳統理論

國內關於網路犯罪的定義與理解，迄今不出林山田教授在民國七十三年間所提的電腦犯罪理論範圍[27]。可以說，國內學界稱為網路犯罪理論者，在內容上與過去所稱的電腦犯罪大致相同，用以指涉電腦犯罪中較為側重網路運用的一種類型[28]，本文襲用。

（一）定義

依林山田教授，電腦犯罪依所包含的範圍廣狹不同，分為廣義說、狹義說與折衷說。他認為，所謂的電腦犯罪乃指「行為人濫用電腦，或使用足以破壞電腦

---

24 沈宗靈著，林文雄校訂，法理學，頁 451。另參考周錫瑋立委於 2001/2/7 所自行舉辦的「刑法部分條文修正案—有關信用卡部分」研究會的發言：「信用卡犯罪型態已轉型為跨國犯罪，並有完整的犯罪分工，因此在刑事政策上，如何提高犯罪成本，擠壓犯罪者的活動空間，已經成為國際制定相關法制之共識。」中時電子報 2001/3/2。參閱：
http://news.sina.com.tw/newsCenter/twSociety/chinatimes/2001/0302/2878970.html5j/ visited at 2001/4/15

25 人的理解與意義，人的存在與秩序安排，永遠無法絕對的客觀或量化。無論對實存現象如何分析，當為規範必要與否的說理與檢驗，只能從另一個更高位的當為規範去推演。

26 論述可參閱Orin S. Kerr , Cybercrime’s Scope: Interpreting ’’Access’’ and ‘’Authorization’’ in computer misuse Statutes, 78 NY L.Rev. （ 2003/11 刊出 ） download from http://ssrn.com/abstract=399740

27 林山田，論電腦犯罪，軍法專刊第三十卷第八期，民國七十三年；林山田，電腦犯罪與刑法，電腦犯罪問題研討會實錄，民國七十四年；林山田，電腦犯罪之研究，政大法學評論，第三十期，民國七十四年。

28 「指具有網際網路特性的犯罪，亦即以行為人所違犯之故意或過失的犯罪行為中，具有網際網路特性者，均屬之。」林宜隆，建構預防網路犯罪整合安全體系之研究新取向，中央警察大學學報第三十三期，民國八十七年，頁 379。

系統正常運作之行為，而形成之與電腦特質有關之犯罪；而所謂的電腦特質，以行為之違犯、追訴或審判是否需要電腦之專業知識為準。廣義說界定過廣，將許多不具備電腦電腦特質之案件亦納入電腦犯罪之範圍;狹義說將電腦犯罪限制在財產犯罪，顯屬過狹，雖然電腦犯罪之主要犯罪類型固屬破壞財產法益之財產罪，但亦有破壞其他法益之可能；故應以折衷說為宜[29]。」

此外，對於將電腦犯罪定義為電腦濫用的觀點，林山田教授認為，電腦犯罪固然是濫用電腦而形成之犯罪行為，但也會構成一些非屬犯罪之不法行為，如非法刺探或或洩漏電腦資料[30]，而電腦犯罪除濫用電腦形成之犯罪外，也包括破壞電腦而形成之犯罪。因此二者應為重疊的概念，並不完全相同[31]。

（二）類型

林山田教授依當時已經發生的電腦犯罪案例，將電腦犯罪區分為電腦操縱、電腦間諜、電腦破壞和電腦竊用四種類型[32]：

電腦操縱，指行為人為達非法操縱電腦資料處理結果，以實現其犯罪目的，而故意更改電腦資料或電腦程式或竄改處理結果之電腦犯罪行為;亦屬電腦犯罪的主要型態。依電腦資料處理的工作階段，尚可再區分為三種：1. 輸入操縱，指行為人輸入經偽造、變造或不完整的電腦資料，而得操縱電腦，使電腦輸出不正確的資料處理結果；2. 程式操縱，指行為人竄改正確的電腦程式，或在原程式預留空間，擅自加上自行設計的犯罪程式，下達電腦錯誤的處理指令，而得操縱電腦，輸出不正確的資料處理結果；3. 輸出操縱，指行為人竄改電腦處理的正確輸出結果。

---

29 參閱氏著，電腦犯罪與刑法，頁 32-34；電腦犯罪之研究，頁 137-141。有認為，林教授此處所謂的電腦特質概念在操作上並不具備控制電腦犯罪外延之功能，且電腦濫用與電腦犯罪之區別亦不真正存在，電腦犯罪與電腦濫用實為同義詞。參閱蔡仲彥，刑法增修電腦條款之檢討，成功大學碩士論文，民國九十二年，頁 18 以下。

30 請注意，林山田教授為文時，刑法對於這兩類行為都尚未過問。

31 氏著，電腦犯罪與刑法，頁 32-33。

32 氏著，電腦犯罪與刑法，頁 35-39。

另，電腦間諜方式的電腦犯罪，指行為人以間諜手段，非法刺探或蒐集電腦資料或電腦程式，並進而加以非法使用。電腦破壞，指行為人以非法方法，故意破壞電腦硬體或軟體，使電腦系統失效。電腦竊用，指無權者使用電腦設備所違犯的「使用竊取」行為。

