中國內地與澳門網絡犯罪的刑法比較及完善建議

楊秀莉*

一、網絡犯罪的概念與特徵

(一) 網絡犯罪的定義

網絡犯罪伴隨着計算機的應用和網絡的普及而出現，探討網絡犯罪問題首先需要明確其定義。中國刑法學上對網絡犯罪的研究是從計算機相關犯罪研究的基礎上過渡而來，雖然刑法對計算機網絡犯罪方面的規定不斷力求完善與改進，但是未曾對網絡犯罪從法律上給予明確的解釋。而國外的網絡犯罪之立法理論日漸成熟並已經形成了比較完備的法律制度，因而對於網絡犯罪的定義可通過借鑒國外的立法解釋來予以明確。在國外網絡犯罪的大量立法中，我們可引用於2004年7月1日生效的歐洲理事會《關於網絡犯罪的公約》其序言中的表述：“危害計算機系統網絡和數據的保密性、完整性和可用性以及濫用這些系統、網絡和數據的行爲”。主要指那些通過國際互聯網和其他計算機網絡實施的犯罪，特別是利用互聯網實施的侵犯著作權犯罪、計算機相關的詐騙犯罪、兒童色情犯罪和侵犯信息網絡安全的犯罪行爲。上述定義從兩個方面來對網絡犯罪予以概述，其屬於廣義上的網絡犯罪，一類是實施危害計算機網絡系統、數據和信息的行爲；另一類是利用互聯網實施的其他犯罪行爲。因此，本文將從廣義的網絡犯罪之角度去分析相關的立法與司法問題。

該規定主要體現了網絡犯罪的形式多樣性，不僅是對計算機網絡本身的破壞還包括運用計算機網絡實施的其他犯罪；同時還有網絡犯罪的技能性以及關聯性，計算機網絡系統的相互關聯性必然導致網絡犯罪會“牽一髮而動全身”從而使整個網絡系統受到破壞。

(二) 網絡犯罪的現狀與特徵

根據InternetWordStats.com的統計，過去十年，互聯網使用呈現爆炸式增長。用戶數量從2000年的3.61億升至2010年的近20億，增長超過5倍。同時電子商務發展爲網絡犯罪分子帶來了更大的謀財商機，其已成爲網絡犯罪的主要攻擊目標，互聯網已經漸變爲網絡犯罪分子誘惑難擋的金錢、信息寶庫，網絡犯罪的形式也呈多樣性發展，主要表現有以下幾方面：

首先，電腦病毒入侵危險網絡安全。2000年的“I Love You”蠕蟲病毒的入侵，損失高達150億美元；而以“網絡犯罪損失榜”榜首之名的My Doom蠕蟲病毒感染，直接影響網絡使用和在線銷售，導致高達380億美元的損失。[1] 電腦病毒的傳播使大範圍的網絡使用者的網絡信息安全遭到破壞，政府部門的重要信息也面臨着威脅，病毒成爲了計算機網絡的“瘟疫”並對人們時刻造成威脅和引起恐慌。其次，利用網絡進行詐騙和盜竊。隨着電子商務的迅猛發展，其潛在財富的誘惑導致了運用網絡進行的財產犯罪成爲了最普遍的犯罪形式，例如僅在網絡詐騙就可以有以下幾種：信用卡詐騙，通過發送虛假商品信息的郵件，騙取用戶登入相關網站套取個人信用卡信息予以詐騙；設置釣魚軟件，則是提供虛假的網站信息來騙取用戶登錄虛假的網上銀行的網頁套取用戶的信息資料進而提取用戶的重要信息或財物；虛假中獎消息，利用人們的貪利心理來騙取高額的手續費用；以及假冒殺毒軟件來騙取購買殺毒軟件和升級的費用；網上購物詐騙等。而網絡盜竊則集中表現爲網絡虛擬財產的盜竊行爲。最後，網絡犯罪還表現爲利用網絡進行的淫穢物品傳播、網絡洗錢、網絡間諜以及在網絡上進行有組織的犯罪活動等方式。

