

日本不法連線行為禁止法簡介

李茂生

國立臺灣大學法律學院

一、前言

日本於一九九九年四月十六日透過閣僚會議向第一百五十四次國會提出了「不法連線行為禁止法草案」，在經過其眾議院以及參議院的審議後，同年八月六日獲得與會國會議員的一致同意，並於同年同月十三日以平成十一年法律第一二八號的文號予以公布。該法訂有日出條款，關於以刑罰禁止不法連線行為的部分（法第三、四、九條以及第八條第一款）是於公布半年後，亦即兩千年二月十三日起實施，至於對於業者等立於防備立場者所為都道府縣公安委員會的援助以及國家所為宣導啟發活動等部分（法第五條至第七條，以及第八條第二款），則是於法律公布後一年內以政令實施。

關於刑罰法規的修訂或增訂等，一般而言日本朝野都是採取非常慎重的態度。本法雖然有一部分是屬於行政援助以及宣導啟發活動等的規定，但是終究是以刑罰法規為重心，而且這些新的刑罰法規可以說是超越了傳統刑罰法規的範疇，而以新的觀點禁止了一些網路上的活動。本來按照以往的慣例，這個法律應該不是那麼快速地、而且沒有經過充分討論下即可通過審議而實施。但是事實卻不是如此。其實，在這個充滿詭譎氣氛的立法過程中，我們可以觀察到一些國際上的壓力，基於此點，甚至於可以判定這個法律僅是先進國家資本全球化的諸動作中有關網路交易安全政策的一環。

我國雖然號稱在國際經濟中佔有一席之地，但事實上最近卻有日益下滑的傾向。究其原因，不外是破壞環境的產業（不論是否為傳統產業抑或高科技產業）逐漸移轉至較為落後的國家，以及投資環境變為惡劣，不僅不易扶植國內更高一層次的產業，也無法吸引外資前來投資。而投資環境的諸種惡劣條件中，不可諱言的，網路交易上的危險指數應該是外資等非常顧慮的一點。基於此點，最近我國政府也開始重視網路上國家級的安全問題，而展開了一連串的研究委託動作。

本文透過介紹日本最新的「不法連線行為禁止法」，除了闡明上述先進國家的全球網路交易安全政策的內容外，亦企圖揭發隱藏於該國際性政策背後，會侵害到我國國民權益的弊端。在我國亦將被納入先進國家資本全球化運動中一環的此刻，應該留意到經濟優先的考量有時不僅是喪權辱國，嚴重的時候，甚至於會扼殺我國於二十一世紀中的生機。而這個生機應該是潛藏在透過網路生活自發性觸發新時代國民形象的可能性中。

二、不法連線行為禁止法的概略內容

如前所述，日本的不法連線禁止法是由兩個部分所構成。首先介紹防禦政策的部分。這個部分又可分成兩項，一為連線管理者的防禦責任，另一則為地方政府與中央政府的援助責任。

法第五條規定管理連線的人平日應該致力於ID密碼等連線用識別符號的管理，同時其亦應經常檢驗連線控制機能的有效性，於有必要時應儘速採取提高該機能或防止不法連線行為的必要措施。關於這些必要措施的內容等，早在法公布實施前，即已由國家公安委員會（其實就是隸屬於其下的委員會輔佐機關—國家警察廳）、通產省以及郵政省等透過導引書的發表而公諸於世，其中還包含了連線利用行為記錄的保存、檢視等。

至於地方以及中央政府的援助責任方面，則是規定於第六及第七條。法第六條規定，當連線管理者發現其所掌管的電腦有發生不法連線行為的情形時，其可申請地方政府就該些行為的防止方面，提供必要的資料、建言以及指導；而地方政府為達成此項任務其可委託特定的第三人進行案例的分析等作業（該受委託人若有洩密情事，則會被依法第八條第二款科以一年以下有期徒刑或五十萬日圓以下罰金）。與以上地方政府的責任相配合，法第七條規定了中央政府的責務。第七條規定，國家公安委員會、通產省大臣以及郵政省大臣應該至少每年一次公布不法連線行為事案的發生狀態以及有關控制連線機能方面的研究開發情形；除此之外，其亦應致力於啟發、普及關於防禦不法連線行為的知識。

當然政府機關於執行這些任務時，應該要有其一定的技術能力，而這方面技術能力的開發體制等，則是早在不法連線行為禁止法公布實施前即已由警察廳所主導的系統法修正中得到法律依據。

日本警察廳於一九九八年時即已鑒於網路犯罪的增加而開始主導「特定公共電信系統開發關連技術的研究推展法（簡稱系統法）」的修訂。此系統法在一九九九年五月修正通過，根據新修訂條文，主管機關得命令電信及廣播機構（此機構是基於日本通信及廣播機構法，在郵政大臣的認可下所成立者，其資本金一千餘億日圓，擁有百餘名員工）進行關於高科技犯罪（亦即以電信通訊為手段的犯罪）的情報蒐集以及防治技術的開發。而警察廳藉此助力，將可確保關於電信方面最高級的技術能力，並依此而引導地方警察進行相關的犯罪防治工作。

以上除被委託研究者的洩密禁止規定外，都是宣示規定，目的雖然是在於建設安全的網路及通訊環境，但是終究僅是一種期待，並無任何保證。不過在這些宣示規定中仍舊有一條顯露出不一樣的企圖，此即連線管理者得申請地方政府提供資料、建言及指導的條文。這個條文配上系統法的修訂，致使地方警察能夠有能力與機會直接接觸到網路的世界。換言之，擁有能力的警察並不一定會有機會接觸到民間的網路上活動，這是因為網路行為的抗國家權力的特色使然，但是假若能夠利用民間自己的監視力量，並提供一些優惠待遇，則警方只要以逸待勞，就會有機會積極介入網路世界。

不過，縱或如此，假設所設定的介入時機過遲時，例如規定已經發生實害後始能進行介入，則亦有可能會因為連線管理者考慮到商業利益而亟欲掩飾實害，進而失去介入的良機。所以「不法連線行為禁止法」又新設了幾個新的犯罪類型，藉以促使連線管理者能夠在實害發生前提早申請國家的介入。此即所謂的「在國民的同意下警方所為的早期介入」，其防止犯罪發生的機能是遠高於「在實害發生後未得同意下的警方積極介入」。

不法連線行為禁止法之重心在於新的犯罪行為類型的設定。根據法第三條規定，所謂的不法連線行為是指「利用網路連線將電腦置於連線控制機能所限定的特定利用狀態下的不法行為」，其行為態樣有二，其一，未得同意而輸入他人的識別符號，其二，以輸入識別符號以外的方法，輸入訊息或指令，進而迂迴規避連線控制機能所為特定利用的限制。基本上這種行為類型並不是以往所謂的「無權利用電腦網路資源」行為，因為其並不以利用特定電腦網路資源為條件，此外，其亦非各種傳統電腦網路犯罪，例如竊取、竄改資料的行為，或干擾電磁記錄處理等行為的預備行為類型，而是單獨存在的入侵行為類型，其所保護的法益，亦即保護客體是社會對於「網路連線控制機能」的信賴。依法，行為人只要故意地做了以上的兩種動作之一，將電腦置於特定的狀態下，即會被根據第八條第一款科以一年以下或五十萬日圓以下罰金。

除以上的主要犯罪行為類型外，不法連線禁止法亦於第四條規定了助長不法連線行為的禁止行為類型，並於第九條中規定了應有的刑罰（三十萬日圓以下罰金）。這種助長不法連線行為的禁止行為類型，其行為態樣有二，其一為公開他人的連線識別符號，並告知該識別符號是使用於某特定電腦的特定利用，其二，向知悉這些訊息的第三人提供該識別符號。不過，雖然某些軟體得測出規避連線控制機能所為特定限制時所需的特殊訊息或特殊指令，但是因為這些軟體有時是為了確認系統安全性而開發或提供者，所以此次的立法並沒有去考慮規制這類軟體的必要性。

此外，雖然這種行為類似於不法連線行為的幫助行為，但是法律基本上主要是著重於提供他人識別符號的這種客觀行為會產生的助長不法連線行為的危險性，所以並不以「有助於他人的不法連線行為」的目的或認識為要件。據此，若只是單純提供，並認識自己是在提供他人的識別符號時，僅會被科以提供罪的刑罰，但是假若另有幫助他人不法連線行為的目的或認識時，事實上該當行為會被認為是不法連線的犯罪行為的幫助行為，因而法定刑將會被提高（日本刑法第六十三條規定，幫助犯依正犯之刑減輕之）。

據以上的介紹可知，不法連線行為禁止法所創設出來的犯罪類型，雖然實際上通常都會導致其後的傳統電腦網路犯罪行為，但是該法透過立法技巧，將新型的犯罪行為的保護客體（亦即保護法益）抽象化，並切斷現實上整體犯罪行為於犯意上的連鎖性，藉此將整體犯罪行為的前階段獨立出來，就此成立一個新的、但處罰比較輕的犯罪類型。而一般而言，只要連線管理者認識到這些事實，則其應會主動地、積極地提供尚未產生實害的案例與警方，而警方則可藉著「被害人」積極的通報，即時地介入本來是不可視的網路世界以進行管制。

三、 國際情勢的壓力

日本於一九八七年修訂刑法，增訂了一些關於電腦網路犯罪的條文，不過這些條文基本上仍舊是維持住了「保護傳統法益」的基本態度，連「電腦的無權使用行為」的犯罪化要求，都因為這個要求會創設出新的法益（例如電腦持有者的使用權等）而於立法時被否決掉。不料於一九九九年時，日本卻以特別刑法的立法方式，將較諸無權使用

用行為更屬前階段的侵入行為予以犯罪化。其背後實是有一定的國際情勢壓力。

雖說是國際情勢，一言以蔽之，此不外是美國的要求。美國是一個資訊大國，在二十世紀的末期起，其即已確認二十一世紀將會是資訊以及生物科技的時代，而生物科技的發展實際上必須依賴於得大量且快速處理資訊的電腦科技的發達，但是電腦科技於開發的當時並沒有考慮到太多的安全措施，這造成了電腦以及其後發展出來的網路系統的脆弱性，於處理大量而且重要的資訊時，根本無法確保該些資訊不會受到侵害。於是在保護本國利益的大前提下，其快速地展開數階段的資訊管制法制的發展歷程，特別是生物科技日益成熟的九〇年代起，更可以說是有了迥異於以往的新發展。

美國有關電腦犯罪或電腦網路犯罪的規制趨勢大略可分為四期。首先為七〇年代後半開始一直到八〇年代前半段的第一期與第二期。第一期法規的規制目的在於仍舊是稀有的電腦資源的分配與保護，雖然有處罰單純無權限使用電腦的行為的法律（例如南卡羅萊納州的電腦犯罪法），但是需有其他目的或後續動作（例如詐財等）為條件始加以處罰的法規仍為多數。至於第二期，刑法規定的目的則開始明確地轉向物理性財產利益的保護。這一期的特色在於處罰以獲得財產上利益為目的的不法侵入行為（亦即將不法侵入電腦系統的行為當成手段而進行的財產犯罪）。這個時代的特色是除政府、銀行外，一般公司或個人也開始使用電腦系統。

第一期與第二期間的差異其實僅是反應出使用電腦處理事務的行業或個人有逐漸增加的現象而已，刑法所保障的法益仍舊是維持在傳統財產法益的範疇內。真正有質的轉變發生的是八〇年代後半起至九〇年代前半為止的第三期。第三期的重點在於智慧財產權的保護，這不外是物理性財產外，另將刑法的保護法益擴張到無形的資訊（特別是生物產業中的商業機密）之上。

此再加上，世界性的無國界網路革命已經悄悄展開，對於做為重要資本的無形資訊的保護已經不能將眼光侷限在自己本國而已，更重要的是應該如何才能夠防止透過網路由國外所進行的侵犯行為。這一種考量即成為發展到第四期規制的重要轉折點。當時縱或要求他國為國際刑事活動的合作，亦苦於他國沒有這般先進，並沒有設訂相關的類似處罰規定，在無雙罰情形存在的情事下，做為犯罪行為地的他國當然沒有義務亦無可能對美國提供國際刑事司法的協助。而美國方面，亦甚難於無告知的情形下，即從美國透過國際網路「侵入」特定他國的電腦網路系統中進行犯罪偵查活動，如果這個特定的他國也擁有同等程度的網路技術時，該侵入行為即有可能會被發覺，並且被認為是侵犯主權的行動。

在這種欠缺雙罰規定，亦無其他有效國際司法共助管道的局勢下，美國步入了第四期的規制階段。第四期為九〇年代後半到現在為止。於此期，美國開始以間接的方法保護以上的利益。保護的客體不再是系統本身（包含其內具有財產價值的資訊），而是管理系統連線的系統內部特殊保護措施，於是所欲規制的行為被明確訂為「解除或迂迴限制連線措施的行為」。至於進行這類行為後可能會進行的後續行為，例如違法取得 ID 密碼等識別符號後進行連線行為，並於電腦中所為的傳統犯罪行為，則被視為是併罰的他罪。

透過網路得利最多的國家，當然會想去積極地保障既得利益，但是在從全世界各處任何一個端末都可進行對該既得利益的攻擊行為的網路時代，若只是一昧強調自己國內既有的有形以及無形財產的保護，則根本無法得到他國的認同，於是做為最大的資訊國的美國當然會開始主張較為中性的、或較具普遍性的「犯罪類型」，以謀求其他國家的同意，並允以設定雙罰規定，以此為基礎可進行國際刑事司法上的共助（對於同類的行為兩國都同時規定是犯罪行為時，始有國際刑事司法共助的可能）。

當然僅有雙罰規定以及基於這類規定而變為可能的國際刑事司法共助是無法達成保護特定利益的機能的。因為網路上犯罪的特性，不僅在於其無國界性而已，更重要的是無痕跡性、匿名性等特性。於追查犯罪時，首重即時性的、當場的追捕，只要錯過時機，則可能會永遠無法舉發犯罪人。基於這種需要，美國開始利用國際組織，特別是先進國家組織的 G8，針對其所主張的國際性電腦網路犯罪防制政策，展開一連串半強迫式推銷活動。

例如得立即特定發信源頭的網路設計（獎勵 ISP 使用 SS7，亦即七號共通線路的訊號傳遞方式，或新的 Ip ver. 6，可於 128bit 長的 address 中包含了發信源頭、路徑等訊息）、一般通信紀錄的保存、使用者身分確認系統的確立、於國內確實執行外國所為有關證據保全的請求的程序等。其中最具有「成就」的應該算是 24 小時待命的 contact point（非 Central Authority，而是特設的機構，可獨立地、暫時性地允許外國的電腦網路警察透過網路偵測國內特定網站，或存取其資料）。現在美國正在透過歐盟、ICPO、IOEC 等國際性組織向 G8 以外的國家推廣這些政策。