在網路犯罪，文獻上另有與傳統電腦犯罪較不相同的分類：一、無權侵入型的網路犯罪，包括侵入他人電腦系統、侵入後改寫他人電腦中資料；二、電腦破壞型的網路犯罪：如利用網路散佈電腦病毒；三、網路服務提供型的網路犯罪：包括網路色情、利用網路恐嚇、妨害名譽、詐欺、煽惑他人犯罪等。四、其他類型的網路犯罪：如侵害著作權、侵害商標權及偽造數位簽章[33]。

二、現況與立法簡評

（一）現況

1. 網路犯罪多屬於電腦輔助犯罪：所謂的電腦輔助犯罪，指犯罪行為所利用的電腦功能具有高度的可替代性，例如在網路上散佈色情資訊、販賣禁藥或侵犯著作權物品、網路交易詐欺等行為。在這些行為中，電腦的功能取代了舊有的廣告媒介或通訊設備，成為行為人傳遞訊息的方法。於此，作為工具的電腦並不具備任何特殊性質。

2. 網路犯罪與青少年犯罪、暴力犯罪結合

就當前的網路犯罪現象而言，犯罪人為青少年者，比例並不低[34]，在層出不窮的網路虛擬物品竊盜案件中，即見行為人以暴力手段取得被害人的帳號密碼，以遂行後續取得虛擬物品的行為。由此可知，網路犯罪已產生與青少年犯罪、甚至暴力犯罪結合的趨勢;傳統理論認為電腦犯罪具有白領犯罪與職業犯罪性質的見解，恐有修正必要。

---

33 馮震宇主持，網路使用犯罪問題及預防措施之研究，頁 15。

34 參見 2003 年 03 月 18 日中時晚報，刑事警察局統計。

3.跨國行為：色情網站或販賣侵害著作權物品的網站，為逃避國內刑事追訴機關的查緝，而將資訊刊登於由外國網路商提供、主機位於國外的免費網頁。該等免費網頁取得並不困難，又無嚴格的身分查核或使用條件限制，行為人可以虛偽資料使用免費網頁，造成偵查上的困難。

（二）成因

在電腦輔助犯罪中，電腦之所以被利用，是由於電腦的功能多樣化發展後，取代了某些舊有工具的功能；因此而被犯罪者加以利用，與傳統上所設想的電腦犯罪，並無直接關係。目前被官方列為網路犯罪的案例，多屬這種類型。網路犯罪中引人注目的駭客、電腦操縱、經濟犯罪等行為，目前的犯罪現象中反未多見。由於電腦犯罪必然依賴電腦的存在，當電腦的擁有越趨普及、電腦被廣泛的使用時，犯罪型態必然會隨之多樣化；甚且是越貼近於生活層面的多樣化。在只有國家或大企業等財力豐厚的組織有能力及需求使用電腦時，工作場所中電腦的功能也必然侷限在非生活化的事務處理，電腦犯罪的對象也因此侷限在電腦本來所處理的那些事務。因此，早期的電腦犯罪被歸類為專業人員的職業犯罪、白領犯罪，或高度技術性、專業性的智慧型犯罪。反之，現今的電腦犯罪，在網路訊息功能與社會運作、日常生活發生密切的互動後，基於技術上或便利性的原因，從事犯罪者在行為過程中藉助於電腦網路，當屬自然[35]。這個物質條件上的變化，足以大致解釋目前網路犯罪趨向多樣化的原因[36]。

其次，電腦網路犯罪之所以被認為是一種新型態的白領犯罪，是導因於理論建構當時的物質條件，僅有少數人能掌握電腦技術，符合白領犯罪中專業人員的類型。就當前情況而言，由於電腦的普及，電腦知識也隨之普及，非專業人員亦可能具有電腦技術知識，網路犯罪與白領犯罪已經不再具有必然的關係；縱使在

35 就此而言，與網路有關的各式犯罪只是反映了社會上早已存在的問題。當然，網際網路或許對某些犯罪有所助長，或因網路的使用特性而發展出獨特的犯罪行為方式，但這些黑暗面絕非是由網路本身所創造出來。「網路世界」是一個經常被誤認為真實的形容詞，然而，不論「虛擬社會」如何真實，犯罪動機往往還是根植於現實的經濟利益或古老的人性。一如經濟犯罪的成因，犯罪學原因論無能為力。

36 蔡仲彥，刑法新增電腦條款之檢討，前揭碩士論文，頁 44 以下。

高技術性的網路犯罪，而不僅是網路輔助犯罪的情況中，亦是如此[37]。

（三）刑法新增「妨害電腦使用罪章」簡評

近年來，刑法迭有小幅變動。甫通過的妨害電腦使用罪章，是繼1999年後，較大規模的立法。本文要對此做一些評論。這個修正案，立法者有其值得尊敬的理想使命，過程中也應該諮詢過不少專家意見，更必然參考了其他國家的立法經驗。總括來看，電腦犯罪的增訂有過深刻的思考，亦有值得稱許之處，然而，在大量援引美國立法例的情況下，法條的文字敘述是否充分考慮到解釋上的困難？是否有其必要？可能還有商榷餘地。文中所述，不代表立法者的決定有誤，不過意在提醒，犯罪化的結果未必是正確性的終極標準。