面對着世界快速發展的網絡犯罪形勢，中國當前的網絡犯罪狀況也不容樂觀，其主要表現爲以下幾個

* 澳門大學法學院碩士研究生

方面：一是利用計算機犯罪的案件呈多發趨勢，涉案金額高，種類多、領域廣，給國家、社會和人民的財產權和其他合法權益帶來巨大的損失。這其中賭博、竊取密碼、網絡色情、網絡入侵、傳播病毒、網絡詐騙、非法盜版、信息炸彈等犯罪事件更是屢屢出現。二是犯罪方法和類型呈現多樣化趨勢。活動天窗、社交方法、數據欺騙、蠕蟲、冒名頂替、意大利香腸術、木馬技術、邏輯炸彈、乘機而入、利用掃描器、廢品利用等。這些形式和類型的計算機犯罪技術含量越來越高，案件的偵破難度日益增大。三是部分案件呈現集中爆發和高發的趨勢。如侵犯計算機安全(包括非法入侵和破壞計算機信息系統，製作或傳播計算機病毒，閱讀、截獲或複製篡改傳遞中的計算機信息)，尤其值得注意的是危害計算機網絡安全的案件增幅較大，利用網絡複製、傳播各種垃圾信息侵犯國家和公民合法權益的案件愈演愈烈，利用網絡傳播色情信息的案件爆炸式增長，利用網絡進行詐騙、盜竊的案件特別突出。四是計算機犯罪的國際化趨勢日益凸顯。網絡環境的時間性和空間性特徵導致通過國際互聯網實施計算機犯罪行爲的人數猛增，跨國計算機犯罪正在成爲影響全人類發展和國際社會安全的國際犯罪。[2]

網絡犯罪的出現及嚴重的犯罪後果不僅影響了全社會的安全及穩定，而且給傳統的刑法立法及理論帶來全新的挑戰，成爲世界各國共同關注的全球性犯罪。第一、網絡犯罪對中國傳統刑法關於犯罪的規定和理論提出了新的挑戰，主要表現爲通過虛擬空間實施犯罪突破了傳統犯罪的時間、空間之限制；實施犯罪主體和危害客體的不確定性使其具有廣泛的危險性；網絡犯罪的既遂與未遂犯罪形態的沒有客觀的量化標準等。第二、犯罪的技能性、隱匿性。網絡犯罪是運用網絡數據、信息和程序的專門技術實施犯罪，尤其是在以病毒、黑客等方式實施的犯罪完成後，亦要等到發生實質的危害結果才對犯罪進行調查分析，這給網絡犯罪的預防和打擊帶來了很大的困難。第三、網絡犯罪的多樣性。網絡犯罪是由計算機犯罪發展而來，運用了網絡這一特殊的技術空間，該類犯罪不僅僅局限於對計算機系統的破壞，而是更多地利用網絡侵害公民的人身、財產權益，如網絡誹謗、網絡詐騙、網絡色情等。第四、網絡犯罪的跨區域性。由於網絡具有互聯、便捷、高效等特點，利用網絡實施跨國性、跨區域的有組織犯罪的趨勢越發明顯，這也對中國網絡犯罪的跨國、跨區域的合作提出了新的要求。另外中國近年來網民數量的急劇增長，不同形式和特點的網絡犯罪已嚴重擾亂正常的社會、經濟秩序侵害公民的合法權益。因此，加強對中國的網絡犯罪的立法研究，可從中國內地和澳門之間進行區際間的法律制度比較進而予以借鑒、吸收，完善自身立法。