在美國進行第四期的電腦網路犯罪規制活動的初期，其即已為以上新的電腦網路犯罪防制政策重新設定了犯罪的分類標準，藉此做為向世界推廣其規制政策的基礎。在我國根據老舊的觀念而制定並實施新修訂刑法條文的一九九七年，G8 即於當年的十二月間在華盛頓召開司法及內政部長會議，會中在美國的主導下使用了最新的用語—高科技犯罪。這個犯罪被定義成：（一）熟習於高科技技術的犯罪者以電腦以及電氣通信系統為攻擊標的，企圖無權限地竊取或竄改重要資訊，或意圖紊亂重要的商業、公共系統的犯罪；（二）組織犯罪的成員或恐怖份子，利用上述新的技術而進行的傳統犯罪。第一段的定義，其特定的犯罪類型可以導出獨立規制不正連線行為的法規的妥當性，而第二段的定義則除了可以達成第一段定義的任務外，另可誘使其他國家基於危機感而同意諸多的無國界、無障礙的國際圍捕技術。

日本即是在這種的國際情勢壓力下，邁出了第一步，其立法規定了不法連線行為的可罰性。不過，在圍捕技術方面，日本仍舊是維護了主權國家應有的尊嚴，而不願意直接了當地建設符合美國所要求的犯罪偵防體制。換言之，雖然日本基於美國的要求而訂立了符合雙罰規定的禁止不法連線行為的刑罰法規，但是仍舊是以日方警檢為國際性犯罪的偵防主體，而不願意讓美國的犯罪偵防勢力長驅直入日本的網路世界。日方有關網路要塞化的相關措施，例如前述「特定公共電信系統開發關連技術的研究推展法」的修訂，以及不法連線行為禁止法中關於促使連線管理者積極通報的隱藏起來的立法目的

等，處處都顯示出實現國權的企圖。如此看來，雖說網路是無國界的，其可促進全球化的進程，但是只要是牽涉到國家產業發展的問題，這些都會變成霧中看花的虛幻。

四、 結語—對我國的啟示

我國目前正處於發展經濟的歧路上。雖然現行法上並沒有任何的犯罪類型是符合於前述先進國家於發展雙罰規定的制度時所新訂的犯罪類型（於我國無任何法規可以處罰單純的不法連線行為），於能力上亦無偵防國際電腦網路犯罪的實力，但是實際上以我國電腦網路的發展狀況而言，處於競爭關係的各國以及其他跨國的國際性企業，甚有可能會透過我國的網路而進行對於他國企業或國際企業經營體的侵犯行動。亦即，我國的網路系統不僅是不安全，其甚至於可能成為國際性犯罪的天堂，因為只要經過我國的網路系統，則基本上即可規避國際性的犯罪追查行動。自己不安全也就算了，問題在於當先進國家因為我國對於網路安全的怠慢態度而產生損害，且進一步又無法進行有效的防禦動作時，其勢必會對我國採取嚴重的抗議行動。

為迴避這種情事的發生，最簡單的方法即是完全將我國納入美國等先進國家的設計中，不僅是訂立符合雙罰規定的新型犯罪類型，並且也同意讓先進國家無障礙地進入我國諸ISP中進行任意的存取資訊行為。然而，這種方法讓我國的網路系統赤裸裸地曝曬在他國的強權之下，不僅是喪權辱國，同時也會將我國國民的利益置於無限的危險狀態下。此際，或許日本所採的方法是一個可行的方案。但是，這種方案是以本國擁有強而有力的電腦網路犯罪偵防能力，且網路系統亦擁有一定程度的安全性為前提要件，而以目前的狀態而言，我國根本無法滿足這些條件。

二〇〇一年一月行政院開始留意到網路安全的問題，其透過國家資通安全會報，以行政院國家資訊通信發展推動小組NICI統籌諸般事務，並於其下設置了綜合業務、技術服務等七個工作組，企圖積極地建設起全國性的網路安全機制，同時政府也委託資策會科法中心針對資通安全進行前置作業的法制研究工作。雖然晚了日本數年，但是應該還是不算太遲。然而，問題仍舊會發生。

以日本的目前狀況而言，警方已經開始透過民間通訊機構等的研究而掌握到先進的偵防技術，而前置化的犯罪類型以及其輕微的處罰規定亦開始誘導業者進行早期的積極通報。此際，防止警方、業者聯合體制不會過度干涉網路使用者的自由或侵犯其隱私的機制，根本都沒有被建設起來。為了偵防犯罪，甚有可能會犧牲一些國民透過網路活動而創設自己的多元新形象的可能性。

網路之所以具有魅力，不在於其蘊含的商機，而在於使用者可以透過多元的訊息來源，重新組合出對於事物的新觀點，並且可以自由地移動人際關係上的定位，發現新的人際上連結，表現出自己如同變色龍一般的多樣面貌。知行合一、表裡一致等傳統的人格道德觀，早已是過眼雲煙。而這種的新人格觀，正是在二十一世紀，在一個不斷創造新秩序的複雜社會系統中，讓新世代的人們可以活得更像自己的重要關鍵。

反之，政府的力量則是主要置於既有利益或既成秩序的保障層面上，對其而言，每

一個新的變化都是一種不友善的挑戰。而就業者而言，網路使用者的每一個變化，每一項資訊都是讓其能夠分析消費者性向，並藉此發展新商機的重點。這兩個外表上不甚相同的傾向，亦即一個厭惡變化，一個積極利用變化的兩種傾向結合在一起時，兩相得利的措施將是政府所立的法賦予業者蒐集使用者資訊並予以分析的合法依據，而業者的上述行動將可提供政府控制變化時所需的資訊。事實上，因為業者所進行的資訊蒐集以及分析，進一步會導出消費傾向的塑造行動（例如新的廣告誘導活動），而只要消費傾向固定化，則政府方面亦可免於一些導因於變動過鉅而產生的不便。政府與業者兩相得利的情況下，唯一被犧牲掉的不外是做為消費者的網路利用者自行塑造自己的多樣人格的可能性。而以長遠的眼光觀之，多樣化的國民卻是國家社會發展的基本動力。

在犯罪的前置化以及使用者資訊的公開化等政策已然形成的現在，我國是否仍舊擁有調和「在國際壓力下勢必成立的產官結合體」與「企求自由多變的國民」間互相矛盾的利益的可能性？這就要看政策釐訂者是否有長遠的遠光。而筆者基本上是採悲觀的態度，無法肯認調和機制的存在可能性，不過仍舊會於悲觀中繼續努力地在自己的創造活動中展現出一種對於趨於中心化的主流傾向的脫中心化異端所為的挑戰。

參考文獻：

1. 河原淳平「ハイテク犯罪対策に関する国際的動向について」警察学論集52卷9号（1999年）。
2. 黒澤正和「不正アクセス行為の禁止等に関する法律の制定について」警察学論集52卷11号（1999年）。
3. 高橋郁夫「コンピュータの無権限アクセスの法的覚書—イギリス・コンピュータミスユース法1990の示唆」判例タイムズ1006号（1999年）。
4. 露木康浩、砂田務、檜垣重臣「不正アクセス行為の禁止等に関する法律の解説」警察学論集52卷11号（1999年）。
5. 「特集ハイテク犯罪対策」法律ひろば53卷6号（2000年）。
6. 夏井高人「アメリカ合衆国におけるコンピュータ犯罪立法動向—無権限アクセスを中心とする比較法的検討と日本法への示唆—」判例タイムズ1008号（1999年）。
7. 早川剛史「ハイテク犯罪対策に関する技術開発を促進するための新たな法制の整備について—特定公共電気通信システム開発関連技術に関する研究開発の推進に関する法律の解説—」警察学論集52卷11号（1999年）。
8. 檜垣重臣「不正アクセス行為の禁止等に関する法律」法律のひろば52卷12号（1999年）。
9. 安富潔「安全なネットワーク社会実現に向けての課題」警察学論集51卷10号（1998年）。
10. 李茂生「權力、主體與刑事法—法邊緣的論述（第四篇：回顧與展望—資本、資訊與

電腦犯罪)」國立台灣大學法學叢書 111 號，瀚蘆圖書出版有限公司(1998年)。

作者簡介

李茂生 日本一橋大學法學博士，現任台灣大學法律系 教授。教授法學緒論、犯罪學、刑事政策學、刑法總則、刑法分則、刑法實例演習、刑罰學專題研究、監獄學、監獄法、少年事件處理法理論、少年事件處理法實務、刑事社會學、「資訊、科技與法律」、日文法學名著選讀，日文電腦初級，電腦與法律資料處理等科目。

等男子真的誤信了！應該探究的是，到底這個不符事實的宣稱與錯誤，是否具有直接招致財產損失的特性在內？這正是前文所述，國內文獻上甚少提及的動機錯誤（前文貳、四）！就金錢借貸而言，甲是否就讀台大新研所根本是交易上無關緊要的事項（在其他的詐欺案型，學經歷的資格可能成為交易上的重要事項，例如甲若應徵記者但卻謊稱台大新研所畢業）；在此，乙等男子所陷於者，是一種「淑女竊窺學歷佳」而求之不得的純粹動機錯誤。在道德上，如同有人不齒乙男所為一樣，或許也有人齒甲女所為，但法律上甲不會因此受處罰。

乙男咎由自取嗎？這點非關緊要。其實，本案並不是不能構成普通詐欺罪，但是重點既不在於甲「高不高檔」，也不在於甲「是否就讀名校名所」，而在於甲於借貸當時是否存心不還？是否因而欺瞞了其履行債務的客觀能力（外在事實）與主觀意願（內在事實）？坊間八卦取向的報導者，想必不知道這個關鍵，所以也未提供任何訊息可供判讀。不過，甲果真被提起公訴，借貸當時的償債能力與意願，才是實體上及訴訟上讓人傷腦筋的爭點！

台湾におけるコンピュータ犯罪 の法的規制—その現状と問題点

李茂生*

目次

- I. 始めに
- II. 刑法部分改正の経緯
- III. 刑法部分改正の主な内容と問題
- IV. 新しい刑法条文の執行状況
- V. 終りに

I. 始めに

国際的に見て、コンピュータの生産やネットワーク関連商品の製造に関しては、台湾はすでに一席を占める地位に立っている。それだけでなく、国の政策にも関連しているが、台湾はいち早くアメリカなどの先進国の唱導するNII政策を採用し、現在光ファイバを利用するネットワーク(教育関係の無料TANETや民間業者の経営する商業sparg net)や電話回線を利用する低料金ISDNネットワーク(HINETやSEEDNET)や同軸ケーブルを利用するネットワーク(例えば東森寛頻)などがすでに全国に普及している。小中学校の通信簿さえ、電子メールを通して行われるようになっていっている。

それにもかかわらず、法的分野においては、一般論としてのサイバー・ローを論ずる論者がいるという程度に止まらず、法的整備はほとんど行われていない現状にあると言わざるを得ない。その中では、サイバー・ワールドにおける経済活動の規制に関する法律はほとんど欠如している¹。現状では、野放しの状態にあるともいえる。

勿論、現実にはサイバー・ワールドにおいて活動している人々は自身の安全や財産の保護、ひいては社会道徳の維持のため

¹たとえば、DN(Domain Name)登録の問題は前からすでに通信やネットワークにおける経済行為の障害になっているという認識があるにもかかわらず、現在になっても解決されていない。有名なYahooのDNはすでに「新建業汽車(自動車)会社」によって登録済みである。それ以外に、digital signature(法業があるもの)、現在は立法院に眠っているまま)やkey escrowやencryptionなどに関する体制も、ほとんどできていない。

めに、活動の規制に関して色々の提案や方策を論じているが、政府側の怠慢のせいなのか、現在のところ、議論の方向は政府側に傾るよりはむしろ自律や自粛の方に向けられている。リベラリズムの観点からして、他律的・強制的な規制を最小限に抑え、できれば行動する人々の自主性に任せる秩序はもつとも望ましいかもしれない。しかし、台湾では、近代化のメルクマールとしての理性的啓蒙がほとんど進行していないし、伝統的な共同体もすでに崩壊されたため、自律を行うに必要な自主的秩序を生成するメカニズムはどう探してもなかなか見つからないのである。

このような状態の下では、サイバー・ワールドにおける行為に対する刑法の規制は、その規模や法改正のスピードからして、まさに異色を帯びるものであるといえよう。刑法の改正は憲法のほどでもないにしても、国民の権益に重大な影響を与えるだけに、普通は慎重に行われるべきであるが、今回のコンピュータ犯罪関係の刑法部分改正案の場合は、今回のこの議論などが全然されずに、すんなりとできたのである。もつと奇妙なところは、その後、批判や非難なども全然見られないことである。

本論文は台湾でのコンピュータ犯罪の刑法の規制内容を紹介し、その問題点を暴き、それに法の実施状態の紹介を加え、よって今回のコンピュータ犯罪の刑法部分改正運動の後ろにある深層にスポットライトをあてることにする。

II. 刑法部分改正の経緯

台湾の現行刑法は1935年に国が最高の道義体であるというイデオロギーの下で制定された法律である。教唆犯の独立性や不能犯の処罰など主観論をもってしか解釈できない様々の規

定は溢れている。実務や学説の方も、現在でも主観説は主流の地位をしめている²。主観説の下では、もともと法執行機関の恣意が抑えられきれないし、刑法そのものも政治的に利用されやすいのである。1992年に内乱罪に関する刑法条文が改正されるまでは、(旧)刑法百条第一項のいわゆる「平和内乱罪」³や第二項の「陰謀内乱罪」によって投獄された夥しいケースはまさにその好例であった。このような状況のもとで、行政府によって推し進められてきた刑法改正運動やその成果には、刑法の根本的な精神に基づき反省が見られないのは、当然ともいえることであろう。

台湾の政府は1974年に「刑法研修委員会」を組織し、社会の変動に歩調を合わせるといふ大義名分の下で、刑法の改正に力を入れるようになった。そして、非常に短い期間の中で、「研修」を終え、1976年と1978年にそれぞれ刑法総論改正草案と刑法各論改正草案を発表した。主観主義の主軸を維持しながら、規制の範疇を拡大したという批判がなかったわけではないが、全体として異論を押さえた「順調な」法改正運動であった。

ところが、主観主義の柔軟性のせいにか、政府側はこうい

² 教科書だけは日本やドイツのそれに倣って、個人法益、社会法益、国家法益という順番に沿って、条文を並び替えている。その中で、個人法益以外の法益を「超個人法益」と名付け、一切否定するという過激な論説も出ている。ただし、これらはすべて表面上の変化である。その中身は依然として主観説(特に行為無価値論)である。

³ つまり、平和的な手段をもって政治改革を訴える人々の活動は、場合によって統治の秩序を乱すという目的をもつ犯罪行為と見なされるのである。

った刑法改正草案を立法院に提出する必要性や緊迫性に対してあまり感じていなかったまま、草案をそのまま眠られさせたのである。この間、自動車関係や石化関係の重工業を發展させようとする政府の経済政策が挫折し、新興のコンピュータ産業における民間企業の活力に注目し始めた行政府は、心機一転して柔軟な体勢を持って産業政策を変えた⁴。これは台湾の情報(中国語でいうと、資訊)社会の芽生えであった。