1. 未經授權進入他人電腦系統

將「未經授權進入」（Unauthorized Access）當成是一種不法行為，不易沿用傳統的犯罪構成要件予以保護；入罪化的關鍵，應該在於維護電腦系統完整性的法益（資訊隱私權）要求。理由很簡單：縱使入侵者不具犯罪故意，也很可能因為單純的擅入他人電腦系統，而破壞他人無體的財產利益（否則市面上又何需那麼多的系統備份與復原軟體？）至於無權侵入後的使用他人電腦行為，本質上未嘗不可能是詐欺、竊盜，甚至公共危險的前階段行為？反映到刑事政策，重心似乎就只是：在如何的程度與範圍內，將行為人羅織入罪？

在過去的二十五年中，美國五十個洲與聯邦政府，均陸續立法禁止「未經授權進入他人電腦」的行為。雖然這些立法動作意在劃清犯罪化與否的界線，由彼邦的經驗可知，對於何謂「進入」（"access"）？何時、如何進入始為「未授權」（"unauthorized"）？迄今卻無人能解[38]。為了避免不當犯罪化，克爾（Kerr）

37 如日前造成嚴重影響的「疾風」病毒，其製作者之一年僅十八歲，參閱中國時報 2003 年 8 月 30 日新聞。本土的例子，如數年前的CIH病毒，亦是如此。

38 Orin S. Kerr ,前揭文，頁 24 以下。該文頁 53 更提及最近的民事判決解釋模式：「任何電腦使用者的違約行為」均屬未經授權侵入。（Recent decisions interpreting the federal statute in civil cases suggest that any breach of contract with a computer owner renders use of that computer an

建議規範性的理解「未經授權進入」的行為，換言之，以不成文的「有密碼保護的」(code-based restrictions）電腦予以限縮。理由有四：適度釐清網路使用自由與隱私權保障間的界線、反應傳統犯罪中的「同意」要件、符合刑罰目的理論與避免可能的憲法爭議[39]。我國新增的刑法第三五八條規定:「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」亦注意及此，值得肯定。

解釋學上的疑義是，本罪的保護法益既然在於資訊安全（類如妨礙秘密的刺探行為）[40]，杜絕單純的電腦入侵行為，更是為了防止進一步的電腦犯罪（侵犯隱私或電腦操縱)，其法律性質似應解為抽象危險犯？若然，本罪的刑度設計即有不當。作為第三六０條的前階行為，在不法內涵上如何得與其作相同評價？

2. 電腦資料的取得與刪改

刑法新增第三五九條規定：「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。」德國刑法類似條文，在第二０二條a探知數據罪（其構成要件:「行為人確定無權，仍為自己或他人，獲得為防止他人無權取得，而特別設有保全措施的電磁紀錄者，處三年以下有期徒刑或罰金。」）與第三０三條a電磁紀錄變更罪（其構成要件:「行為人違法刪除或扣押電磁紀錄（§202a②），使其無法使用或予以變更者，處二年以下有期徒刑或罰金。」）問題在於，所謂刪除或變更電磁紀錄，本就可能成立普通毀損（§354）[41]或變造文書罪[42]；此部

---

unauthorized access.）若導入刑事法，將使網路上的契約行為被大量犯罪化，製造潛在的數以百萬記的犯罪人於他們瀏覽網站與寫信時。近期討論Access的專文，參閱Doug Hyne, Examining the Legal Challenges to the Restriction of Computer Access as a term of Probation or Supervised Release, 28 N.E.J. on Crim. & Civ. Con. 215, Summer , 2002.

39 Orin S. Kerr ,前揭文，頁 55 以下。

40 請注意，立法者似乎不這麼想。節錄本條部分立法理由如下:「……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。」

41 Wesels/ Hillenkamp, Strafrecht BT/2 , 23.Aufl., 2000, Rdn.49ff. (Datenveränderung und

分立法，即顯蛇足。（重罪化、重刑化？）一旦立法成功，競合問題怕仍是無法揮離的註腳[43]。

若行為人刪除變更他人電磁紀錄，而未達妨害電腦系統正常運作程度，依第三五九條為五年以下有期徒刑；若行為人以刪除變更他人電磁紀錄之方式，致生妨礙他人電腦系統正常運作之情形，第三六０條卻定為三年以下有期徒刑。同樣是實害結果，程度較重者，反而較其中間階段在刑度上為輕，顯見本條亦同樣面臨刑度設計不當的問題。