二、內地與澳門網絡犯罪立法概況及比較

(一) 內地刑法的立法概況

縱觀內地對計算機網絡犯罪的刑事立法狀況，從計算機犯罪的立法過渡到網絡犯罪的立法大致經歷了三個階段。第一、計算機犯罪立法開啓階段。內地對網絡犯罪的立法探究開始於計算機犯罪立法，1983年由國務院批准公安部計算機和監察司負責全國計算機安全工作。明確規定了該司的職責之一是負責起草計算機安全規章、法規、法律及研究如何偵破計算機違法犯罪案件，並於1988年正式完成的《中華人民共和國計算機信息系統安全保護條例》(草案)的起草工作，其在1994年正式實施，進而在立法上開始了對計算機的信息安全和計算機犯罪進行保護。該條例實施時互聯網在中國計算機應用還未普及，該條例主要是圍繞對計算機系統和數據的安全進行保護，並沒有涉及網絡安全與保護問題。第二、網絡犯罪的立法階段。隨着互聯網在中國得以廣泛的普及，網絡信息安全和公民網絡權益侵害等問題隨着利用網絡實施的犯罪也接踵而來，引起立法者和民眾的關注。總結、吸收刑法專家學者的意見後，於1997年刑法修改中增加了第285、286條分別規定了非法侵入計算機信息系統罪、破壞計算機信息系統罪兩項罪名以及第287條規定利用計算機實施的金融詐騙、盜竊、貪污、挪用公款、竊取國家秘密或其他犯罪的依照刑法有關規定定罪處罰。將計算機網絡犯罪寫入刑法是立法上的一大進步，但是由於在罪名中只注重對國家及高端技術領域的保護而忽略了對遭受網絡犯罪廣泛侵害的商業和個人信息的保護，僅將計算機犯罪保護的對象限於的系統和數據的完整性，再者沒有對利用網絡實行的傳統犯罪進行重點規範，如網絡盜竊、網絡詐騙依照盜竊、與詐騙罪予以處罰，從而導致了這幾項罪的設置不能真正體現出有力打擊網絡犯罪的目的和作用。發展至2000年，全國人大常委會通過了《關於維護互聯網安全的決定》列舉了利用互聯網實施的21種犯罪行爲，主要是對刑法第287條規定的犯罪行爲予以明細的列舉，但沒有規定具體的罪名設置和責任承擔。第三、網絡犯罪立法的修整、完善階段。[3] 2009年《刑法修正案(七)》對網絡犯罪增設了三個新罪名，分別是非

法獲取計算機數據罪、非法控制計算機信息系統罪[4]和爲非法侵入、控制計算機信息系統非法提供程序、工具罪。[5] 非法獲取計算機數據罪將刑法第285條對國家事務、國防建設、尖端科學技術領域之外的計算機信息系統納入實體刑法的保護範圍，擴大了刑法對網絡犯罪打擊的範圍。

(二) 澳門刑事立法概況

澳門特別行政區對網絡犯罪的刑法規定，反映了澳門計算機網絡信息技術的應用與發展的特點。最開始對網絡犯罪進行規範的是《澳門刑法典》第213條的“資訊詐騙罪”以及第187條“以資訊方式做出的侵入(私人生活)”兩項罪名。資訊詐騙罪處罰行爲人以任何方式介入資訊處理之程序或結果，而侵害他人的財產法益的行爲，同時打擊行爲人透過網路侵入銀行電腦系統，並篡改其中程式或資料以增加資金賬戶數額的行爲。該項罪名突出了網絡犯罪與傳統犯罪的不同特點和形式以及立法者對該類犯罪的重視。另一項“以資訊方式做出的侵入罪”突出了對私人生活的保護，因爲資訊的介入方式具有隱匿性和及時性的特點，極大地侵害私人生活秩序，所以有必要予以保護。但是澳門的刑法對電腦網絡的罪名之設置和刑罰處罰的範圍很有限，網絡犯罪隨着社會向前發展而不斷地變遷，呈現多種方式和形態。因此，澳門立法機構在分析澳門網絡發展特徵以及澳門社會特點的基礎上，於2009年制定了《打擊電腦犯罪法》以此來改善澳門刑事立法中關於網絡犯罪的單一性的立法狀況。該項法律首先通過刑法相關規定對不當進入計算機系統；不當獲取、使用或提供計算機數據；不當截取計算機數據；損害計算機數據；干擾計算機系統；用作實施犯罪的計算機裝置或計算機數據；計算機僞造；計算機詐騙八項電腦犯罪行爲的犯罪構成和刑罰，對於特殊主體實施的電腦犯罪進行了加重規定，並對法人實施的電腦犯罪的形式責任予以明確的規定，並且將《刑法典》的規定與該法律補充適用，最大程度的實現刑法對電腦犯罪的打擊。另外鑒於電腦犯罪的新型化的特點，該法律中對完善電腦犯罪的刑事訴訟程序上規定進行了關於電腦犯罪的證據的收集進行了相關的補充規定，主要包括對電腦資料的扣押程序和進行電腦犯罪刑事偵查的特殊措施，從刑事訴訟中保障了刑法中對網絡犯罪的罪名的規定得以真正的實行。

(三) 兩地網絡犯罪刑法制度的比較

探討網絡犯罪的概念、特徵以及對內地和澳門的網絡法刑事立法的簡要概括，主要爲了能夠從刑法的立法以及具體的罪名規定中比較兩地關於網絡犯罪的聯繫與區別，進而總結兩地立法各自立法的特點。