あとの十年間、台湾ではハイテク製品の生産ゾーンの建設などに関する産業政策が着々と執行されていた背後には、政府側による刑法改正運動も静かではあるが徐々に動き始めた。そして、ついに1990年の一月に行政府と司法部が連名で刑法改正草案を立法院に提出した。十二、三年前の草案と比べて、こをもつて構成されるコンピュータ犯罪関連の条文であった。ところが、分裂によって政治的に動揺している与党(国民党)はこの刑法改正草案の国会審議に力を入れる余裕が全然なかったため、草案がまた冬眠状態に入った。

状況が変わったのは五年後の1995年のときであった。当時、与党の国会議員である張建國と陳健民両氏をはじめ、二十名の国会議員は、刑法改正草案の中の「コンピュータ犯罪関係条文」を草案本体から切り離し、単体として国会に提案することに署名した。その提案の理由として、台湾をアジアの経済運営中心にレベルアップすること、情報社会の進展に歩調を合

⁴ その以前、行政府は産業發展に対して主導権を握ってきたが、八十年代以後になってから、段段と民間の産業發展に対して助成や指導する立場に変わっていく。

わせることなどであった⁵。

ところで、同年行政府によって提案された「電腦(すなわち、コンピュータ)処理個人資料保護法草案」が順調に国会審議を通過したにもかかわらず、刑法部分改正草案は依然として動く気配が見られなかった。劇的な変化が起こったのは、その二年後の1997年であった。「劇的」というのは、ほとんどの人はこの提案もまた国会議員が政治的舞台を欲して、でたらめに遊んだ所産であると感じたが、しかしだれもこの「遊び」を相手にしていなかった二年間を経た1997年に、急に何の論議もせず、この刑法部分改正草案は国会の「審議」をパスしたからである。

Ⅲ. 刑法部分改正の主な内容と問題点

1990年行政府によって国会に提出した「刑法改正草案」の中でのコンピュータ関連条文は、十一ヶ条によって構成されている。これに比べて、1995年に国会議員が提案し、1997年に国会の審議をパスし、総統(大統領)府によって公布され、実施に付された「刑法部分改正条文」は、九ヶ条しか残されていない。削除された二つの条文は、それぞれ「許可なしに他人のコンピュータを利用することの犯罪化」と「コンピュータやその関連設備を利用し横領罪を犯した場合の刑の加重」に関するものであった。

実は、当時行政府によって提出された(全面的)法改正草案は、刑法に限られなかった。それに、国会にはあまつた法

⁵ 立法院議案関連文書、院総第二四六号、委員提案第一三〇〇号(1995年7月5日)。

案研究経費があることにも加えて、すべての(全面的)法改正草案を(指名された)学者グループに研究案として委託し、民間の専門家の審査に付するようになった。そして、民間専門家の審査の末、刑法関係の研究報告によれば、「許可なしに他人のコンピュータを利用することの犯罪化」は、使用窃盗に等しく、行政府の刑法改正草案の中での「使用窃盗」関連条文と一緒に削除すべきであり⁶、横領に関する刑の加重については、横領罪には第二項犯罪(不法利益)が設けられていないため、コンピュータやその関連設備を利用し横領罪を犯すことがまづ考えられないということであった⁷。国会議員は以上の民間専門家の審査意見を受け入れ、1995年に刑法部分改正草案を提案するとき、以上の二か条を削除したわけである。

このような出来事からして、コンピュータ犯罪の規制に関する行政府の法案の内容は粗雑であるといえよう。しかし、これをもって学者グループの審査は丁寧に行われ、問題がないとは言いきれない。

1997年に実施された刑法部分改正の諸条文を三つの部分

⁶ 1995年での台湾の状況から見ると、コンピュータやインターネットが普及した社会においてコンピュータを利用することはすでに僅少の資源ではないので、このような行為を犯罪化するほど保護に値する法益が存在していないということがわかる。しかし、後述のように、学者グループはそのかわりに新型の不正侵入行為を適当に重罰化すべきであるということの重要性を全然感じていなかったため、コンピュータ資源の利用行為の犯罪化を時代遅れの発想としてみるのではなく、むしろ使用窃盗に関する旧来の疑念に基づいてコンピュータの無断使用行為の犯罪化に反対しただけであると考えられる。

⁷ 立法院委託「刑法分則草案評估」報告、3-88と3-108ページ(1995年)。

に分けてみることができる。それは、(一)コンピュータ詐欺罪の新設、(二)電磁記録の準文書化、(三)電磁記録の準動産化などである。以下は簡単に説明する。

まずはコンピュータ詐欺罪について説明する。台湾は日本の刑法第246の2条に倣って、第339の3条を新設した。それだけでなく、「本当のコンピュータ詐欺」の第339の3条以外に、同じ章に第339の1と339の2条も一緒に設けられている。第339の1条の行為対象は自動販売機、第339の2条のそれはATMに限られている。そして、行為態様に関しては、第339の3の不正方法とは、虚偽の資料や不正指令の入力に限られているが、第339の1と2条のそれは、単に不正方法と規定されているだけである。

第339の1条の規定によって規制される犯罪行為は、もともと軽微な窃盗で、窃盗罪の規定をもつて情状を酌量して量刑すればいいのに、わざと詐欺罪として条文を新たに設け、処罰する理由は、おそらく機械も騙されることがあるということを示したかっただけである。だから、その法定刑も一年以下の懲役に抑えられている。このような新設条文の意味はわからないわけではないが、一応贅物ともいえよう。

このような規定は別に解釈論に害を与えることがないのに対して、第339の2の規定は大きな問題を引き起こしている。第339の2条はもともと日増しに嚴重化しつつあるキャッシュ・カード犯罪に対処するため、設けられた条文である。ATMな

。窃盗罪には第一項犯罪しかないので、詐欺罪の場合は第二項犯罪が設けられている。第339の1条第2項には詐欺罪の規定格式に従って、「不法利益を得る」という文言があるが、こういった犯罪行為はまず考えられないであろう。

台湾におけるコンピュータ犯罪の法的規制—その現状と問題点 9

だから現金をおろす量の制限があることを鑑み、法定刑を普通の詐欺罪(五年以下の懲役)より低く制定されている(三年以下の懲役)。ところが、第339の2条はその対象としてATMに制限されると、類似的の犯罪行為、つまりクレジットカードの濫用の場合は、第339の3条(七年以下の懲役)を適用しない限り、適当に処罰されえないようになる。したがって、新しい解釈論として、キャッシュ・カード犯罪に第339の2条、クレジットカード犯罪に第339の3条を別々に適用するという主張が有力になっている。

だが、そうすると、第339の3条の定型による制限、つまりオンラインシステムを故意に弄ってコンピュータにある(財産関係の)データを改竄するという特別な行為態様の限定は、無意味なことになってしまう。また、この定型の制限を無視する解釈論をさらに押し進むと、次のような不適切な状態が引き起こされるであろう。つまり、カードの溢れている社会には、一旦カードを濫用すると、ATMを対象とする犯罪を除いて、その行為態様如何と構わず、該当のカード(例えば、プリペイド・カード)利用行為はオンラインシステムと関連するなら、すべて第339の3条の定型化実行行為とみなされ、重い刑に処される恐れが出てくる。

この奇妙な解釈論は、次の「電磁記録の準文書化」の条文の新設によって別の問題を起こしている。「電磁記録の準文書化」については、台湾の場合、日本と違って、法例として新しい条文が設けられている。すなわち、全刑法典にわたつ

。日本の場合は、文書偽造罪と文書毀損罪に分けてそれぞれ違う文書の定義が設けられている。これはおそらく保護法益の違いによるものである。これに比して、台湾の刑法の場合は、人の意思を表明するもの

て、すべての「文書」という文言の意味合いの範疇には電磁記録が含まれるようになっていくというわけである。他の条文での拡大適用は別として、上記の問題と関連して、解釈論上問題となっているのは文書偽造の部分である。

空白のクレジットカード・カードのうしろにある磁気ストライプに盗み取った他人のカード情報を書き込んで、偽りの消費行為を行い、よって銀行に所定の金額を自分の架空の会社の口座に振り込ませる事例に対しては、実務上、私文書偽造罪で処される。しかし、実物のクレジットカード・カードを使わずに、単にインターネットを通して、盗み取った他人のカード情報をインターネット上、偽りの買い物を行った後、銀行から消費した金額の振込みを受け取ったケースの場合は、刑法第339の3条が適用されるのである。前者の法定刑は五年以下の懲役であるのに対して、後者の場合は前述のように七年以下の懲役である。このような法の適用、または法定刑の幅の違いは、インターネット恐怖症によるものであると言わざるを得ない。

クレジットカード・カードの国際組織の情報によると、香港とマカオの中国帰還にもなつて、この二つの地域におけるクレジットカード・カード犯罪グループは中国の厳罰体制に臨んで文書偽造として軽くしか罰されない台湾に移転したため、去年(2000年)あたりから台湾はすでに日本と香港に抜きん出て、アジアにおけるクレジットカード・カード犯罪率のもっとも高い地域になつており、銀行が年間三十億台湾ドル(約一億アメリカドル)の

であるなら、「権利義務の存否、得喪を証明するためのもの」や「事実証明に関するもの」など、構いなしにあらゆる関連条文の中で文書とみなす。

●台湾におけるコンピュータ犯罪の法的規制—その現状と問題点 11

損失を蒙っているそうである¹⁰。このような状況がそれ以上悪化すると、台湾ではすべてのクレジットカード・カード犯罪に対して、その行為態様はどうかであれ、一律に第339の3で処理する可能性もないわけではない。

それだけでなく、キャッシュ・カード犯罪の場合も問題が生じつつある。もともと刑法部分改正以前は、1992年に第十一回最高裁判所刑事法廷会議の決議(1992/9/8)によれば、他人のキャッシュ・カードを利用し、ATMから現金をおろした場合は、銀行などの内部の貯金関係の電磁記録が機械の作動によつて変化するが、行為者の行為は文書偽造行為に該当しないのである。ところが、法改正後、このような行為は準文書を偽造する行為に該当するという解釈の可能性が出てきたため、実務家の中で、以上の行為は第339の2条に規定されている「不正方法」に該当する以外、偽造行為にも該当するから、五年以下の懲役の文書偽造罪で処されるべきであるという説も有力¹¹である。

このような説には一理があるにもかかわらず、キャッシュ・カード犯罪に対しては、実務上裁判官たちは依然として準文書の規定を無視し、第339の2条をもつて判決をくだしている。一見してこのような実務は厳罰傾向の強い上記の説を退けているが、その理由が不明であるだけに、犯罪状況の変化によつて、同様な行為に対して第339の2条から私文書偽造罪、ひいては第339の3条へと適用の条文を変えていくかもしれないと思われる。

¹⁰ 2001年2月27日、中国時報、13版(財經焦点)。

¹¹ 陳煥生「刑法上之電腦犯罪」刑事法雜誌42卷3号7-9ページ(1998年)。

案の定、2001年6月に、立法府が非常に複雑な審議を終えて、刑法第201の1条を増設した。この条文は有価証券偽造罪の中の一つであり、個人の財産だけを保護する詐欺罪と違って、有価証券の流通に関する信頼などの社会法益を保護するのである。その内容は次のとおりである。使用に供するため、クレジット・カード、キャッシュ・カード、プリペイド・カードなどの電磁記録(すなわち磁気ストライプ)を偽造しまたは変造することに対して、有期懲役一年以上七年以下に処するということである。その法定刑はほぼ刑法第339の1条の七年以下有期懲役と同様であった。

以上のことをおいて、電磁記録の準文書化に関連して二つの条文が今回の刑法部分改正で修訂されている。

一つは文書毀損罪の関係規定である。電子記録が文書と見なされる以上、電子記録を毀棄することは、文書毀棄罪に該当するが、毀棄のほどでなく、単にその処理を邪魔する程度(つまり、意思の表明に供するという文書の機能が妨害される)のことなら、文書毀棄罪に該当しない。このような行為(主にコンピュータウイルスの投与行為)も規制すべきであるという一心で、刑法部分改正法案は文書毀棄罪の第二項を設けた。しかし、他人の電磁記録の処理を阻害することは、文書毀棄罪の実行行為よりはむしろ器物損壊行為に類似するので(つまり、コンピュータシステムの文書処理機能の妨害)、文書毀棄罪の第二項を設けるのではなく、器物損壊罪の第二項を新設すべきである。両者の差は法定刑にあり、前者の法定刑が三年以下の有期懲役に対して、後者のそれが二年以下だけである。この一年の差異はまさに文書が毀棄されたか、あるいはその意思表示機能が妨害されたかというところにある。

以上は意味のない議論であるといわれるかもしれないが、電磁記録の準文書化に関連するもう一つの改正はそうでは

なかつた。これは信書開封罪の規定の下段の増設である。

もともと信書開封罪は無断で他人の封緘されている信書、文書あるいは図画を開くことを規制するだけであるが、法改正によって封緘などを施すことのできない電磁記録も文書として見なされるようになるので、新たな対処が必要になる。この必要に応じて、刑法部分改正法案は信書開封罪の規定の下段に、「他の方法をもって信書、文書または図画の内容を覗くこと」という文言を設けたのである。法定刑はもとの拘留と罰金(選択)にとどまっている。

封緘を開くこと以外の方法とは、コンピュータシステムのことを頭の中に入れて考えると、無断に他人のコンピュータシステムの中の保護プログラムを破壊し、あるいは迂回することによって侵入することであろう。これはコンピュータ犯罪

¹² 旧来の信書開封罪に比べ、「内容を覗く」という要件が付け加えられたが、コンピュータシステムに侵入してからその内容を覗き見しているかどうかを認定することが簡単なものではないので、實際上、勝手に(または推定で)認定するか、あるいはHDや他の電磁記録物に証拠が残っていない限り、犯罪を認定しないかという二者択一の窮境に陥るのである。例えば、PROXYの設定されているコンピュータを通じて犯罪を行う場合は、以上の認定はわりと簡単できるかもしれないし、コンピュータに関する知識を持っていない人以外、だれも犯罪者としてつかめられないであろう。結局、この新たに設けられた要件は、法執行上の邪魔になる。

¹³ ログインする権限があるものの、システムに入ってから使用権限を越えて、進入禁止されているディレクトリに侵入し、その中身を覗き見することは、「他の方法」に該当するかどうかは異論のあるところであるが、権限を設定するプログラムを破壊するか、迂回することは例

の類型の中でヴァルスをばらまくという非侵入の類型以外¹⁴、もつとも重要な犯罪類型である。そして、この犯罪行為は引き続き他のもつとも重大な犯罪を引き起こす可能性を潜んでいる前段階行為であるとも言える¹⁵。こういった重要な犯罪行為を秘密保護の章において、それにその法定刑は非侵入の犯罪類型に較べて、はるかに軽いことは、実は最初コンピュータ犯罪の概念を台湾に導入したとき、ドイツの学者ズイバー氏の所説があまりにも重要視されたことに由来するのである。