至於「取得」，問題更大。立法理由舉的例子是：故意在他人電腦中植入木馬程式，取得電磁紀錄。實際上，行為人所取得、所在乎的，是帳號與密碼；行為人真正重視、所欲達成的目的，乃是有利用價值的資訊，這難道不是一種妨害（他人關於財產權上的）秘密行為嗎？

另一個爭點是：「立法理由與舊刑法第三二三條的電磁紀錄動產化所表現的思考模式並無不同。既然立法理由認同學說意見，肯定『取得』與電磁紀錄性質不符，而修正第三二三條，則本條何以又規定取得他人電磁紀錄之行為，使得同樣的理論爭議，在對本條的解釋上又發生一次？立法理由顯然在邏輯上自相矛盾。[44]」縱使某些電磁紀錄具有商業價值，亦與承載的物品（如磁片或硬碟）大

Computersabotage)：電磁紀錄不是一個物體或財產，所以不受普通毀損物品罪（德國刑法§303）保護；直到 1986 年第二次抗制經濟犯罪法案才將此一缺口堵住。（Krey, Strafrecht BT/2 , 12.Aufl., 1999, Rdn.257a；Rengier, Strafrecht BT/2 , 3.Aufl., 1999, S.286.同）立法目的在於保護有權使用者的資料完整性與可使用性。這些利益具有經濟上的本質。(Sinn und Zweck des Gesetzes ist es, das Interesse an der unversehrten Verwendbarkeit von Daten zu schützen. Träger dieses Interesses und daher Verletzter ist, wer die Berechtigung hat, über die Daten zu verfügen. Dieses Interesse wird oft wirtschaftlicher Natur sein.)

42 法條競合？若然，下一個問題是：特別？補充？還是吸收關係？德國刑法§303a 也是面臨與該國刑法§274I②消除、扣押、使其無法使用或變更文書罪重疊的問題。Wesels/ Hillenkamp, Strafrecht BT/2 , 23.Aufl., 2000, Rdn.50.

43 Rengier, Strafrecht BT/2 , 3.Aufl., 1999, S.287 特別指出德國刑法§303 毀損物品罪相較於§303a 應居於補充地位；換言之，成立法條競合。（Kindhaüser BTII/1, §24 Rdn.22、Lackner/Kühl, §303a Rdn.6 同旨）

44 蔡仲彥，刑法新增電腦條款之檢討，成大法研所碩士論文，民國九十一年，頁 110。

有所別，如何可以，甚至必須將「價值」轉化為「動產」加以保護？

3. 干擾他人電腦—駭客條款

刑法新增第三六０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。」所謂干擾，例如癱瘓網站。解釋上的疑義是，如何與毀損、變更電磁紀錄明確區別？假設，這是一種未達毀損（不堪用）程度的狀態（請注意本條末段「致生損害」的用語），法定刑重於毀損的依據何在？

將他人電腦砸毀，被害人一樣受財產上損害及資料處理上的干擾，該當刑法第三五四條毀損罪，為二年以下有期徒刑；若依本條「以電腦程式或其他電磁方式干擾他人電腦或其相關設備」，致生他人電腦或電信機能可回復的一時性干擾，卻是三年以下有期徒刑。前一情形的不法內涵及損害，難道一定低於後者？以電磁方式干擾他人電腦運作，和以毀損方式干擾他人電腦運作，到底在法益的侵害上有什麼不一樣，而需要另立新條文？除非將本罪往公共危險方向推敲，似無增訂必要。

論者有謂：「『其他電磁方式干擾他人電腦或其相關設備』，用微波爐加熱筆記型電腦，算不算？既然本條意在保護『網路的通訊機能』，換言之，就是電信。若能將本條行為，修正為『以電信之方式干擾……』，或規定為「對具有……功能之電腦，干擾其電信機能……」應是更嚴謹且符合原意的行為描述[45]。」

4. 製作電腦病毒

刑法新增第三六二條規定：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科五十萬元以下罰金。」前段所謂「製作專供犯本章之罪之電腦程式而供自己

45 蔡仲彥，刑法新增電腦條款之檢討，成大法研所碩士論文，民國九十一年，頁 115。

或他人犯本章之罪」的行為，實際上是第三五八條至第三六0條的預備階段（或預備階段的幫助）行為，本條因此可能是實質預備犯。若然，條文卻以「致生損害於公眾或他人」的「實害結果」為要件，何解？可能的處理方式，勢以「客觀處罰條件」為後段性質作結。申言之，「損害」只須客觀存在，而與行為人主觀上對其存在或發生有無認識與預見無關[46]。

肆、組織犯罪

人有營建朋黨的社會性，犯罪人同樣也有這種社會性。理由是，一群人組織起來，更宜於有效率的謀取利潤、壯大行色、降低風險（包括被其他犯罪團體侵犯，被刑事司法機關瓦解的風險）。組織犯罪典型的態樣是，煙毒犯罪、軍火買賣與走私、與夜生活有關的犯罪（主要是色情媒介、人口買賣、經營非法賭場）、收取保護費、非法仲介與控制外籍勞工、偽造貨幣、偽造並濫用非現金交易的給付工具（主要是支票與信用卡）、集體竊盜與入室行竊並集中管理銷贓、竊取名貴轎車銷贓國外、非法傾倒特殊的垃圾。由於組織犯罪的縝密犯罪計畫與行動實施，加深犯罪控制上的困難、穩妥享有極高的犯罪利潤，甚至降低被追訴的風險（沒有直接的被害人或被害人不願告發或不敢向刑事追訴機關陳述意見），而成為國家與社會的挑戰。