1. 立法形式之比較

兩地對網絡犯罪的打擊立法形式最開始都規定於刑法典當中，罪名的設置僅爲網絡犯罪最初表現形式的計算機犯罪類型。如內地僅限於計算機系統和數據安全本身的犯罪，沒有涉及到網絡犯罪的問題，而澳門則是對資訊詐騙罪等爲數不多的罪名進行規範。隨着網絡信息的共享、電子商務的發展，網絡犯罪呈現多樣化的特點，在傳統的計算機犯罪以及資訊詐騙罪基礎上出現入侵網絡系統，網絡詐騙、盜取網絡個人信息資料等犯罪形式。對此，內地於2009年通過《刑法修正案(七)》增設了新型的網絡犯罪罪名，通過在《刑法》中罪名的統一規定來進行規制。澳門則是在2009年通過制定專門的《打擊電腦犯罪法》來防範網絡犯罪。兩地在完善打擊網絡犯罪立法形式主要不同表現爲：內地的刑法修正案通過新增罪名的方式來完善立法，但新設的僅有三個罪名，加上刑法典僅有中的兩項條文的規定，整個刑法對網絡犯罪的立法遠不能滿足中國打擊網絡犯罪的司法實踐的需求，呈現出法律規定的明顯滯後的狀態。而澳門在不斷的探索和立法實踐中，制定了專門的打擊網絡犯罪的法律。從立法層面上將澳門的司法實踐中所需要打擊的網絡犯罪的具體的犯罪類型予以規定，使其有法可依。

2. 具體犯罪之比較

(1) 非法侵入計算機系統罪之比較

內地《刑法》第285條第一款規定的非法侵入計算機信息系統罪與澳門《打擊電腦犯罪法》第4條不當進入計算機系統，其共同點在於都是未經授權故意侵入計算機系統的行爲。其不同爲前者的規定爲防範侵入國家事務、國防建設、尖端科學技術領域，後者的不當進入電腦系統不限於特殊領域，而是只要非法侵入任何電腦系統就構成不當進入電腦系統罪，且該條中第1款規定的犯罪若存有任何不正當意圖，而未經許可進入電腦系統的情況，就屬於非經告訴不得進行刑事程序。

(2) 非法獲取計算機信息罪之比較

內地《刑法》第285條第2款規定的非法獲取計算機信息系統數據、非法控制計算機信息系統罪與澳門《打擊電腦犯罪法》第5條不當獲取使用或提供計算機數據、第6條不當截取計算機數據的規定相似，共同規定了未經授權故意侵犯計算機系統非法獲取電腦數據的行爲。但具體規定所涵蓋的範圍卻有所不同，前者

規定違反國家規定而侵入獲取計算機系統數據，或者是對計算機實施非法控制行爲且情節嚴重，予以刑事處罰；而後者第5條第1款規定未經許可獲取使用電腦數據資料或者即使是正當進入該計算機系統或計算機數據儲存載體，但並非該計算機數據的接收者而獲取、使用資料仍構成該罪，第2款規定如上款所指的計算機數據涉及個人的私人生活，其法定最高刑高於上款犯罪行爲的最高法定刑罰，該罪屬於不經告訴不予處理。

(3) 破壞計算機信息、系統罪之比較

內地《刑法》第286條規定的破壞計算機信息系統罪與《打擊電腦犯罪法》第七條損害計算機數據罪、第8條干擾計算機系統罪相似，都是對非法破壞、干擾計算機信息、系統行爲的打擊。在其罪行的嚴重程度上還有明顯的不同，前者是對計算機系統及信息的破壞，以及故意製作、傳播計算機病毒行爲導致後果嚴重的情況下才能處罰；後者對電腦信息系統、數據的損害或干擾都規定了犯罪未遂仍予以處罰，並且把造成財產損失作爲法定的加重情節，其中第7條第4款第2項還明確如其電腦數據的特殊價值也作爲法定刑的加重情節。