日本でも有名なズイバー氏は、その著作の中でコンピュータ犯罪を分類している¹⁶。台湾の学者の中でドイツ留学経験者は、いち早くズイバー氏の所論に目をつけ、それに倣って、コンピュータ犯罪を四つの類型に分類していた。コンピュータ操縦(不正操作)、コンピュータ破壊(プログラムの改竄など覗き見やコピー)、コンピュータ破壊(プログラムの改竄などを通してその機能を破壊すること)とコンピュータの無断使用

外としてみるべきではないと思われる。

ちなみに、台湾ではコンピュータ・プログラムの機械に対する一連の作動命令であるが、人間の意思を表明するもの、すなわち、文書と見なされていない。

¹⁴ もちろん、ヴァルスをばらまく行為もシステムに侵入してから行うことが考えられる。しかし、ヴァルスをばらまくには、必ずしも進入することを必要とするわけではないのである。

¹⁵ だから、こういった犯罪行為の侵害法益を論ずる場合は、単に個人の秘密だけでなく、他の財産法益や公共秩序に対する公衆の信頼などの危殆化も頭に入れるべきであろう。

¹⁶ ウェルリッヒ・ズイバー著、西田典之、山口厚訳「コンピュータ犯罪と刑法」41, 116-123ページ(成文堂, 1986年)。

●台湾におけるコンピュータ犯罪の法的規制—その現状と問題点 15

(使用窃盗)などはそれである¹⁷。コンピュータがまだ普及しておらず、インターネットも雲の上のことに等しい当時(七十年代の後半から八十年の前半にかけて)にとつては、このような犯罪行為の分類は確かに進んでいるところがあった¹⁸。その後、コンピュータの普及やインターネットの建設に伴って、九十年代の後半から、段階とコンピュータ犯罪の類型を動的に把握する説¹⁹が出てきたが、時間的に遅すぎただけでなく、こういった新しい説は量と質の両方で従来の有力説に抵抗する力を持たず、立法論としても複雑しすぎて、簡単に現行法に手を加えるだけで法改正を遂行することのできる旧分類にかなわないので、刑法部分改正草案にほとんど影響力を発揮することができずに異端視されていた。

こういった事情の下で、旧分類の下でもつとも疑問視されてきたデータの窃盗問題は議論もされずに新しい条文に化したのである。

三種類の新しい条文の最後の一つは、今回の刑法部分改正の諸条文の中でもつとも奇妙なものである。それは電磁記録の準動産化である。改正された刑法によると、窃盗罪の章に限って、電子記録が動産とみなされる。しかし、なぜ全財産犯罪

¹⁷ 林山田「電腦犯罪之研究」政治大学法学評論30期(1984年)は、その草分けの存在である。

¹⁸ 夏井高人「アメリカ合衆国におけるコンピュータ犯罪立法動向—無権限アクセスを中心とする比較法的検討と日本法への示唆—」判例タイムズNo.1088, 100-102ページ(1999年)を参照。

¹⁹ 李茂生「権力、主体と刑事法」182ページ以下(国立台湾大学法学叢書111号, 1998年)、蔡美智「電腦黑客的罪與罰—談網路入侵的法律問題」貴州法務透析1998-7, 17ページ以下(1998年)。

に拡大しないか、電子記録の窃盗という行為の態様はどのように定義すべきか²⁰については、現段階で曖昧のままである。実務上、この条文が適用されているケースは一件もないことからして、わけのわからない法改正とも言えよう。

IV.新しい刑法条文の執行状況

以上説明したように、コンピュータ犯罪に関する台湾の刑法部分改正は、体系的で動的にコンピュータ犯罪行為を類型化した末、行われるものではなかった。それは、第339の3条のような先進的な条文が設けられているにもかかわらず、全体的に見て、相当古い犯罪行為の分類に従って、ばらばらに部分修正を行った「粗雑な全員集合」であるともいえる。その実用性については怪しいところがあった。

それにもかかわらず、国会ではほとんど議論が交わされなかつたし、裁判官や検察官が何らの疑問をも表明せずに拍手を持って新規定を歓迎し、「コンピュータ犯罪と法の施行」という名の研修会に何回も熱心で参加しただけでなく、検察側はもう一歩進んで数名の検察官を召集し、高等検察署にコンピュータ犯罪防止センター（高検署電脳犯罪防制中心）を設置したのである。勿論、第一線の犯罪捜査機関としての刑事警察もこの一連の動きから欠席するわけには行かなかつた。新法の実施に応じて行政院（府）内政部警政署刑事局は、いち早くコンピ

²⁰ これはおそらく、電子記録をコピーしてから原本を削除することを意味するであろう。文書毀損罪の法定刑は三年以下の懲役であるということからして、毀損にコピーをプラスして、窃盗罪の五年以下の懲役に処するということも考えられる。

●台湾におけるコンピュータ犯罪の法的規制—その現状と問題点 17

ュータに関する知識をもつ警察十数名を集め、偵察第九小隊（いわゆる電子警察である特殊の警察で、偵九隊という略称で有名である）を組織し、コンピュータ犯罪の摘発の任に当てさせている。

この偵九隊の隊長を務めている李相臣警官の統計によると、法改正後から去年（2000年）8月までの間、摘発されたコンピュータ犯罪（判決確定されたケースも含めて）は総計27件であった²¹。四年の経過だけで、27件のコンピュータ犯罪が摘発されたことは、台湾の犯罪事情からして確かに驚異たる「数字」である。ほとんどの法執行機関はこのような報告に元気をつけられたそうである。法を改正し、専門の偵察機関を設けるということだけで、台湾でのコンピュータ犯罪の趨勢を抑えることができるという意見をもつむきさえできたほどであった。

ところが、20世紀八十年代の知識を基礎にできた「新型犯罪」の分類に基づいて法改正を行い、そして僅少な人しか新法の執行に投入するという手段だけでコンピュータ犯罪に抵抗することができるかについては、疑問をはさむ余地のあるところである。

李氏の報告の中身をよく分析すると、妙なことが発見されている。つまり、この27件のケースの中の大部分は、インターネットを通して行う伝統的犯罪であるということである。例えば、脅迫、猥褻物散布、不法行為煽動、違法薬物販売、賭博、経済的信用妨害、公然侮辱、伝統的詐欺などがそれである。ヴ

²¹ 李相臣「電脳網路犯罪實務」第四期檢察官資訊法律研修會講義要綱（資策會科技法律中心，2000年）。

イルスの散布やインターネットにおけるCD犯罪やシステムの侵入によるデータの改竄またはコピー²²などは、五件しかなかったし、その被害額からして、世界でも有名なCIHウイルス案以外は、大した犯罪ではなかった。それに、ほとんどの確定されたケースは執行猶予または短期刑に処されている。

さらに、もっと驚くべきなのはこれら伝統的犯罪の中で、以前では見られない行為類型があるということである。例えば、自分のホームページにおいて他のホルノ関係ホームページへのハイパーリンクを指示するだけで、猥褻物散布罪に該当するとか²³、自分のホームページにおいてアメリカのあるホームページからコピーした爆弾を製作する方法や爆弾を自作する場合受傷した写真などを、翻訳した文字とともに展示することは、不法行為煽動罪に該当するといった判決である²⁴。これらの行為はインターネットと関係しない限り、おそらく摘発されないであろう。

とにかく、摘発されたケースの量と質に関するデータだけで、台湾におけるコンピュータ犯罪事情を論断するのは危険

であり、無責任のことでもある。實際上、例えば、銀行(特にシタイ・バンクのような大きな銀行)のコンピュータシステムが侵入され、その顧客の貯金データが改竄されたというような噂は絶つことがなかったし、CD犯罪が夥しいし、インターネットの中にウイルスが横行している。台湾でのネットの安全性に関しては油断のできない状態になっている。事実上、現在摘発されたコンピュータ犯罪は氷山の一角でしかなく、そしてその中でのもっとも軽微なケースである。

以上は台湾国内の事情に関するものだけである。しかし、コンピュータ犯罪と言えば、もっと問題となるのは、そのボーダーレスの性質である。

国連の活動から排除され、NGOの活動さえもろくにも参加していない台湾は、現在国際関係における孤児と呼ばれている。この数十年の間にほとんど公式的な国際会議や活動に参加していないかった。もちろん、国境を越える犯罪の防止に関する国際会議の決議などは、台湾に対してはほとんど効力のないものに等しい。こういった事情の下で、台湾は両罰規定の要請に忠じて法を改正したり、24時間のCP体制をとったり、ひいては128 bit長のlogin記録を許すIP ver. 6を採用すること²⁵は、一切行っていないのである²⁶。

²² 台湾で摘発された最初の典型的な侵入型コンピュータ犯罪は1998年5月に送検した「黄姓軍医侵入案」である。黄という徴兵で軍隊に入った医学生は、ハッカーの技法を利用して、各有名なISPに侵入し、そのシステム・プログラムを破壊したり、顧客関係のデータをコピーしたりしたのである。実害は大したことではなかったが、インターネット族に大きな不安を煽いている。

²³ 新竹地方法院刑事判決，八十八年(1999年)易字第126号判決。または李茂生「網頁中設定色情網站超連結行為的刑事責任」光刊46号ページ(1998年)を参照。

²⁴ 李茂生「執法人員的網路安全恐懼症—無政府文件集的省思」光刊50号ページ(1998年)を参照。

²⁵ 現在諸ISPの中で、HINETを除いて、ログファイルを保存する設備をもつISPが一つもないというのは現実である。馮震宇「網路使用犯罪00年」を参照。

²⁶ もちろん、ここでは決して無条件にこういった先進国の要請を受け入れるべきであると主張するわけではない。先決条件として、他国が国際犯罪の偵察という名目をもって恣意的に自国のコンピュータシ

それにもかかわらず、經濟の舞台では台湾は欠席しなかった。そうすると、國際級のハッカーたちは、一旦わりと進んでいる台湾のネットを経由し他の国のコンピュータシステムに攻撃をかける場合、そのもとのルートがほぼ隠蔽できるようになる。現に台湾は國際的コンピュータ犯罪者グループの天国になりつつあるという懸念を拭き取ることができないのである。

以上のことは段段と常識になってきている現在では、依然として自信満々でコンピュータ犯罪者がコントロールされていると言いつつ、台湾の法執行者の態度には、なんか怪しいところがあるといわざるを得ない。おそらく、法改正や新法の執行などの行動の背後には、犯罪をコントロールすること以外の企みが潜んでいるであろう。

コンピュータ犯罪の概念が台湾に紹介された時期は、十年代の初頭である。当時、官民合わせて全台湾で千六百五十個のコンピュータシステムが存在しなかった²⁷。それにもかかわらず、台湾政府はすぐこの新型犯罪に注目し、学者と実務家(当時僅少の技術者をも含めて)百人近いを司法官訓練所(つまり司法研修所)に集め、研究会を開いた。そして、研究会で発表された論文や会議記録などを一冊の本²⁸にまとめ、その後の三年間、三刷したのである。

それ以来、コンピュータ犯罪に関する論文は雨後の竹の子のように現れ出ている。しかし、その後十年の間、実際の犯罪は一件も報道されていなかった。日本やアメリカなどと異な

って、台湾の場合は、コンピュータ犯罪元年といえる大きくてセンセーショナルな事件がなかった。強いていえば、1994年から1995年にかけて発生したエゾン事件は、それに当たる。それにしては、日本の三和銀行事件とは比べものにはならなかった。

事件の経緯は以下のようである。1994年にあるものが台湾での香港エゾン会社から離職し、新しい会社に転職した。転職後、香港エゾン会社に対する恨みで、以前熟知したスーパーアイザーのパスワードを利用して、新会社のネットを通して香港エゾン会社のコンピュータシステムに侵入し、そのデータベースにあるモジュールの中の六行の順番を入れ替えた。香港エゾン会社はこの行為を察知せずに、入れ替わったモジュールに基づいてICチップを作ったが、作動不能の不良品になった。これをもって、香港エゾンは当時の著作権法第九十三条第一項第一号に基づいて告訴を提出したが、著作権の所有者が日本のエゾン会社であるため、当事者適格性には問題があるという理由で、その告訴は不受理の羽目で終わった²⁹。

この事件はラスコムを通して一時的に大騒ぎになって、刑法部分改正の切っ掛けの一つにもなった。ところが、法改正や法施行機関の能力の増進には不十分なところがあるだけでなく、予防措置として金のかかるコンピュータシステムの要塞化などの動きは、政府側および企業側ともに見かけられなかった。唯一見られる顕著な変化は、インターネットにおける言論の規制、猥褻物の流通の禁止、賭博の摘発などが厳しくなっ

²⁷ ムに侵入することを阻止できる体制を敷くべきである。

²⁷ 莊耀春「電腦犯罪」電腦犯罪問題研討會實錄218ページ(法務通訊雜誌社, 1985年)。

²⁸ 前掲註の「電腦犯罪問題研討會實錄」。

²⁹ 八十六年度(1997年)易字第470号, 台湾台北地方法院刑事判決。

いることである。

主観主義の流行っている台湾では、これらの行為を禁止するには、法改正し、専門の摘発機関を創らなくても、旧来の体制で十分間に合うのであるが、政府はわざと大きな動作をとり、一方で国民の不安を煽ぎながら、他方自分自身の動きに対して正当化の基礎をつくった。そして、この動きとは新しい時代における新しい社会倫理(の一部)の創設である。

大澤真幸氏のいうように、理想の時代が終わり、虚構の時代に突入する場合は、真実味のある理想の喪失という空白を埋め立てるには、虚構への反転として終末論が提唱されるようになる³⁰。台湾の場合は、オウムの行ったサリン事件ほどではないが、主役が政府であるということはやはり注意すべきである。

「反攻大陸」というスローガンの中で、台湾の国民たちは「整頓、清潔、簡單、素朴、迅速、確實」の生活を強いられ、軽工業と加工産業に一生を捧げた。個性を失いながら、一応「理想」に向かって奮進している人生を送ってきたわけである。だが、八十年代の後半から、こういった「理想」は戒嚴令の失効によって急に失われた。そして、数年後、「他律的理想」を持たない台湾の国民は不条理なインターネットの世界を味わい始めており、カオスの中で自分なりの複雑系を創ろうとしている。ところが、政府や社会における支配階層は、コンピュータやインターネットを新世代の資本の一種としてみるようになり、勝手に動いていくデザインツクリのない国民が新秩序の建

³⁰ 大澤真幸「虚構の時代の果てーオウムと世界最終戦争」37-88ページ(1996年、筑摩新書)。

設に相応しくないと考えるのである。

そこで、政府は教育改革を行い、義務教育の延長可能性をはかったり、専門学校を大学に変換したりして、ニュー・デザインツクリンを積極的に作り出すメカニズムを試運転しはじめている。他方、こういったメカニズムは長期間教育や一律的な生活に我慢できない夥しい中退生を生み出している以外、その硬直的な教育方針の下で、新世代の産業に柔軟に適応できない高学歴のものをも産出している。前者は少年犯罪の予備軍になるのに対して、後者は主にインターネットの世界を漂い始める。前述した台湾のコンピュータ犯罪対策は、まさにこれらの高学歴者を対象とする消極的な「再」デザインツクリンのメカニズムの一面をあらわすものである。だから、そのあらゆる面で、何らかのノスタルジーの雰囲気も漂っているわけである。