（一）定義

依一九九0年德國司法界與警察界共同組成的「組織犯罪的刑事追訴」研究小組對其所下的定義，認為：「組織犯罪是追求利潤或追求權勢之有計畫的犯罪活動；組織犯罪是由兩個以上之參與者，長期間或不定期間在下列之情況下分工共同合作：a. 運用營業或類似商業之結構，b. 使用武力或其他足以使人屈服之手段，c. 影響政治、公共行政、司法或經濟[47]。」依König，組織犯罪係由委任、知

46 關於製作電腦病毒與訴訟法上「不證自明原則」之關係，可參閱 Meiring De Villiers, Virus Ex Machina: Res Ipsa Loquitur, 2003 Stan. Tech. L. Rev. 1

47 林東茂，德國的組織犯罪及其法律上的對抗措施，危險犯與經濟刑法，2002/11 初版三刷，頁175。原文、評論與其他類似定義，可參考http://people.freenet.de/kvlampe/okdef.htm不贅。

識與三個行為特徵所組成：①犯罪集團，每個集團均有其核心首腦；②保護者，維護犯罪所得利益；③專業支援，提高組織利益[48]。

我國組織犯罪防制條例第二條則定義為：「本條例所稱組織犯罪，係指三人以上，有內部管理結構，以犯罪為宗旨或以其成員從事犯罪活動，具有集團性、常習性、脅迫性或暴力性之組織。」依此，我國法律上所稱之組織犯罪較向來理解的組織犯罪為寬：實務與學者多以傳統暴力幫派犯罪的觀點來詮釋組織犯罪，惟依組織犯罪防制條例，卻非僅指幫派等組織，而尚包含其他依法律設立之法人或社團，具有前述不法活動特徵、以從事犯罪之目的而存在者。如以洗錢為業之金融、投資公司，或以非法手段討債為業之債權回收公司等，仍屬組織犯罪集團，不因其是否依法律組成而有差別。

台灣的組織犯罪，較常涉入的經濟活動如圍標工程、開設地下錢莊、介入上市公司董監事選舉，炒作股票等。此類經濟活動在表面上均為合法的商業行為，但過程中以涉入強暴脅迫等手段，以獲取鉅額的經濟利益。美國RICO法的內容，主要亦係針對類此的恐嚇勒索活動（racketeering activity）[49]。其聯邦法院對於「企業」概念的解釋，甚至包含政府機關與無正式名稱卻實際構成組織者[50]。據此，勉強可認為白領犯罪與組織犯罪在追求經濟利益的型態上有部分交集。事實上，以經濟犯罪型態出現的組織犯罪，依德國學者 2002 年的研究，比例僅占 11.6%[51]。從獲取經濟利益的角度觀察，組織犯罪與洗錢結合較深。

（二）特質

1. 主要目標在獲取極大利潤：組織犯罪採取理智而有計畫的行動，希求在以

48 參閱 Dorean Marguerite König, The Criminal Justice System Facing the Challenge of Organized Crime, 44 Wayne L. Rev. 1351, 1359(1998).

49 依該法（18 U.S.C. §1962），大意指「任何人直接或間接，以恐嚇勒索型態或以所收取的非法債務接受任何收入，將其收入之任何部分或所得，直接或間接用於或投資於任何從事或其業務影響洲際或國外商業之企業者，為違法。」

50 United States v. Turkette, 452 U.S. 576, 583(1981).2

51 http://www.bmi.bund.de/dokumente/Pressemitteilung/ix_92410.htm近四成集中在毒品犯罪。

最小的風險，在最短之時間內，牟取最大之利益。並會附隨的以所得利益去圖求權力與社會地位及影響力，藉以鞏固其組織成員之向心力與服從性。

2.具有分工與專業的行為方式：犯罪組織中有明確的分工，每個人專門從事某種策劃或執行計畫。由於快速的科技與經濟發展，使得組織犯罪的成員必須去觀察合法與非法的市場，並且分析、找尋洗錢與投資的新管道，將促指組織犯罪將會更朝專業化發展。

3.職業化：一切有組織的犯罪都是職業犯，長期依靠犯罪活動維持生計，熟練掌握犯罪技巧，具有明確無誤的犯罪生涯、犯罪自我形象和犯罪價值觀念。這些職業犯相當富有彈性，可以在政治、經濟或科技的領域當中有良好的適應，在犯罪人群體當中有良好的掩飾，不容易被刑事追訴機關或競爭者打擾。