(4) 提供實施犯罪的電腦程序罪之比較

內地《刑法》第285條第3款與《打擊電腦犯罪法》第9條共同的對非法提供實施計算機犯罪的程序行爲進行打擊。在罪行的具體規定上也存在着差別，前者規定爲提供專門侵入、非法控制計算機系統的程序、工具或者是在明知他人爲非法用途而予以提供且情節嚴重的行爲，予以處罰；後者除了專門提供之外還包括製造、進口、出口、出售、分發予以實施電腦犯罪的電腦裝置、計算機程序或電腦數據的行爲。由此可見兩者雖然都對非法提供犯罪工具的幫助行爲予以刑事打擊，但是後者的打擊範圍更爲寬泛，突出的反映了網絡犯罪中的信息、技術之間緊密聯繫的特點，對整個犯罪鏈條進行嚴厲地打擊和有效地防範。

(5) 利用計算機實施的其它犯罪之比較

內地《刑法》第287條總括性的對利用計算機實施的金融詐騙、盜竊、貪污、挪用公款、竊取國家秘密或者其它犯罪的，依照該法有關規定定罪處罰，沒有規定出具體犯罪的罪名、罪狀和處罰。而澳門《打擊電腦犯罪法》第10條計算機僞造、第11條計算機詐騙成立獨立的犯罪並具體的犯罪行爲以及刑罰都進行了詳細的規定。僅從形式上，內地的刑法對利用網絡實施的犯罪的刑法處罰範圍更爲廣泛，但是未能體現出利用網絡這一特殊的媒介和工具實施的傳統犯罪的行爲特點，不能真正實現通過刑法預防、打擊網絡犯罪的目的。澳門雖然僅在兩項法律條文中對利用電腦網絡實施的傳統犯罪進行獨立罪名的規定，但是這兩個罪名的規定是打擊網絡犯罪立法上的探索和突破，也爲司法實踐中打擊電腦僞造和電腦詐騙的犯罪提供了法律依據，並能夠讓司法實務部門在打擊犯罪中積累更多的經驗，從而促進相關的立法的改革和完善。

三、內地與澳門立法比較

兩地的網絡犯罪的概念、立法概況以及對網絡犯罪的刑事立法進行概括性的比較研究，可以發現內地刑法雖然對網絡犯罪的刑法規定在不斷進步，但是面對網絡犯罪對傳統犯罪形式的挑戰，以及其犯罪技能型、隱匿性、多樣性等特徵，內地現行刑法之相關規定出現了無法應對新形式網絡犯罪的困境。

澳門打擊網絡犯罪的法律不斷完善與發展，總結概括其主要體現了以下幾個特點：第一、立法縝密。澳門在通過在司法實踐過程中總結了網絡犯罪的特徵後，制定了專門的《打擊電腦犯罪法》，該法第2條定義中就分別對計算機系統、計算機數據、計算機程序、互聯網服務的登記用戶的基本數據等涉及該項法律中的技術術語予以明確的定義，能爲司法實踐對該類技術術語進行規範解釋的同時又體現了立法的縝密程度。第二、實體法與程序法的並重。澳門的立法中，完善刑事實體法的罪名設置和對相適應的刑事程序法的規定，主要體現在對電腦犯罪的扣押及特別措施的採取等，這是將刑事立法與刑事司法緊密結合的立法模式的突破，有利於打擊網絡犯罪的法律體系改革和完善。第三、科學的定罪、量刑。澳門打擊網絡犯罪的罪名規定中，除了保護公共網絡信息安全的同時還突出了對澳門居民的私人的網絡信息安全保護，凡未經許可而進入電腦系統或不當截取個人網絡數據信息的行爲都規定成立相應的犯罪，予以定罪處罰。同時考慮到網絡犯罪侵害到居民個人的隱私信息等問題，在對相關侵入獲取計算機及其信息的犯罪中，規定爲非經告訴不得進行刑事程序的罪刑。在量刑層面上，對未遂犯罪的處罰，如《打擊電腦犯罪》第6條規定的實施未經許可而借技術方法截取計算機系統未公開資料的行爲，犯罪未遂仍舊予以處罰。加強打擊網絡犯罪的合作與交流；在對網絡犯罪的量刑處罰中，將犯罪造成的財產損失作爲法定的加重情節，能對網絡犯罪的量刑有了法定的判斷依據。