社会生活を脅かす重大な新型犯罪の抑制に力を入れないで、他の目的のために、刑法を操作し、国民の心や生活態度を弄る政府に対しては、学者としては許すわけにはいかないはずである。ところが、最後の防衛線といわれる学术界も陥落しつつある。近頃、国際的に児童ポルノのことは話題となり、コンセンサスを得ているようになる。この趨勢に乗って、刑法学者の中で、害された児童(未成年者)がなくとも、合成のポルノ写真も禁止すべきであり、このような写真自体が邪悪であるから、単純な所持でも罰すべしと、主張し始めているものも出てきた³¹。これはまさに主観主義刑法理論の極致である。

³¹ 高玉泉「論國際網路上児童色情資訊之法律管制ー兼評我國兒童及少年性交易防制條例之相關規定」政治大学法学評論60期195-197ページ(1998年)。

V. 終りに

最低の道德基準としての刑法の動向は注目し値するところである。というのは、刑法に規制されている行為の中で、「法定犯」と呼ばれる犯罪行為のカテゴリーがあるものの、これらの行為の規制は現在の社会的共同感情をあまり離れてはいないからである。しかし、社会的共同感情とは何か。

これはおそらく理性的会話を通して構築されたものでなく、逆に社会階級の中での上級階層の人々は、生存を求め人間の深い欲望に注目し、排除と差別のメカニズムを利用し、もつとも凄まじい法的規制の体制を敷くことを通して、創られたものである³²。デュルケムの言い方に換えると、次のとおりである。社会が分業によって進化すると、連帯が薄くなるが、社会支配階層にとつては、これは混乱で我慢できないことである。従つて、彼らは段段と社会に尽くすことをやめるようになる。このような事態を防止するため、統治者は儀式的な刑法を利用し、社会での悪(不都合なことだけであるが)を暴いて処罰することを通して、社会連帯を厚くするというわけである³³。

刑法は以上のような一側面を有するのである。しかし、人間社会が存在する限り、人間の生存欲望が消えない限り、この刑法の悪き側面は厳正たる事実としてわれわれの目の

³² 今村仁司「近代性の構造—「企て」から「試み」へ」208-225頁(講談社, 1994年)。

³³ ジェイムズ・M・インゲナラリテイ著/松村良之・宮澤節生・川本哲郎・土井隆義共訳「刑事法の法社会学—デュルケム・ヴェーバー・デュルケム—」137-145頁(東信堂, 1994年)。

前に攀えているであろう。そして、これを少しでも和らげるには、政治や経済などの体制から幾分独立した司法に頼らざるを得ない。この場合、歴史の教訓からできた、法解釈をコントロールする理論が必要になる。これは客観主義の刑法理論に他ならなかった。

主観主義の刑法理論は以上の側面を反省もせずに受け入れ、あるいは正当化するものである。支配階層は凄まじい法的規制を利用し、新しい社会通念か、いやもつと正確に言えば、社会連帯を作り始めているにもかかわらず、主観主義に支配されている司法がコントロール体制や規律メカニズムに荷担すること以外何もできなかった。

本文は以上のような刑法的規制を紹介し、その執行状態の分析を通して、当の規制はいかに人間の活動の計り知れない可能性を制限するかを暴くのである。台湾の社会は現在まさに物凄い勢いで動いている段階にある。政治問題によって鎮圧された静かな社会から解放され、目的もなかつたただひたすらに揺れ始めている。今まで台湾では、人々はすべてアレンジされている人生や社会学によって設計されたプログラムに従つて、支配者のいう通りに確定されていた道を歩んできた。古い支配体制が崩壊された現在では、国民たちは不確定的な未来に面して、すべもなく人生の痛みを感じ始めている。籠の中に養われてきた鶏が急に野原に野放しされたように、台湾人は現在戸惑っている。しかし、戸惑っているが、不確定的な人生の可能性から生じた痛みを克服するたびに、人々が生への欲望を感じ始めている。これは本当の自律性や主体を獲得するための第一

歩である³⁴。その戦いの空間として、サイバーワールドが存在している。そして、そのもっとも大きな敵はまさに主観主義を基本教義とする刑法執行機関である。

サイバーワールドでの戦いは幕をあげたばかりなのに、すでにぐったりする人々にとつて、2000年12月の出来事は勇気をつけることであろう。労働者の合法的権利を守るために、鉄道線路の上に座り込んで電車の運行を阻止することで当局と資本側に抗議した末、公共交通安全妨害罪で一年の懲役に処された烈士が、受刑してから半年経った国際人権日において、恩赦で釈放された。しかし、これは政治人物の遊びごっこかは、誰も確定の答えをくれないし、この事件をもつて裁判官たちの考えが変わるとは限らないのである。

台灣電腦犯罪之法的規制

— 其現狀與問題點 —

中文摘要

台灣於1997年訂定了有關電腦犯罪的刑法部份修正條文。就當時有關電腦網路犯罪的國際性規制傾向而言，這些條文都已經是有點落後，縱或是如此，從立法過程以及內容而言，其草率的情形是已到達令人瞠目結舌的地步。

本文將這些條文分成三部分予以解說，一為電腦詐欺罪的新設，二為電磁記錄的準文書化，三則為電磁記錄的準動產化，並一一指出其缺失的所在。

於九〇年代的末期，基於八〇年代的知識制定「新的」刑法規範一事，本來就已經是非常荒謬，此再加上，除了一些研討會或研討會外，台灣就電腦犯罪的防制僅投入了微薄的人力與物力，於這種情形下，數年後就新修訂條文的實施狀態，政府亦僅能提出令人質疑的成績單。

於詳查半官方的資料後，本文發覺官方所揭發的電腦犯罪類型，大體上都是一些利用電腦網路所進行的傳統犯罪，而且就已確定的案例而言，所科處的刑罰通常都是短期自由刑、罰金或緩刑。大張旗鼓的結果，竟然僅能達成這種程度的結果，到底這一連串的活動其真義何在？難道台灣的電腦網路犯罪的實際情況並不嚴重嗎？於網路無國界的現在，難道台灣不會成為國際犯罪組織的犯罪行為的跳板？

本文認為，如今政府僅是利用風行於學界以及實務界的主觀主義刑法理論，透過新型犯罪的揭發，標示出雖然結果不嚴重但是行為可議的「不妥行為」而已。

³⁴ 森岡正博「無痛文明論(一)」弘教44号62-96ページ(1998年)。

於理想的時代已經結束，社會正一頭衝入虛構的時代的現在，為了翻轉虛構的假象，通常都會由新興宗教等提倡世界末日論，聲稱世界已經毫無秩序，處處充滿著令人無法忍受的不妥當行為，藉此企圖求取暴力重整秩序時所需的新具體立足點。在台灣，不是由奧姆真理教等暴力團體來進行世界末日論的宣導，反倒是由政府來主導這件事情。而世界末日論（易言之，網路無秩序論）的目的僅在於新世代的人類的暴力性再規訓而已。

主觀主義的刑法理論過度地重視行為無價值的部分，所以根本沒有力量抗拒這種局勢，而所謂的刑法謙抑性等原則性的論述，也僅能在前後矛盾的刑法教科書中的某頁裡苟延殘喘。於這種情形下，所會被犧牲掉的僅是國民於新的世代中本來可以獲得到的無限發展可能性。

由兩岸海上走私行為論準走私罪

周成瑜

目次

- 壹、前言
- 貳、立法經過及立法目的
- 參、自「大陸地區」私運物品進入「台灣地區」走私行為之適用海域範圍
- 肆、自「台灣地區」私運物品前往「大陸地區」走私行為之概念
- 伍、在公海以接駁方式私運大陸物品進入「台灣地區」之行為概念
- 陸、結論

我國電腦網路犯罪的虛像與實相

國立臺灣大學法律學院 李茂生

摘要

網路科技日新月異，帶來無限的希望也帶來了無限的不確定性。就勇於創新的人而言，網路是代表了新機，但是對守舊的人而言，這卻代表了混亂。那對於擁有許多既得利益應該是屬於守舊一派，但是又掌握了時代先機的人而言，網路到底代表了什麼？

本文首先立於遠較法律制度更為寬廣的角度，分析這類階層人士或國家於網路時代所採的新對策。其謀略式的法運用，是有一定的脈絡可循。先進國家透過國際性的活動，不斷地推銷新的網路規制法律制度，而其中頗具特色的即是新的犯罪類型以及偵防技巧的發明。其目的不外是利用國際的力量來保障自己國家或人民的利益。

我國其實於最初即已留意到這種新型犯罪侵害國內各類秩序的可能性與嚴重性，超乎現實狀況的電腦犯罪類型的採用，以及立法上的建言等，都足以證明當時為政者以及研究者擁有足夠的睿智以及敏銳的眼光。可惜的是，於學術以及實務的大拜拜後，我國卻缺乏有系統的追蹤與補強，這種怠慢導致現在不管是刑罰規範抑或執法能力、狀態方面，都呈現出一種脫離國際性趨勢的光怪陸離現象。抗拒不了使用高科技的真正電腦網路犯罪，但又不得不執行精緻老舊的新法規，這是目前法執行狀態的困境。

本文並不是想去建議我國應該立即趕上國際趨勢，並為了先進國家所推廣的新秩序而努力，對我國而言，這並不是應走的路線。現在必須考量的是放棄這數年來錯誤的執法政策，正面考慮強化立法與執法的能量，一方面抗拒阻國外勢力的入侵，另一方面也能保障網路於文化發展方面的正面機制。

壹、前言

於國內討論與電腦相關的犯罪時，八〇年代使用電腦犯罪一詞，而九〇年代後順應網路的發達，論者開始使用網路犯罪這個名詞。表面上似乎是後者取代前者的範疇，但事實上二者間的範疇並不是替代關係，而是前者廣、後者狹。網路一定利用電腦，但是電腦並不一定要連線。因此，所謂的電腦犯罪其範疇應該廣於網路犯罪。¹

以上的形式上定義範疇的議論，貌似無任何意義，但是只要詳查有關這類犯罪的類型分析論述的內容，立即可以發現這種的議論其實是有實質意義存在。簡而言之，因為觀察的重點從一般的電腦發展到連線的電腦，或甚至於到電腦與電腦間的無限連結空間時，觀察點的變化會引出所重（保護）利益的變遷，而這種變遷也同時會牽動犯罪類型的重心移轉。在我國的情形，更重要的是當犯罪類型的重要點開始轉變時，立法方面無法跟進，或縱或可以跟進，事實上的偵防能力也無法隨著時代的變動而立即提升。在這一種的情勢下，首當其衝的犯罪偵防機關，若不是採舵為心態繼續槍斃太平，即是盡其所能開發具有新型外衣的「傳統」犯罪，以製造民心（民怨？），企圖以民間自衛的能力來防遏新型犯罪的發生，並以創造新秩序的方式維護住這個已經逐漸式微的傳統秩序。而我國有關這類犯罪的立法以及執法的虛像與真相，正是如此。

本文稱這類的新型犯罪為電腦網路犯罪，並將重點置於「網路（的特質）」之上，嘗試描繪出由電腦犯罪發展到電腦網路犯罪的國際性歷程，之後再佐以我國立法與執法情形的描繪，襯托出我國有關電腦網路犯罪的法規制的實像與虛像。然而，所謂的虛像或許僅是以先進國家的觀點進行觀察後的所得，就我國本身而言，這不是虛像而是實像。實像與虛像之間並不存在任何實體的問題，而僅有觀察點的不同而已。重點在於，當國內自認的實像形成後，如果仍舊墨守於國內的觀點進行反論（例如，按我國的現行法進行批判性的法解釋等），則系統的進化將會永遠停頓在靜止的狀態。所以本文的目的並不僅止於利用外的觀點解構國內實像，進而將國內的情事以虛像的方式暴露出來而已，真正的目的還更在於當兩個形象得以並存時，實像的虛像式說明將引起被稱為虛像的實像系統本身的變化。而這個變化將會使得系統更加複雜，更加具有抗壓性，藉此可以生存在於幾近混沌的現象中。

為達成這個目的，以下本文將分成三部分來進行論述，首先說明基礎的社會背景，然後以國際性的觀點說明犯罪類型的演進以及立法、執法技術方面的進展，並烘托出最新的論述與先進國家全球性資本政策間的關係，最後基於這個國際性的觀點，將國內執法人上光怪陸離的現象披露出來。於結論的部分，本文將會提示作者對於我國未來相關刑事政策走向上的建言。

貳、資本與網路

如眾所皆知，電腦網路是起源於美國的國防需要。美國於六〇年代時即於西海岸的洛磯山脈東南端海拔一千八百公尺處成立了核子戰爭司令部。同時，美國為了避免核子戰爭發生時指揮系統一瞬間毀於核子攻擊，於是發展出將指揮系統分散到各個以網路連結起來的據點，而各個據點都能獨立地發揮全面性的指揮功能。這個司令部於冷戰結束後，不僅是沒有撤銷，其更改制成北美航空宇宙防衛司令部（NORAD），除了負責蒐集地球上所有衛星、飛機、船艦的情報外，另集中處理由美國國家安全局（NSA）所竊聽得來的所有已經破譯密碼的通訊情報。事實上，一連串的地域紛爭，例如一九九一年的沙漠風暴或一九九九年的科索沃戰爭等，此司令部都發揮了一定的網路戰爭機能。²

這種當初為了達成國防目的而架構的電腦網路，當然會具有匿名性、無痕跡性，無時空限制以及得大量傳輸訊息等的特性，但是更重要的是其為了防止系統癱瘓而設計出來的「脫中心化」的架構。所謂「脫中新化」的架構，換言之，亦即在網路的世界中任何一個節點都是中心，或都是可取代中心發揮作用的代用品，嚴格說來，何謂中心何謂端末一事，於網路中並不是非常重要的事情。

當網路方面的技術日益成熟，首先留意到網路特性的不外是最為靈巧、敏感的產業界。產業界所著目的是電腦網路上訊息的大量快速傳遞以及處理的現象，這種功能不僅是有助於新產品的開發、客服等訊息的整理，其甚至於可以進一步發展成新的廣告機制。果然不出所料，數年後這種的電腦網路運用創造了新的商業契機。不過，同時電腦網路的脫中心化以及匿名、無痕跡的特質，也引起了惡性的競爭和企業某程度的脆弱化。詳言如下。

首先，因為電腦網路的脫中心化性質，使得許多人士於無雄厚資本的情事下，亦湧身投入網路商業中，造成所謂的dot.com現象，這些新興的業者雖然最終在一片合併與結束營業的哀號中應聲倒地，但整體的商業秩序已經大受損傷，這還不