4.掩飾性：前述職業化的另一種表現即是掩飾性，組織犯罪的許多犯罪活動都經過巧妙的掩飾，從外表看，是合法的行為或是有合法的商業活動作掩護，增加刑事偵查追訴的困難。

5.階層組織：每個犯罪組織都受一個決策中心的指揮領導。決策中心負責探測活動的時機，評估風險、代價與利潤，並監控犯罪計畫的實施。組織的決策與領導階層不直接接觸實施犯罪活動的組織成員，通常由處於決策階層與執行階層間的「隔離聯絡人員」指導、監控犯罪計畫的精確實施。這些聯絡人員從事合法職業，只負責把決策中心的命令轉達給執行者，並把執行成果匯報給決策階層。通常刑事追訴機關只能深入到聯絡人員這一層，很難追訴到組織犯罪的幕後人物。

6.活動範圍都市化：組織犯罪基於下數原因，幾乎分佈在大都市中：(1)大都市經濟結構熱絡，資本集中，提供組織犯罪良好的機會，去找尋有償債能力的被害人；(2)金融中心有利於組織犯罪就其利潤所得加以確保、增值並加以合法化，適於投資、洗錢；(3)良好的交通條件增加犯罪人的機動性與貨品的流通；(4)由於大都市的犯罪人口集中，組織犯罪容易徵召新的成員；(5)大都市的刑事追溯機關工作負擔已甚繁重，而對付組織犯罪則因必須在法律上、策略上、組織

上更加講究，使得他們可能樂於對付比較容易處理的一般犯罪(6)人口稠密的大都市，有很高的人口流動性與匿名性，娛樂及消費需求旺盛，價值觀念容易受到誘導與改變，這些情形適合組織犯罪的活動發展。

7. 手段暴力脅迫化：組織犯罪者不論所從事者為合法或非法行業，常須利用暴力或威脅手段遂行其目的，對其而言，暴力或威脅乃被工具化，而非表達之方法，固然並非所有之犯罪組織均使用暴力，但其對外存有暴力之威脅，乃係其不變之特徵。

8. 對執法及政治體系採行腐化策略：除了使用暴力威脅外，犯罪組織另須依賴對執法及政治體系之腐化策略，以達成其目的，若缺乏執法或政治體系之腐化及對犯罪組織之包闢、支持或刻意忽略，犯罪組織仍難確保壯大發展，因此行賄、勾串、滲透乃成為犯罪組織不可缺少之伎倆。

伍、形成結合型犯罪的可能

如前文所述，網路犯罪與專業知識並非完全交集；凡利用網路功能者，均屬網路犯罪。雖然目前發生的網路犯罪多屬此種電腦輔助犯罪，但是依賴電腦網路技術基礎或設計上缺陷的白領犯罪或組織犯罪，現實上仍然極有可能發生。可以想像將誘發利用網路的白領犯罪情況，如：

1. 市場或技術的因素—策略性行為（strategic behavior）

大公司利用其在市場上或技術上所佔有的優勢地位，在程式設計上故意採用不利於競爭對手的方法，或在程式中插入不利於競爭對手訊息的不正競爭手法。最著名的例子，莫過於微軟為了獨佔瀏覽器市場，而自Windows98 版作業系統開始，故意將Internet Explore瀏覽器作為整個使用者介面的核心部分，促使Windows的作業系統使用者，在無意識中習慣於使用其產品，並使競爭產品喪失接近使用

者而能展現其品質的機會，以此方法，微軟遂取得瀏覽器市場的有利競爭地位[52]。

其次，因近年來以「物件導向」及「使用者無需關心」的軟體設計理念，漸漸形成了「使用者無從關心」的局面；網路發達後，軟體有更好的機會流通，軟體設計者因而較以前有更大的機會去左右使用者的使用習慣。簡單的說，使用者對電腦及網路的正常使用，所倚勢的者對網路、資訊業者、程式撰寫者的信賴，而非理解；使用者通常無法參與自己所使用的產品實質內容，也無力修改，無從得知某個程式的功能，是否一如其文字說明，甚至是否用心良善（如 cookie）。以上兩種情況，市場和技術資訊的不對等，使得消費者處於毫無防備的地位。

2. 網路（信用卡）交易機制過於簡陋

在目前以信用卡做為主要支付工具[53]的電子商務交易過程中，一切交易所必

---

52 其他不正競爭的例子，請參考Wendy Goldman Rohm, The Micorsoft files ,Random House, 1998.; Cambell, Christopher P., Fit to be Tied: How United States v. Microsoft Corp. Incorrectly Changed the Standard for Sherman Act Tying Violations Involving Software, 22 Loy. L.A. Ent. L. Rev. 583, 2002; Schanzenbach, Max, Network Effects and Antitrust Law: Predation, Affirmative Defenses, and the Case of U.S. v. Microsoft, 2002 Stan. Tech. L. Rev. 4.