內地網絡犯罪立法在網絡犯罪高犯罪率發展的今天，體現了立法者對網絡信息、財產安全的重視，但是對網絡犯罪的立法保護範圍和打擊力度仍存在很大的不足，主要表現在：一是中國現行刑法關於網絡犯罪的規定明顯站在維護國家利益和安全的立場上，對社會公共利益和個人權益的保護遠遠不夠，這有悖於現代法治觀念和人權觀念。[6] 二是立法對於計算機網絡信息系統的保護範圍過於狹窄，罪名設置較少，對於很多新型網絡犯罪並未直接加以規定，導致司法實踐中刑事法律規範可操作性差，立法仍舊只是網絡犯罪的“冰山一角”。三是在對網絡犯罪的打擊力度偏輕。中國刑法第285條、第286條規定犯罪後果特別嚴重的才處以5年以上有期徒刑(第286條第一款)，所規定侵害信息系統犯罪的法定刑種類單一，難以發揮刑罰的懲戒功能。從以上三方面的分析可見內地對網絡犯罪的刑事立法存在着法益保護範圍、罪名設置、以及刑罰規定上的單一，要實現有效預防和打擊網絡犯罪，還應該在加強理論和實務研究的基礎上通過比較借鑒來不斷的完善立法。

四、評析與建議

內地打擊網絡犯罪的立法與澳門進行比較後，二者在網絡犯罪的犯罪與刑罰、打擊範圍、立法技術等方面都存在着差異，並顯現出內地該項立法的缺陷和不足。因此就內地關於打擊網絡犯罪的刑事立法完善，提出以下幾點建議：

(一) 探索完善立法

針對當前網絡犯罪的多元化，制定專門打擊網絡犯罪的法律是當今經濟社會發展的必然趨勢。如澳門爲打擊網絡犯罪頒佈實施了專門打擊網絡犯罪的法律，內地可以此爲借鑒和參考，結合司法實踐部門尤其是公安部門打擊網絡犯罪的經驗爲基礎制定一章專門打擊網絡犯罪的刑法章節，此專門章節中要通過對網絡犯罪專門術語從立法上予以明確，同時還應擴大現行刑法中關於網絡犯罪的罪名設置來充實該專門章節的內容，通過立法機關自上而下的立法來實現網絡犯罪的立法規制，這樣才能夠最大程度的發揮法律對與實務部門提供法律依據，遵循“罪刑法定”原則來完善立法。

同時從多個角度充實現有立法體系。關於網絡犯罪的規範，可以從多個角度對立法體系進行充實。一方面，要提高立法的縝密程度。對於網絡犯罪中具體的技術用語的規範使用需要具體的司法解釋來予以明確界定，避免司法過程中對特定領域的不同解釋而導致裁判不公。另一方面，完善立法體系還應該對刑事程序法中相關內容予以規定，實現實體法和程序法相配合跟上網絡犯罪的動態變化，尤其在刑事訴訟法中要對網絡犯罪偵查中的扣押和強制手段、法定證據種類的制度予以探討和完善。

(二) 增加網絡犯罪罪名設置

通過與澳門立法進行比較，不難發現內地目前網絡犯罪的罪名設置不夠全面，不能有效打擊當今快速，多元的網絡犯罪。增加和完善與計算機犯罪相關罪名是對網絡犯罪立法完善的關鍵環節。這同樣要求從中國打擊網絡犯罪的實踐中來總結和歸納罪名的設置。首先，對計算機網絡系統、數據、信息的保護方面。可將該類的犯罪行爲增設破壞計算機系統、數據罪以及非法獲取計算機信息罪，這是以計算機的系統和信息安全爲主要保護客體，包括利用計算機病毒、蠕蟲等實施的行爲從法律上規定出其危險程度作爲規制犯罪的主要依據。其次，網絡信息傳播方面的犯罪。可增設以網絡實施的非法傳播淫穢信息罪，這樣從網絡信息傳播的源頭和傳播方式對網絡中非法傳播淫穢信息、謀取利益的行爲進行打擊，還應該給專門以未成年爲主要犯罪對象的行爲人處以較重的刑罰處罰，實現罪責刑相適應原則要求。再次，可增設網絡盜竊、網絡詐騙罪。這類罪名的規定是爲了更好的保護電子商務及電子消費的過程中公民、法人的商業秘密及財產利益(包括虛擬財產)。該類網絡犯罪表現出其犯罪影響範圍的廣泛性、犯罪對象的不特定性以及貪利性等特徵。以傳統刑法的盜竊與詐騙等財產犯罪的打擊已不足以應對以網絡爲主要工具和媒介實施的侵犯財產的犯罪，因此也不能緊戴着傳統犯罪的“帽子”來解決新型犯罪。應該設立專門的罪名進行規制通過從犯罪的主觀方面、客觀方面等來進行細化將能夠有效地震懾和防範網絡犯罪，只有通過專門的罪名設置，在刑法體系中從特殊罪名與一般罪名之間競合的關係，選擇適用特殊罪名的規定來對網絡實施的侵犯財產利益的行爲有效的打擊。