其嚴重，其次更令人憂心的是企業界的脆弱化。許多積極利用電腦網路的公司行號，雖然大力重開新的商業機制，但是卻完全忽略了這個新機制容易被侵犯的脆弱性。於尚未完成要虛化的準備，而DN (Domain Name) 登錄、電子簽章 (digital signature)、認證 (key escrow 或 encryption 等) 制度等都尚未成熟之際，冒然大量使用電腦網路進行商業活動一事，僅是引發了別有用心者利用網路的匿名以及無痕跡的特性，以獲取不正暴利的興趣，而這些別有用心人士的行為，不僅是無法全然以傳統法律予以規制，縱或得以予以規範性的規制，實際上其形跡也不易被查獲。姑不論這些目前的困境，問題的重點應該是為何縱或知道這些困難，企業界仍舊是一頭沒入洪流？其實，這事涉到資本主義的發展，當資本發達到一定的程度，資本的重整與轉型是勢在必行，企業界若不能跟從這種的發展，則其也僅剩下破滅一途而已。

資本主義至今共有四個生命週期，各週期都有其生產及消費的特質，也各自擁有不同的資本型態。³於物質缺乏的時代，人們致力於農產品的改良，其所擁有的資本是遺傳因子。其後經過產業革命，人們開始從事單一產物的大量生產，生產日益富裕化，而此際其所運用的資本不外是經濟因子。而後，整個產業開始多元化、相對化，相應於此，產物轉化成多樣但少量生產，並且透過資訊的傳遞、活化物流，讓世人能夠從多樣但少量的產物中組合出個人的特色。此階段的資本被謂為文明因子。

以上的三個生命週期都是以物質為中心，所有有關資本的論述，若不是採唯心論的立場，主張主觀控制客觀，則是反其道而改採客觀控制主觀的唯物論。但是不論採取那一個立場，終究所謂的主客二元其實僅是意指主客合一情境下的主從區別而已。

真正分離主觀與客觀二元，讓二者互相交集、影響，但又分別擁有兩套不同的系統一事，是要等到資本主義進化到第四生命週期的此刻始有眉目出現。資本主義的第四生命週期的資本是為文化因子，人們開始從事與物質生產無直接關係的創意生產，而且消費的重點也由客觀物質的消費逐漸轉移到主觀意念的消費上，這種發展形成了兩套生產及消費系統。簡而言之，人們開始理解到人類慾望的滿足不僅是透過物質的生產以及消費始能達成，經過主觀資訊等的生產與消費，亦能獲得另類的滿足。異類的日本卡通 Serial Experiments Lain 或美國電影 Matrix (駭客任務) 都表達了藝文界對於新世界誕生的期待與恐懼。

其實第四生命週期的誕生是有賴於第三生命週期時產業界大量利用電腦網路從事生產以及消費的活用資本的舉動。產業界以政府為後盾發展了商業電腦網路，深入社會中，從基礎的光纖、同軸電纜、ADSL、無線傳輸等物質建設，到訊息的

創作與傳遞，在在影響到人們的現實生活。當然，當世人被商業廣告所吸引而進入網路世界後，其自然會發覺與其被動接受資訊 (其實是被規訓) 倒不如積極創造資訊是要求得有趣。此再加上網路的脫中心化，導致以往傳遞訊息的一對一 (例如電話) 或一對多 (例如平面媒體) 方式開始轉型到多對多的訊息傳遞模式。每個人都可以將自己當成訊息的創造者、傳遞者以及接收者，況且又有匿名性的特質可以免除傳統道德或甚至法律的拘束，這更加地刺激了一般民眾活用網路創造自我的興趣。這些現象在在顯示出與傳統的前三個生命週期迥然相異的新文化的誕生。網路之所以被稱為最後現代的場域，而其中的生活態樣該視為是人類慾望的無羈絆的釋放，其理由正在於此。

總而言之，第三生命週期時的網路利用，使得產業界一方面得 (透過廣告的擴散以及人力節約) 無限擴張勢力範圍，但同時也帶來了產業的脆弱化。而第四生命週期時的網路生活，則更是改變了生產與消費的模式，甚至於創造出一個新的文化，且這個文化含有破壞傳統產業基礎典範，亦即勞動與性 (的節慾) 的規訓的潛在能力⁴，這對傳統產業而言，不外是當前威脅到其生存的最迫切的危機。

現在正值第三生命週期與第四生命週期交會之際，文化態樣以及生活模式正在激烈地變動中，做為以國家極端的物理性暴力為後盾的最终社會控制手段的刑法，會加重處罰或新訂犯罪行為類型以求秩序的回穩，這本是預料中之事，也是刑法這個法律系統於綱要設計上的根本。不過，這種刑法的保守傾向，若被忽用，則情事將會變得非常惡劣。

對於以第三生命週期為最高發展狀態的傳統產業而言，為維護其脆弱化的結構，並進一步於第四生命週期中重新塑造合乎其理想的人的形象，其會用盡所有的社會影響力，這是在所難免的事情，恐怖的是當緩不急之際，企業界亦會藉著其政治以及經濟上的優勢，主張應該重新檢討刑法法規，企圖藉著刑法的上述宿命性暴力謀取新的出路。而當刑法的功能不再是當前最終法秩序的維護，反倒擴張到新秩序的創造時，刑法的執行將會帶有儀式性的色彩，其執行狀態亦會有恣意的選擇性執法現象產生。這是歷史的教訓，也是涂爾幹的教示，但是當局者迷，我們通常都會在當場忘記這個教訓，而僅於事後做一些的歷史回顧，並再度地進行無意義的反省而已。

本文作者無意將自己視為歷史外的第三者審級來審判當前社會上有權有勢的一群，這未免過於自我膨脹。以下作者僅是憑著社會人文學科的工作者的良心，忠實地記錄下這段終究會被視為歷史而予以研究的現在。

參、電腦網路犯罪的分類以及立法概況

八〇年代初期的一九八三年，我國僅有一千六百五十六套電腦系統，雖然比諸一九七四年的六十九套而言，這是令人驚異的成長，但尚難謂我國已經步入資訊化的時代。在當時 2 bit 的漢字處理系統（主要是由日本開發出來的文字處理系統）尚未成熟，但是已有論者將外國的文獻引進，開始談論「電腦」犯罪的問題。⁵

論者通常是將電腦犯罪分成四個種類，此即電腦操縱、電腦間諜、電腦破壞以及電腦竊用。所謂電腦操縱是指以輸入指令或資訊等方法，超越電腦本身所設定的機能而予以操作之態。電腦間諜則是意指侵入電腦窺視或複製存取於該電腦中的資訊。至於電腦破壞則是指利用病毒（在當時通常是使用磁碟片傳遞病毒）等方法破壞電腦機能或令其產生機能障礙。最後所謂的電腦竊用，則是意指無權使用他人電腦資源一事。

以當年的時空背景觀之，這種的分類其實可謂僅是憑藉著稀有的案例，再配上想像所創造出來的。其不僅是沒有留意到整體的犯罪流程，而且也根本無法顧慮到當時並不普遍的網路架構。

詳言之，首先以犯罪進行的狀態而言，應該是有人合法或非法地利用他人的電腦，其後進行不正的或合法的操作，其目的可能在於破壞電腦機能，亦有可能是窺視或竊取資訊，當然最後行為人也可以利用這一連串的過程所得進行傳統的犯罪。若當時的論者能夠以這種動態的類型分析，配上實質法益保護的考量⁶，或許即可引導立法政策或活動，明白地基於各類型犯罪對於法益侵害的危險程度上差異，訂出嚴謹的、必須予以規制的行為態樣，並區分其相對應的刑度。更重要的是，若當時的論者能夠這樣做，則必然能夠避免刑法規制過度前置化。可惜的是，這都不是當時的情境。

其次有關網路的問題，其實這是無法苛責當時導入上述分類的論者，因為八〇年代時網路尚未發達。但是奇妙的是，在網路架構逐漸具有雛形的九〇年代，許多的論者仍舊沿襲著這種舊時代的分類，而絲毫看不到任何思索上或分析上的進展。

這種急慢導致我國於一九九七年修正刑法，正式將電腦犯罪的相關條文納入刑法之際，修正條文的內容不僅是漏洞百出，甚至可以說是根本無法配合上時代

的潮流。

我國有關電腦犯罪的新修條文，大體上可以區分成三類，此即電腦記錄的動產化、電腦記錄的準文書化以及電腦詐欺罪的新設等三類。電腦記錄的動產化基本上是對應於上述分類中的電腦間諜類型，而電腦記錄的準文書化，則是對應於電腦破壞類型，至於電腦詐欺罪則是對應於電腦操縱類型。至於電腦竊用類型方面，則是基於此類型的行為與使用竊盜類似，在使用竊盜並未使犯罪化的現行刑法架構中，並不適合貿然將電腦竊用類型的行為犯罪化等等的理由，最後終於沒有出現在新修條文中。

姑不論這些新修條文於整合性、妥適性上的諸多問題，僅就未被納入修正範疇的電腦竊用類型而言，立法者即已犯下見樹不見林的錯誤。其實，在國際上，電腦竊用的情形已經不是問題所在，雖然我國基於其他的理由而表面上符合了國際趨勢，但是事實上卻是喪失了一個立足於國際觀察本國刑法規定的良機。而這個誤失是來自於對於網路發展及其特性的不理解。

八〇年代時不僅是網路尚未成形，而且電腦資源也是非常珍貴。所以八〇年代的電腦犯罪分類才會把電腦竊用視為重要的、應該加以犯罪化的行為類型。不過，等到我國修訂有關電腦犯罪相關條文的九〇年代後半期的時候，事實上，電腦的資源透過網路的發達已經不再是稀有的事物，甚至於已經成為日常生活中到處可見之物。於這種階段若還在暢談電腦資源的稀有性，進而主張嚴罰未得同意任意利用他人電腦資源一事，真的會貽笑大方。

以資訊大國的美國為例，美國有關電腦犯罪或電腦網路犯罪的規制趨勢大略可分為四期。⁷首先為七〇年代後半開始一直到八〇年代前半段的第一期與第二期。第一期法規的規制目的在於稀少資源的分配與保護，雖然有處罰單純無權使用電腦的行為的法律（例如南卡羅萊納州的電腦犯罪法），但是需有其他目的或後續動作的法規仍為多數。至於第二期，刑法規定的目的則開始明確地轉向物理性財產利益的保護。這一期的特色在於處罰以獲得財產上利益為目的的不法侵入行為（亦即將不法侵入電腦系統的行為當成手段而進行的財產犯罪⁸）。這個時代的特色是除政府、銀行外，一般公司或個人也開始使用電腦系統。

第一期與第二期間的差異其實僅是反應出使用電腦處理事務的行業或個人有逐漸增加的現象而已，基本上並沒有考慮太多透過網路入侵的問題。真正有質的轉變發生的是八〇年代後半起至九〇年代前半為止的第三期。第三期的重點在於智慧財產權的保護。僅基於此點，我們已經可以明確查知美國已經逐漸步入資本主義的第四生命週期，除了保護傳統的第三生命週期的有形財產外，開始保護做為第四生命週期重點的無形資訊（特別是商業上機密）。此再加上，世界性的無

國際網路革命已經展開，對於做為重要資本的無形資訊的保護已經不能將眼光局限在自己本國而已，更重要的是應該如何才能夠防止透過網路由國外所進行的侵犯行為。這一種考慮即成為發展到第四期規制的重要轉折點。當時縱或要求他國為國際刑事活動的合作，亦苦於他國沒有這般先進，並沒有設計相關的類似處罰規定，在無雙罰情形存在的情況下，做為犯罪行為地的他國當然沒有義務亦無可能對美國提供國際刑事司法的協助。而美國方面，亦甚難於無告知的情形下，即從美國透過國際刑事司法的協助。而美國方面，亦甚難於無告知的情形下，如果這個特定的他國也擁有同等程度的網路技術時，該侵入行為即有可能會被發覺，並被認為是侵犯主權的行動。

在這種欠缺雙罰規定，亦無其他有效國際司法共助管道的局勢下，美國步入第四期的規制階段。第四期為九〇年代後半到現在為止。於此期，美國開始以間接的方法保護以上的利益。保護的客體不再是系統本身（包含其內具有財產價值的資訊），而是管理系統連線的系統內部特殊的保護措施，於是所欲規制的行為被明確訂為「解除或迂迴限制連線措施的行為」。至於進行這類行為後的當然後續行為，例如違法取得 ID 等密碼後的連線行為等（亦即以前所謂的電腦竊用行為），則被視為不可罰的後行為。不過若連線後另有其他行為（意指該當於以往的其他三種電腦犯罪類型的行為，以及其後的傳統犯罪行為），則為併罰的他罪。這類新法規的例子頗多，例如 1998 年依據 WIPO 條約而訂的電子媒體著作權法第一百零三條，即是佳例之一。其他另有許多規制破壞與迂迴資料庫或色情資訊連線限制行為的新法規都如雨後春筍般地出現。

透過網路得利最多的國家，當然會去想積極地保障既得利益，但是在從全世界各處任何一個末端都可進行對該既得利益的攻擊行為的網路時代，若只是一味強調自己國內既有的有形以及無形財產的保護，則根本無法得到他國的認同，於是做為最大的資訊大國的美國當然會開始主張較為中性的、或較具普遍性的「犯罪類型」，以求其他國家的同意，並允以設定雙罰規定，以此為基礎可進行國際刑事司法上的共助。

當然僅有雙罰規定以及基於這類規定而變為可能的國際刑事司法共助是無法達成保護特定利益的機能的。因為網路上犯罪的特性，不僅在於其無國界性而已，更重要的是無痕跡性、匿名性等特性。於追查犯罪時，首重即時性的、當場的追捕，只要錯過時機，則可能會永遠無法舉發犯罪人。基於這種需要，美國開始利用國際組織，特別是先進國家組織的 G8，針對其所主張的國際性電腦網路犯罪防制政策，展開一連串的非強迫式推銷活動。

例如得立即特定發信源頭的網路設計（獎勵 ISP 使用 SS7，亦即七號共通線路

的信號傳遞方式，或新的 Ip ver 6，可於 128bit 長的 address 中包含了發信源頭、路徑等訊息）、一般通信紀錄的保存⁹、使用者身分認證系統的確立、於國內確實執行外國所為有關證據保全的請求的程序等。其中最為「成就」的應該算是 24 小時待命的 contact point（非 Central Authority，而是特設的機構，可獨立地、暫時性地允許外國的電腦網路警察透過網路偵測國內特定網站，或存取其資料）。現在美國正在透過歐盟、ICPO、IOEC 等國際性組織向 G8 以外的國家推廣這些政策。¹⁰