53 就電子付款系統而言，大體可分成三類：透過銀行付款、以電子資金移轉（electronic funds transfer；簡稱EFT）付款、以電子貨幣付款。透過銀行付款的方式係傳統支付的形式，其中銀行帳戶均為現金交易、支票及信用卡交易之主要付款基礎。在線上商務取代面對面交易時，許多問題馬上會出現。例如：付款方式及交易雙方身份驗證等交易安全問題。為了解決上述電子交易之付款問題，即形成電子資金移轉付款及電子貨幣付款兩種支付方式。就電子資金移轉支付方式而言，當消費者於線上發出訂單時，其個人私密付款資訊（例如信用卡或銀行帳號）隨著訂單一起傳送。EFT係透過銀行與主要公司間安全的私密網路，傳送信用卡號或電子支票（單純的支票影像）。安全電子交易（SET）協定為Visa或 Master Card共同支持而以信用卡為基礎的系統，使用數位證書，即所謂的「數位信用卡」。此種付款系統又稱作記錄式資金移轉系統（notational funds transfer; NFT），因為它像傳統電子金融轉帳及電匯之記錄帳戶結算買賣之方式。由於線上傳輸的付款資訊包括機密的財務資訊，因此如果第三者攔截機密資訊，付款之消費者可能會遭財務損失。為保護傳輸之付款訊息的真確性及確保不同付款協定系統間的互通性，1996 年Visa及Master Card提出SET協定，保證可在不同硬體平台與網站瀏覽器間互通。此安全電子交易協定由微軟、網景、IBM、GTE、VeriSign及其它電子商務主要參與者所支援。除了以信用卡付款為基礎的交易提供標準的通訊協定及訊息格式外，SET利用數位簽章、消費者與商店身份識別，透過加密及訊息真確性提供私密性。http://www.npf.org.tw/LIBRARY/FM-R-089-007.HTM。

須的工具都可被數據化、資訊化，這其實也同時代表消費者對於交易過程的喪失控制。在消費者持有實體的信用卡，並且應在簽帳單上簽名，才能完成交易的情形，只要妥善保管信用卡，即可以有效的避免被冒刷；然而，透過網路使用信用卡，所在乎的仍然是身份與資料的安全性與真實性，也因此，偽變造或行使支付工具的情形，一樣存在。已知的犯罪型態如在網路上擷取他人信用卡號（在加密的傳輸過程中[54]，資訊仍可能被擷取而盜用或變造），或利用信用卡號產生器（Credit Wizard程式）產生卡號，而於電子商店消費。2000 年 10 月公布施行電子簽章法[55]，依該法第九條第一項：「依法令規定應簽名或蓋章者，經相對人同意，得以電子簽章為之。」然現況卻是，仍有極多的網站並未採行SET或SLL兩種通用的網路付款安全機制。換言之，使用者僅需輸入信用卡卡號及有效截止年月二項資料，即可完全取代實體特約商店的刷卡動作。面對日新月異的科技發展，網路信用卡認證機制的不健全，縱使將有形體的信用卡視為有價證券，仍然不能依照新增的第二0一條之一加以處罰。處罰網路上擷取他人信用卡號的行為，依舊有賴傳統的刑法規範，如偽造文書、詐欺。

3. 小額電子貨幣的使用

54 為了確保交易資訊的安全性，利用加密的技術(Cryptography) 可以使得資訊的傳送不會被中途攔截和被塗改；同時，可以保證送出來的資訊無法銷毀，讓送者(sender)無法否認曾經送出這樣的資訊，使得進行交易的買方無法反悔或失信。加密的技術同時也可以做為辨識送出資訊的人的真偽，這種可以產生數位簽章(digital signature)的技術，稱為 encryption。利用這項技術，網路的使用者可以創造一個類似個人簽名的數位簽章，每次這個使用者要送出任何訊息，都可以將其個人的數位簽章附在上面，以資證明這個訊息的正確性。這項技術甚至可以知道經過數位簽章送出去的訊息是否有被更改過，因而能一定程度確保電子交易的安全性。

55 依該法第二條關於用詞定義的規定，所謂電子簽章，是指「依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。」；所謂數位簽章，是指「將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。」；所謂憑證，是指「載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。」須說明者，設置公開金鑰認證機構是為了解決利用網路傳輸訊息或進行交易時所衍生的身份辨識及資料安全等問題，手寫簽名或使用印章方式已經無法滿足需求，使用合適的技術取代傳統的身份辨識方法具有現實之必要性，數位簽名技術的利用即是其中之一。

在塑膠貨幣之後，電子商務也開始嘗試運用電子貨幣（Digital Money）[56]，用以支付網路上的小額消費。所謂電子貨幣是由網路服務提供者（ISP）或其他服務提供者，統一向用戶先收取費用，購買一定的點數後，用戶以扣點數的方式支付ISP或其合作業者所提供的各種小額線上服務，以取代小額消費以線上刷卡方式付款的不便。此種機制的著眼點在於，消費者不太會透過網路成立每筆金額十幾二十元的交易，如果能夠讓消費者一次預存以減少付費手續的麻煩，應可使消費者樂於使用，而能夠提升交易額。簡單的說，即是「代幣」的電子化；目前遊戲業者的點數計費制度，也可算是其一。關於電子貨幣的使用及結算，由於金額微小，消費者易於輕忽，而完全仰賴業者的計算結果。