(三) 完善刑罰以及細化各罪的量刑情節

完善刑罰的規定，必須以“罪責刑相適應”的原則爲指導，以新增加罪名的社會危害性程度爲主要標準，在主刑中，設置幅度不同的有期徒刑，以及增加

管制、拘役等主刑的適用。在附加刑方面，由於網絡犯罪往往造成巨大的經濟損失，而且不少人實施犯罪的目的就是爲了牟利，所以對其科處罰金等財產刑應屬情理之中，但是中國刑法第285、286 條對網絡犯罪處罰既沒有規定罰金刑，也沒有規定資格刑。[7] 以此，建議將罰金這一附加刑加入刑罰體系當中。

對具體犯罪的量刑情節進行細化，避免自由裁量權的不當使用。對於非法入侵、破壞電腦系統、電腦數據的行爲，刑法中已經予以較爲詳盡的規定，這對保護電腦數據、系統安全以及網絡數據安全起到了積極的作用，有的罪名設置要求後果嚴重才予以處罰，因此要對嚴重的後果進行細化的規定。如澳門的立法中根據財產的損失、損害法益的性質作爲法定刑加重情節，這樣可以避免對網絡犯罪這一虛擬空間犯罪的嚴重後果判斷不准而對罪與非罪以及重罪與輕罪的判斷不准。

(四) 加強網絡犯罪打擊的國際、區際合作

網絡犯罪的跨國性，跨區域性的發展趨勢，對中國在完善網絡犯罪立法上提出了新的挑戰。在國際方面，一方面要加強與國際組織的合作，積極的履行國際條約中的義務和實現條約賦予的權利，如符合中國打擊網絡犯罪的特徵和要求可在國內完善立法；另一方面，與世界其他國家地區的合作，同樣是通過對法律制度的深入探討和研究來尋求共同的合作契機，加強兩國之間在打擊網絡犯罪上的司法協助，並能有效的解決法律制度不同而造成的管轄權衝突等問題。區際合作方面，深入分析與澳門立法進行比較，在比較借鑒的過程中同時還需要加強區際合作的主要方式，發現兩地立法的差異來尋求共同打擊區際網絡犯罪的合作契機。

五、結語

網絡犯罪伴隨着現代化網絡的爆炸式發展而出現並且急劇地擴散，也已發展成爲全球共同關注的犯罪，通過區際間網絡犯罪的刑法制度，吸收立法經驗，查缺補漏，有利於內地網絡犯罪立法的不斷完善與發展，才能更全面地防範與打擊網絡犯罪，進而穩固內地的經濟社會發展秩序，保障公民的人身、財產等合法權益。希望此文對兩地網絡犯罪的分析、比較及建議能對內地網絡犯罪的立法有所幫助。

註釋：

1 《網絡犯罪十年回顧》，載於《微電腦世界 PC World》，2011 年，第 3 期

2 向陽：《預防和懲治計算機犯罪的法律建構》，載於《法制與社會》，第 3 期，2011 年，68-69 頁

3 皮勇：《我國網絡犯罪刑法立法研究——兼論我國刑法修正案(七)中的網絡犯罪立法》，載於《河北法學》，2009 年 6 月，第 50 頁

4 非法控制計算機罪，指故意非法控制國家事務、國防建設、尖端科學技術領域之外的計算機信息系統情節嚴重的行爲。

5 指提供專門用於侵入、非法控制計算機信息系統的程序、工具，或者明知他人實施侵入、非法控制計算機信息系統違法犯罪行爲而爲其提供程序、工具，情節嚴重的行爲。

6 王光坤：《試論我國網絡犯罪及刑事立法完善》，北京，中國政法大學碩士學位論文，2006 年，第 27 頁。

7 同上註。