在美國進行第四期的電腦網路犯罪規制活動的初期，其即已為以上新的電腦網路犯罪防制政策重新設定了犯罪的分類標準，藉此做為向世界推廣其規制政策的基礎。在我國根據老舊的分類而制定並實施新修訂刑法條文的一九九七年，G8 即於當年的十二月間在華盛頓召開司法及內政部長會議，會中在美國的主導下使用了最新的用語——高科技犯罪。這個犯罪被定義成：（一）熟習於高科技技術的犯罪者以電腦以及電氣通信系統為攻擊標的，企圖無權限地竊取或篡改重要資訊，或意圖紊亂重要的商業、公共系統的犯罪；（二）組織犯罪的成員或恐怖份子，利用上述新的技術而進行的傳統犯罪。¹¹ 第一段的定義，其特定的犯罪類型可以導出獨立規制不正連線行為的法規的妥當性，而第二段的定義則除了可以達成第一段定義的任務外，另可誘使其他國家基於危機感而同意諸多的無國界、無障礙的國際圍捕技術。不過，現今國際社會是以較符合現實的國際性兒童色情犯罪的規制，來達成上述的兩個目的。

雖然我國似乎沒有受到這波國際情勢的影響，但是亦仍有業餘的法律研究者開始留意到這種的國際動向，進而主張電腦網路應分成三類，一為以網路為犯罪工具的犯罪，二為以網路為犯罪場所的犯罪，三為以網路及連結在網路上的電腦系統為攻擊目標的犯罪。氏並主張只有後二者才是所謂的電腦網路犯罪。¹² 姑不論此分類中第一類與第二類的區分標準上的曖昧性¹³，僅就得區分電腦網路上傳統犯罪與電腦網路犯罪這兩大類型一事，即可予以適當的評價。不僅如此，若能詳查該分類的細部說明，亦應可發覺該論者已經可以明確掌握電腦網路犯罪於犯罪實行時的動態發展結構。只不過該論者並沒有留意到自己所稱的第三類型犯罪其國際規制趨勢早已是發展到利益抽象化、概念化的階段，而規制方面的具體計劃已經到達確立國際性雙罰原則以及無國界、無障礙的圍捕技術的境界。

肆、光怪陸離的我國執法狀態

如前所述，我國有關電腦犯罪的新修刑法條文是基於八〇年代初期的知識（約略等同於美國的第三期）所制定出來的，但是當時的社會狀況卻已經是步入相當於美國第三期的境界。這是一件非常奇妙的事情，因為起初導入基礎知識時，舉國的態勢並非不積極，之所以會產生這樣的奇妙情景，其問題是出在之後的基礎知識升格必要性方面的忽視以及立法、執法態勢方面的怠慢。

八〇年代時導入的基礎知識，其實並不落後，甚至是一種超越了社會現實的知識。而後政府也沒有怠慢，其立即留意到電腦犯罪會成為未來犯罪防制的重心所在，於是召集了學者與實務家近百人聚集於司法官訓練所進行研討，並於事後將研討會論文以及會議記錄彙集成冊¹⁴，於之後的三年內三度印刷再版。問題是發生在之後的十年，雖然有關電腦犯罪的論文如雨後春筍般地出現，但是大體上而言都是了無新意，甚至可以說是喃喃自語而已。更糟糕的是，相關的政府機關也沒有採取任何有意義的準備動作¹⁵。

然而就在這研究成果以及準備動作幾乎一片空白的十年間，社會已經透過網路建設而快速地發展到相當於美國第三期的境界，而以美國為首的先進國家則已經在美國的領導下正式步入第四期的規制階段。正在此時，一些立法委員透過連署，在沒有經過充分討論，也沒有任何研究者參與的情形下，於一九九七年草率地制定了沒有經過時的修正條文。簡而言之，若以美國的發展為說明的基準，可以說是國際社會如火如荼地邁入第四期，而我國的社會局勢是處於第三期，但法律卻是屬於第二期的產物。

更嚴重的是縱或法律是屬於第二期的產物，因為執法單位的臨陣態勢可能連第一期的程度都沒有，所以這些條文的實際運用狀態，可謂是光怪陸離。雖然相應於新修條文的實施，實務界開始定期召開有關新法施行的研習會，企圖增強法官與檢察官偵辦電腦犯罪的能力，而高檢署也成立了電腦犯罪防制中心，甚至於第一線的警察方面，也有了專門偵辦電腦犯罪的內政部警政署刑事局偵九隊，但是如前所述，電腦犯罪已經發展成電腦網路犯罪，而電腦網路犯罪的偵防工作不是僅僅憑以上的研習會或少數的人力即可負擔，這還牽涉到許多的基礎建設。

姑不論為偵防國際性電腦網路犯罪時所必需的雙罰原則或24小時CP體制，連偵防（特別是追蹤）國內電腦網路犯罪時所不可或缺的網路登錄記錄的保存體

制，都不存在，事實上現在有短期保存登錄記錄的ISP也只有HINET一家而已¹⁶，更遑論SS7的使用或Ip ver. 6的更新等。此再加上浮動（虛擬）IP以及網路咖啡廳的普及等情勢的發展¹⁷，在這樣的情況下，再神勇的警檢可能也無法集發「真正聰明的」電腦網路犯罪者。

以進行網路攻擊能力的程度來區分「專家」時，我們可以將這些人分成五等級，第五等級的專家是真正的新加入者，第四等級是程度較高的業餘份子，第三等級是專業駭客（為違法賺錢或受企業委託而進行侵襲行動的駭客），至於第二等級的專家則通常是隸屬於犯罪組織或恐怖組織，而最高等級的駭客則是先進國家情報機關的成員。根據權威機關的推測，全世界第三等級的駭客有五到十萬人左右，而第二等級則有一萬到一萬人，至於最頂級的駭客則約有一千名左右。¹⁸以我國目前的網路發達狀況以及偵防體制的態勢而言，理論上這些高手應該是非常樂意經由我國的網路而進行國際級的犯罪行為，因為只要經由我國的ISP，則基本上其犯罪的蹤跡將會中斷，任何人都無法繼續追查。如此一來，我國將會成為國際電腦網路犯罪者的天堂。如果這只是理論上的假設，現實並不是如此，則唯一能夠解釋我國的網路並沒有成為犯罪者天堂的說法，即將是所有從事國際性電腦網路犯罪偵防的高手，都可以不要經過官方或私人的允許，而任意地進入任何的系統中，無痕跡地進行犯罪蒐證的工作，所以電腦網路犯罪者，不太想利用我國的網路系統。

真相如何，無法得知，但是有一個事實是於我國根本沒有真正的電腦網路犯罪已被舉發。根據偵九隊隊長李相臣警官的統計，修法後到2000年8月為止的四年之間，警方共檢舉了二十七件的電腦網路犯罪。¹⁹假若這二十七件的電腦網路犯罪是真正的電腦網路犯罪，則這將是令人驚異的成果。不過經仔細查閱這二十七件所謂的電腦網路犯罪的記錄後，發覺其中的大部分都是由網路所犯的傳統犯罪，例如恐嚇、猥褻物散布、不法行為煽惑、違禁藥品販賣、賭博、妨害信用、公然侮辱、傳統詐欺等²⁰，而且都沒有使用所謂的高科技技術，至於散布病毒、網路上的信用卡犯罪以及侵入系統改竄資料²¹等的案件僅有五件而已。從這些犯罪的被害額而言，除世界有名的CIH病毒案外，都不能算是嚴重的犯罪，而且幾乎所有被定罪的案子都是被處以緩刑或短期自由刑。更重要的是，在這二十七個案子中並沒有該當於（美國）第二期犯罪規制策略中處於標準地位的刑法第三百三十九條之三的犯罪。

進一步若我們詳查這些所謂的電腦網路犯罪的判決資料，則會發覺更令人驚異的現象。雖然這些犯罪者其實根本沒有利用到G8所設定義中所謂的高科技，因為他們都留下了明顯的犯罪痕跡，但是法院對於這種「愚蠢」的犯行，其判決卻

是以最高標準來確定罪名（不是指罪責，因為其被科處的刑罰都非常輕），這種傾向會過度地擴張了刑法的規制範圍。舉例言之，例如於自己的網頁中用超連結的方式指示了他處色情網頁的網址，雖然於網頁上沒有任何的色情圖片或撰擬文字，這也被視為該當於散布猥褻物品罪²²，此外對於將美國有關炸彈製作的方法、自行製作炸彈時爆炸受傷的照片等，下載並予以部份翻譯後，登載於自己的網頁上的行為，亦被視為該當於煽惑不法行為罪²³。

這些行為若不是發生在網路上，大概都不會被舉發。再者，縱或警察將這類行為予以舉發，則檢院雙方亦應考量罪刑法定主義中的實質要求，而決定是否應該予以起訴或判刑。罪刑法定主義並不只是要求司法人員考量溯及既往禁止、類推禁止等形式上要求，其更要求實質正當程序的考量，亦即罪刑法定主義要求司法人員留意到司法程序啟動行為本身的正當性，例如程序是針對如何的事件開始進行的，以及做為開始程序前提的事件，其要件是否明確、合理等。這些罪刑法定主義的實質層面會要求法律的意義必須要明確，而且縱或得用限縮解釋（或限定的合憲性解釋）的方法將具體個案中的處罰基準予以明確化，若這種解釋仍舊是超乎一般人的理解範圍，即應該認為這類的刑罰法規並不合乎明確性要求。此外，雖然文義的概念明確，只要處罰的範圍過於廣泛，有時亦會包含了本來即沒有處罰價值的行為，此際亦應認為該刑罰法規不合乎合理性的要求。²⁴

具體而言，上述的兩種行為到底會不會有紊亂刑法所欲保障的公共秩序的客觀可能性、概然性等，都是應該予以具體考量之事²⁵，而不是可以盲目地因為這些行為是發生在網路上，所以就認定其一定會對社會公共秩序產生損害。²⁶可惜的是，在這兩個判決中，根本看不出來做為專業法律人員的警檢院，曾經做過類似的考量。在無國界的網路中，國內外處處充斥著相似的訊息隨時可以擷取，於這種情勢下，為何只有這兩位思慮不深、莽撞、技術低劣，但是對於多元化網路環境充滿了憧憬的年輕人，會被視為是電腦網路犯罪而被起訴判刑？執法人員似乎應該更深入地去理解網路社會與公共秩序間的關係。

不僅是執法人員於認知上有令人質疑之處，連部份的年輕學者，其相關的論述都會令人難以置信。

前述的略提及先進國家有利用對於較中性的、具有普遍性的犯罪的非難，來激起共憤，藉此而確立起國際級圍剿電腦網路犯罪體制的傾向。這類犯罪的典型即是國際性兒童色情活動。所謂的兒童是指十八歲以下的未成年人，如果成人為滿足自己的慾望而實際上侵害到這些未成年人的身心發展，對於這種行為或許應該利用刑罰予以制止。但是因為先進國家另有別的目的，所以現今的主流傾向是連沒有具體被害人的電腦合成照片亦被視為照片本身即為邪惡之物，不僅是要

取締製作的行為，甚至於只要單純持有邪惡孩子以收縮、處罰，²⁷國內有論者未能掌握住電腦網路犯罪的規制的發展歷程，也沒有留意到這種擴張處罰範圍的動作其背後真正意義所在，就在沒有確切理解的情形下，即立刻主張我國亦應跟進，甚至於曲解我國刑法規定，認為單純持有猥褻物品亦可利用現行法予以處罰。²⁸

總而言之，我國目前的規制情況是第二期的法律、第一期的執法能力，但卻有類似於第四期的判決與學說。而在沒有參與國際組織活動，且NGO也不甚發達的情況下，我國明顯地並不是在追從美國的脚步，參與其電腦網路犯罪的規制計劃。則這種將法益抽象化、概念化，或甚至於擴張處罰範圍的傾向，其形成的理由就有許多種可能的解釋。其一，我們可以將這種傾向視為近十年來風行全臺的刑法主觀主義的產物。其二，這種傾向的形成是因為執法單位無法適切執行新法，在心急之下只好在其能力範圍內急就章地揭發「愚蠢」的犯罪人，以彰顯執法效率，並維護住單位的活存。其三，於網路發達的時代，舊有秩序開始不穩，為求鄉愁式的安堵感，執法單位透過選擇性執法強調舊有社會道德秩序的必要性。

就筆者而言，這三種說法均有道理存在，事實上或許是以主觀主義為基本教義的刑法系統受到做為其環境的其他系統，例如政治以及社會系統的刺激，於是自我再製了變調的元素，繼續維持其自身的運轉。不論如何，這種既閉鎖又開放的刑法系統，其運轉已經產生了不良的後果，這就是在刑法謙抑原則喪失作用的時刻，人民不僅無法正確預測自己於網路上行為的合法性，進而喪失對於法系統的信賴，其更喪失了透過多元的網路發展新世紀人類應有的多元人格的可能性。這種情形若再繼續進行下去，於主客兩種概念系統既分離又互相影響的後現代中，我國即有可能會失去挑戰國際時的僅有的資本，此即精良的人力資源以及其所散發出來的創意。

於此並不是要主張放棄電腦網路犯罪的偵防工作，更不是主張我們應該犧牲國民的隱私或甚至於國權的威嚴，而臣服於先進國家的壓力下，替這些國家的法益保護而努力。放眼國際，我們可以查知我國有可能成為國際性電腦網路犯罪的天堂，而國內真正會利用高科技進行犯罪的電腦網路犯罪者或許已經悄悄地展開活動。當務之急應該是不要再浪費精力在較無實益或甚至有有害的犯罪偵防活動上，人力要精，更要用在刀口。再者，比諸消極防堵，更重要的應是網路要塞化的活動以及使用者的自覺與警覺。

伍、結 論

做為最低道德標準的刑法，其最近的動向有值得我們注目之處。因為刑法所規制的行為中，雖然有所謂「法定犯」的犯罪行為犯罪，但是對於這類行為的規制，仍舊是不能過度偏離現在的社會共同感情。問題是何謂社會的共同感情。

所謂的社會共同感情恐怕不是透過理性的對話而形成的，與此相反，社會共同感情毋寧是由社會中的上階層留意到求生存的人類慾望，利用排除與差異的機制，透過補設最為凌厲的法規制體制而創設出來的。²⁹ 誠如奈爾幹所云，隨著社會的分工，連帶日益薄弱，對社會上的支配階層而言，這種現象不外是混亂無法忍受的情勢，於是會日漸不願替社會付出自己的力量；為防止這種事態的發生，統治者通常會利用儀式性的刑罰，舉發社會上的惡（其實有時僅是不太適宜的行為而已）並予以處罰，藉此增強社會的連帶。³⁰

縱或許多人都無法認同上述的言說，但無可否認的，只要有人類社會存在，只要人類的生存慾望不會消失，則刑法或多或少都會帶有一些這種的色彩，這是一種存在於人類歷史上的嚴酷事實。