以上三例，形成如夏普羅所言的「白領犯罪的結構性犯罪機會」。其結果，將減低對網路秩序、電子交易機制之信賴。

再觀察組織犯罪與網路犯罪。由其利用網路的可能性而言，關鍵亦在於網路交易的安全性問題。過往對此，均著重於在訊息傳輸過程中，如何保密；對於有權取得授權資訊的他方，即出賣人或提供服務之人的可信度問題，卻無能為力。目前組織犯罪利用網路從事犯罪活動，固然以販賣盜版光碟為主，若電子商務的利潤能夠再提高、犯罪組織能掌握相關技術，組織犯罪介入分食網路「交易安全」大餅應該可以預期。

陸、抗制對策（代結語）

---

56 譬如資策會所經營的ISP或亞太線上，均提供此種電子貨幣的制度。意指能夠重複儲值或是預付，持有者向電子貨幣發行組織支付傳統貨幣，而發行者把等值的現金價值的資訊轉為數位訊號以電子、磁力或光學形式儲存在持有者的科技介面上，是各種電子支付付款方式的總稱。用來儲存的媒介，可能是智慧型IC卡（Smart Card），也可能是以應用於網際網路上的各種Network money。參閱http://www.lib.fcu.edu.tw/students/team02/03.htm目前已開發的兩類數位貨幣為Digi Cash公司所發展的Ecash （數位現金）及Mondex公司發展的智慧卡。Ecash是基於線上交易的網技網路付款系統所開發出來的數位貨幣協定。其使用公開金鑰加密技術以維護數位貨幣的真確性。Digi Cash公司授權Ecash技術給銀行，銀行轉提紙幣為數位貨幣並作驗證、清算、及結算帳戶，並以貨幣伺服器來驗證、清算及結算帳戶。參閱http://www.npf.org.tw/LIBRARY/FM-R-089-007.HTM

本文所談的，主要是以電腦網路為工具的結合型犯罪。網路經濟犯罪，對於電子商務市場的發展，尤其網路證券交易與網路拍賣的型態，直接構成威脅；傳統的犯罪構成要件，面對網路上無實體的交易型態，可能力有未逮。問題的抗制對策，化約的說，就是網路犯罪的抗制對策。其次，白領犯罪、組織犯罪與經濟犯罪間固有差異，就其犯罪動機經常是在獲取經濟利益，並因此進行攻擊經濟秩序的活動而言，抗制對策上應有重疊。

法益的原貌與保護的界線，總是在社會觀念與需求間擺盪。就網路犯罪而言，技術面的抗制比法律面重要。投大眾所好而一味加重刑罰，不是良好的刑事政策。犯罪人所考量的，從來不僅行為在刑罰上的嚴重性因素而已，尚且有行為被查獲追訴的可能性；隨高刑度而來的，往往是更精密、更龐大的犯罪計畫。遺憾的是，最近刑法新增的妨害電腦使用罪章，即有濫用重刑的嫌疑。另一原因，在於網路犯罪的問題，其關鍵似乎不在無法可罰或刑罰過輕；事實上，大部分的網路犯罪行為，都可能藉由解釋，輕易以現有的法律予以掌握。在網路這個互動、多元且資訊量驚人的環境裡，監控困難、偵查不易與跨國犯罪行為，或許才是焦點[57]。

白領犯罪，可以說是一種計算性的賭博；當被逮捕和懲罰的機會較低時，白領犯罪發生的可能性自然相對提高。換句話說，當事人會依據風險，來判斷是否從事違法行為。就此而言，加重刑罰是一個不對題的解決方案。除了有利宣導外，對於有效的偵查與追訴的問題，無能提供任何助力。以犧牲刑法的罪刑相當原則作為代價，是否值得，法律工作者亦須深思。

事實上，整個網路、經濟、白領與組織犯罪的關鍵在於，隨著新型態電子支付系統的使用，財產犯罪，尤其是詐欺與洗錢行為的構成要件，面對網路時代，能否規範電子貨幣與網路銀行所帶來的衝擊？為什麼思考的藥方總是「治亂世用

57 網路經濟犯罪超越了國境，對於現行以國家主權為基礎的立法、司法體系產生衝擊。認為可以單純依賴刑法加以制約，恐怕是過份天真的想法。擺盪在犯罪化與秩序罰之間，刑事政策上如何抉擇？

重典」呢？嚴刑峻罰能否解決問題，證諸人類的有限歷史，答案恐怕不用多說[58]。

58 在入罪化與重刑化的相關立法過程中，背後所據者，無非是刑罰理論中的一般預防觀點（Gesichtspunkt der Generalpravention）。問題是，對於經濟犯罪，談一般預防，真的有效嗎？參閱 Schüchter, Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, S.22. 語出 Wassermann。