所以說刑法是最低道德標準。亦即，刑法一方面雖然無法擺脫其做為生存慾望滿足手段的工具性質，但另一方面，其亦必須自我抑制，不要片面地滿足單方面的慾望，而抹殺另一造的慾望，這就是最低的道德標準。更詳細而言，人際關係是一種權力關係，而權力並不是得具體掌握的物理性物質，其是一種在支配與自由間流動的非對稱遊戲規則，在這種形成不穩定權力關係狀態的人際關係中，某造會為了片面地滿足自我的生存慾望而積極地利用所有的力量，包括設定以及執行刑罰法規的力量，企圖「支配」另一造，但是只要這個另一造已被完全支配，則非對稱的人際關係即會消失，社會的進化亦會立即中止，所以做為規範人際關係的系統之一的刑法，應該自我謙抑，肯認系統中存在有僅發揮標示最低社會道德水準的核心綱要，維持住做為權力關係的人際關係中被壓抑的一造反抗對造支配的可能性，而這種反抗的可能性不外就是所謂的「自由」。³¹

刑法就是在這種情形下，一方面承認自己這個系統是基於人類生存的慾望而運作，但另一方面又為了維持住做為權力關係的人際關係，而必須抑制人類的生存慾望。這是刑法的宿命性最根本的吊詭，也是刑法系統綱要中最高核心部份的指導原則，更是刑法教義學的基本。不過，從工業時代發展而來的刑法教義學上

的主觀主義思潮，雖然一方面仍舊主張刑法的謙抑性，但是卻在主客合一的大森下，設計了一連串曖昧的判斷標準，架空了上述的指導原則。於有能力進行支配的社會階層，強而有力地利用刑法的規制企圖披著傳統的外衣，而實際上卻是創造新的社會通念或新的社會連帶時，被主觀主義所支配的司法，除了服從、支援新的控制體制或紀律創造機制以外，可能什麼都無法做。

當然我們是無法要求刑法去達成積極創造權力關係中抵抗可能性的任務的，刑法的機能本來就非常消極。於後工業的時代，或資訊的時代，可以提供權力關係中抵抗可能性的機制的，不外是讓每個人都可能擁有自我形象、自我創造能力的網路社會。現今刑法的機能只在於儘可能不去干涉這個多元的網路社會的發展，允許其能夠自律地創造出新的道德秩序，並允許每個人的自律性倫理反省。而只有主張客觀主義的刑法教義學，才能夠達成這項任務。

本文透過國內外對於網路社會的刑法規制體制以及我國執法狀態的分析，暴露出我國當前的規制體制是如何不當地限制了人們活動的可能性。我國目前正處於激烈變動的時代。人們由政治性鎮壓的宰制社會中獲得解放，漫無目的的在幾近混沌的複雜社會環境中漂蕩。我們應何去何從？應不應該再一次地尋求權威的指引？

以往人們習慣於服從被安排不好的人生旅程，或依據社會工學所設計好的程式而過活，所以當這種傳統支配者的計劃崩壞後，當然會開始面對一連串的不確定，並且感到人生上的真正痛苦，就像是習慣於營養的飼料雜被釋放回原野中一樣，國民開始感到無所適從。但是縱或是無所適從，只要我們能夠直視自己的生存慾望，則自然可以拒絕佛若姆的夢魘，而且只要能夠克服面對不確定性時所會產生出來的痛苦，則每一次的克服都將會產生更高層次的生存慾望企待滿足，由物質性生存的滿足到人際關係的協調，到最後或許會得到肯認自我生存價值的慾望滿足，而諸種層次的生存慾望滿足都是獲取真正的自律以及主體時所不可或缺的。³²

新興的網路社會提供了無限複雜的不確定性，也令我們嘗受到無與倫比的痛苦，以現代的刑法或其他法規範進行極度管制或嘗試建設新秩序的努力，雖然可以緩和痛苦，但終究不是痛苦的克服。何去何從？答案在於反抗可能性的保存與實踐，而無論是低層次的我國刑法規制實踐，還是高層次的美國等先進國家的全球化規制企圖，都無法為人類帶來做為一個生存個體時的幸福的。

後記

一九九八年時，本人曾發表一篇長達九萬字的文章，兩千年時，又獲得機會能夠在第四期檢察官資訊法律研習會中發表相同的意見。但是兩次的經驗都非常慘痛。不僅文章未獲好評，連口頭上的報告，根據聽講意見調查，幾乎都是一句「不知所云」。或許有人會批評說這是自找的，寫出來的東西、說出來的話若沒有人懂，則東西是白寫，話也是白說，而且當「不知所云」的形象形成後是無法再回頭的。

回想起來，確實這些經驗都導因於自己的表述方式。每當說明一個概念，我都嫌煩而跳過好幾個步驟，結果變成每一個論述都有著許多未能明確表述的背景知識。此次雖然想用簡單的論述表達以前不能傳遞的訊息，但是好像還是失敗了。我不能責怪嚴格的字數限制，因為我已經違背了這個限制，而且縱或沒有限制，我也無法說明清楚。本文的背景知識潛藏於本人於一九九九年以及兩千年時所著合計長達十五萬字的兩篇論文中。這兩篇論文分別討論混沌與複雜這兩個現象，而這兩篇文章的背景知識，則是尚未公諸於世。

如此說來，我是一開始就錯了，而且以後也是將錯就錯。這般就這樣錯下去的態度，說起來是非常的自私，不負責任。縱或如此，我還是留下了一些痕跡，讓想懂我的人可以去懂我。我並沒有想在學術界或實務界斷絕所有的人際關係，但是我更想在這種的人際關係中成為永遠不會變成權威的異端。異端的每一次論述都代表了再一次的挫折與漠視，這都會帶來痛苦，不過或許我就是尋求這種痛苦，以便可以自我提升。自我創造痛苦，並且自我克服，這豈不是我的生存之道？所形塑出來的只是一種不斷進行反抗的可能性，一種反抗集團權威也反抗自我權威的異端性存在。

註釋

1 亦有科技方面的專家以務實的观点區分電腦犯罪與網路犯罪。其認為利用網路犯詐欺、名譽毀損、毀棄物散布、著作權侵犯等傳統犯罪者為網路犯罪，而竊

取電腦中所保存的資訊或妨礙電腦處理機能的犯罪，則為電腦犯罪（岸田明「七キユリテイ技術の現状」法律ひろば2000年6月23頁）。這種分類簡單明瞭，而且以實務的觀點而言，針對前者應留意新的偵查技術，至於後者則需要考慮新的立法，僅就此而言是有其優點存在。不過，強將有交集的兩類犯罪硬生生地切割開來一事，可能會導致觀念上的混亂，例如電腦犯罪則不會利用到任何網路上技術等的誤解，勢必難免。

2 宮脇嘉介「サイバーセキユリテイについて」法律ひろば53卷6号36-37頁（2000年）。

3 有關資本主義四個生命週期的詳細論述，請參照李茂生「權力、主體與刑事法」268頁以下（漢蘆，1998年）。

4 詳請參照，前揭註255-258, 278-280頁。

5 詳請參照，前揭註178-179頁。

6 亦即於考量刑法的法益保護機能時，能夠重視實質法益的保護，而不將法益概念抽象化，以免法益概念喪失了對於擴張處罰傾向的批判性、規制性機能。有關刑法的這種法益保護機能，詳請參照堀內捷三「刑法總論」7-8頁（有斐閣，2000年）。

7 有關美國這四個時期的發展，詳請參照夏井高人「アメリカ合衆国におけるコンピュータ犯罪立法動向—無権限アクセスを中心とする比較的検討と日本法への示唆—」判例タイムズNo.1008, 100-102頁（1999年）。

8 我國新修刑法條文中最具有特色的刑法第三百二十九條之三，即為這個時期的產物。

9 當然這會增加業者的負擔，也可能會侵害隱私，所以甚難獲得共識。例如1998年10月生效的歐盟指令（EU Directive）中即規定通信業者必須在通信結束後立即將通信紀錄抹消。

10 那須修「第五回警察政策フォーラム『高度情報通信社とハイテク犯罪』におけるパネルディスカッションの概要について」警察学論集51卷10号19頁以下（1998年）。菊池浩「ハイテク犯罪対策に関する國際的取組」法律ひろば53卷6号29頁以下（2000年）。

11 川原淳平「ハイテク犯罪対策に関する國際的動向について」警察学論集52卷9号42-43頁（1999年）。此外，於這次的會議中，正式以G8的名稱取代舊有的P8稱號。

12 蔡美智「電腦駭客的罪與罰—談網路入侵的法律問題」資訊法務透析1998年7月17頁以下。

- 13 例如，氏將網路上傳替、宣傳色情資訊，但實際上的性行為並不是在網路上進行的犯罪視為是第一類犯罪，而在網路上侮辱他人的犯罪則為第二類犯罪。但是其實這兩種犯罪均是於網路上進行的傳統犯罪行為，殊不因前者另有現實世界中的性行為，而使得二者有質的區分。
- 14 「電腦犯罪問題研討會實錄」（法務通訊雜誌社，1985年）。
- 15 雖然行政院有於刑法修正草案中納入相關條文，並於一九九〇年將草案送交立法院審議，而立法院也有委託學者研究刑法修正草案，但是基本上行政院草案中的相關條文仍舊是立基於八〇年代的基礎知識上所制定的，而學者也只能就這些條文為適當的建議，基本上並沒有將較新的國際情勢納入考量內。
- 16 馮震宇「網路使用犯罪問題及預防措施之研究」69頁（行政院研究發展考核委員會，2000年）。
- 17 想像一下，假若有人利用網路咖啡廳的電腦，使用浮動IP，連線進入網路，並侵入他人的電腦系統中進行破壞的情景，縱或得追查至該部電腦端末，此際還得必須進一步確認於犯罪當時是誰在使用這部電腦，不然是無法舉發犯罪的。而這個問題絕對不是僅透過24小時錄影使用者或進行嚴格的使用者登記制度等方法即可獲得解決，真正的解決方法必須是得即時追蹤的體制建設，不巧的是這正是我國電腦網路犯罪偵防體制上最大的弱點。
- 18 前掲註2，宮脇嘉介「サイバーセキユリテイについて」法律ハクバ53卷6号41頁。
- 19 李相臣「電腦網路犯罪實務」第四期檢察官資訊法律研修會講義要綱（資策會科技法律中心，2000年）。
- 20 其實，李警官根本沒有留意到網路上接交的犯罪行為。按照其標準，這些無計其數的網路上表現自我雄性與雌性魅力的行為，都是電腦網路犯罪。而這些電腦網路犯罪都是針對兒童及少年性交易防制條例第二十九條所為最高法院八十七年度第二次刑事庭會議決議所造成的。這個會議決議的內容可謂是我國刑法解釋學上主觀主義的極致。
- 21 此即於1998年5月送檢的有名的黃姓軍醫案。這是典型的網路入侵案件，其犯罪事實如下。某黃姓的醫學院畢業生於徵召入伍後，利用駭客手法侵入各個有名的ISP，破壞其系統程式，並複製顧客資料。雖然實害不大，但引起了許多網路族的不安。
- 22 新竹地方法院刑事判決，八十八年（1999年）易字第一二六號判決。此外，請參照李茂生「網頁中設定色情網站超連結行為的刑事責任」光碟月刊46號（1998年）。

- 23 李茂生「執法人員的網路安全恐懼症—無政府文件集的省思」光碟月刊50號（1998年）。
- 24 前掲註6，堀內捷三「刑法總論」17-18，23-27頁。
- 25 事實上，這種考量已經牽涉到某不法行為類型，亦即構成要件該當的行為類型是否具有違法性的判斷。假若認為罪刑法定主義僅有形式上的意義（亦即認為這是一種純粹未取形式合法性與法定性的理念。詳請參照川端博「刑法總論講義」42-45頁，成文堂，1995年），基本上是形式上判斷構成要件是否該當時的指導原理，而違法論的指導原理是進行實質考量的法益保護主義，責任論方面則是同樣進行實質考量的責任主義（山口厚「刑法總論」2-7頁，有斐閣，2001年。不過奇妙的是當山口氏為這種的主張後，又於說明罪刑法定主義的內容的部份開始討論刑罰法規的實質明確性與合理性，此點是與川端氏截然不同），那所謂的罪刑法定主義的實質面考量，其實就不外是所謂的違法性判斷上的法益保護考量。
- 26 試比較以下以下兩個相對應的例子。其一，某位教師於課堂上教授爆裂物品的製作方法，但另一位則於網頁上公布其教學或研究成果。其二，某標榜暴露社會黑暗面的電視節目公然告知大眾某商場有販賣色情光碟，而另一位則是於自己的網頁上註明色情項目並以超連結的方式將該商場的網頁予以表明。假若兩案並陳，此際真不知我國的執法人員會如何反應。
- 27 當然以隱私權或肖像權的觀點而言，頭部相片被借用的兒童，其法益是有受到侵害，但是若以法益的重要程度而言，則這類的犯罪似乎還沒有到達要大張旗鼓進行圍剿，而且連單純持有之人亦以助長侵害隱私為由而科以刑罰的程度。
- 28 高玉泉「論國際網路上兒童色情資訊之法律管制—兼評我國兒童及少年性交易防制條例之相關規定」政治大學法學評論60期195-197頁（1998年）。於此並不是要去非難此論者對刑法的錯誤認知，發言是不是有誤謬一事，僅是他人對於該發言的評價而已，於此重點應該是置於導引出這個對論者而言是最為真摯的發言的社會背景。
- 29 今村仁司「近代性の構造—『企て』から『試み』へ」208-225頁（講談社，1994年）。
- 30 ジェームズ・M・インヴァラリテイ著／松村良之、宮澤節生、川本哲郎、土井隆義共訳「刑事法の法社会学—ワルクス、ヴェーバー、デュルケム—」137-145頁（東信堂，1994年）。
- 31 有關權力關係中支配與自由間的關係，詳請參閱良德「フーコーの權力論上

強盜、搶奪犯罪問題與防治對策

國立中正大學犯罪防治研究所教授康所長 楊上博

摘要

近年來，強盜、搶奪犯罪問題屢次引起民眾之嚴重關切，根據台灣刑案統計（民國89）之資料，由民國七十八年之4,106件，增加至八十九年之7,250件，呈現巨幅成長。其中強盜案件八十八年每隔3小時36分發生一件，搶奪案件則每隔2小時39分發生一件，其危害性不容忽視。由於強盜、搶奪犯罪之持續發生已造成受害者極端恐懼，並深深影響及民眾生活之各層面，因此亟待深入瞭解其犯罪行為本質與特性，俾謀求妥適對策因應。

本研究彙集國內外近年來相關之研究成果，並結合筆者實地針對強盜集團所從事之實證研究後發現：有關強盜、搶奪犯罪之成因包含：(一)經濟因素；(二)同儕壓力；(三)貧富差距擴大；(四)大眾傳播媒體之渲染；(五)犯罪與街角負文化之影響；(六)低度自我控制、追求立即享樂；(七)倖倖心理。在防治對策方面則應著重於(一)強化檢察之偵查與預防犯罪能力；(二)致力於機構之防搶作為；(三)加強被害預防與個人自我保護措施。

本研究結合筆者對台灣地區犯罪集團進行本土化之實證研究，除對國外研究進行檢視驗證外，並深入的瞭解國內強盜、搶奪犯罪行為之形成與犯罪歷程。最後，則提出防治強盜、搶奪對策供政府與民眾參考。