前瞻科技與管理　8 卷 2 期，59-80 頁（2018 年 11 月）
Journal of Advanced Technology and Management Vol. 8, No. 2, pp. 59-80 (November, 2018)
DOI:10.6193/JATM.201811_8(2).0003

中國大陸網路安全審查制度研究

陳銘聰 *

國立臺灣大學國家發展研究所博士生

摘 要

中國大陸網民數量躍居世界第一，已經成為網路大國，網路安全審查制度的推出，成為維護網路安全最有效的依據。為此，中國大陸當局制定相關法律法規對網路安全審查制度進行規定，對網路安全審查內容進行細化，增強針對性和可操作性。2018 年 3 月，中共中央網路安全和資訊化領導小組改為中共中央網路安全和資訊化委員會，將網路安全審查的行政級別提升到國家機關級別，將國家安全作為網路安全審查的目標。事實上，中國大陸當局進行網路安全審查已經不是新聞，而是早已落實到人民的生活面上，隨著網路時代的到臨，人民日常生活皆與網路脫不了關係，中國大陸當局是否會假網路安全審查之名，行國家監控之實，侵犯人民基本權利，值得我們關注。

關鍵詞：國家安全、資訊安全、網路安全、網路空間、審查

* 通訊作者：陳銘聰
電子郵件：d06341002@ntu.edu.tw
（收件日期：2018 年 6 月 27 日；修正日期：2018 年 8 月 20 日；接受日期：2018 年 8 月 24 日）

Journal of Advanced Technology and Management Vol. 8, No. 2, pp. 59-80 (November, 2018)
DOI:10.6193/JATM.201811_8(2).0003

Research on Network Security Review System in China

Ming-Tsung Chen*

Ph.D. Student, Graduate Institute of National Development, National Taiwan University

Abstract

The number of Internet users in China ranks first in the world and China has become a big country in the Internet. The introduction of Internet security censorship system has become the most effective basis for maintaining network security. In this regard, the mainland authorities have formulated relevant laws and regulations to regulate the network security review system, refine the content of the network security review, and enhance the pertinence and operability. In March 2018, the Central Leading Group on Network Security and Information Technology was transformed into the Central Committee on Network Security and Information Technology of the Communist Party of China, the administrative level of network security review has been upgraded to the level of state organs, and national security has been taken as the goal of network security review. In fact, the Internet security review by the Chinese authorities is no longer news, but has long been implemented in people's lives. With the advent of the Internet age, people's daily lives are inextricably linked to the Internet. Whether the mainland authorities will conduct state monitoring in the name of Internet security censorship and violate people's basic rights deserves our attention.

Keywords: national security, information security, network security, cyberspace, review

* Corresponding Author: Ming-Tsung Chen
E-mail: d06341002@ntu.edu.tw

壹、前言

2018 年 4 月 28 日，中國大陸兩大網路[1]科技企業「北京字節跳動科技有限公司」與「奇虎 360 科技有限公司」的中共黨委，舉行黨員座談會，兩公司決策高層紛紛表示，強調要做好正能量傳播、加強行業自律，落實中共中央對網路安全審查工作的決策部署。其中，字節跳動公司，要求企業與國家發展政策融合在一起，為建設「數字絲綢之路」[2]盡一份企業的「責任」，而該公司所謂的「責任」，就是確保企業配合國家發展政策，決不能讓網路成為傳播有害資訊、[3]造謠生事的平臺，是網路企業必須堅持的底線。另外，奇虎 360 公司表示，要將「關口前移」，該措施就是把網路安全防護的關口前移到一線，將加強在關鍵資訊基礎設施投入，準備預案，及時採取緊急措施，將網路攻擊造成的損失降到最低；同時將加強日常審查，透過「魔鏡」等檢測工具，掌握網路安全真實情況。資料顯示，字節跳動公司在海外的使用者已超過兩億人，是中國大陸唯一能夠與 Facebook、Google、Youtube 競爭的陸資企業，而奇虎 360 公司則是中國大陸最大的網路安全企業，兩家公司的黨委號召公司員工學習「全國網信工作會議精神」，這一「政治正確」的舉動，讓不少中國大陸網民疑惑字節跳動公司、奇虎 360 公司究竟是國有企業還是私營企業（汪莉絹，2018）？

上述兩大公司為加強對網路空間的控制，開始強化網路科技公司裡的黨委作用，該舉動表示網路安全審查將全面啟動。在此之前，中國大陸當局已經相繼制定《國家安全法》、《網路安全法》、《國家網路空間安全戰略及網路產品》和《服務安全審查辦法（試行）》，透過這些法律法規對網路安全審查制度進行規定，並對網路安全審查的內容進行細化，增強了其針對性和可操作性。自「中國共產黨第十九次全國代表大會」（簡稱十九大）後，網路安全審查更無所不在，一方面體現對網路安全的關注，另一方面也顯示，網路安全等非傳統安全威脅持續蔓延，中國大陸當局將面臨更多的挑戰。

貳、網路安全審查制度的基本概況

自網路誕生開始，就與國家安全結下不解之緣，隨著網路持續滲入人民生活的方方面面，同時也開啟國家安全的新領域，亦即，國家安全不僅保障「現實世界」中有形的、以主權為代表核心價值的安全，而且還要求能夠對「網路空間」中關鍵資訊基礎設施、跨境資料流動、網路資訊等支撐社會生活正常運作的各種行為，保持必要的控制，確保國家的核心利益處於免受威脅和可持續發展的狀態。

---

[1] 網路在中國大陸稱為網絡。

[2] 數字絲綢之路，是中國國家主席習近平主席在「一帶一路國際合作高峰論壇」開幕式上的演講中指出：「我們要堅持創新驅動發展，加強在數位經濟、人工智慧、納米技術、量子電腦等前沿領域合作，推動大資料、雲計算、智慧城市建設，連接成 21 世紀的數字絲綢之路。」（劉思琦編，2017）

[3] 資訊在中國大陸稱為信息。

一、制度形成

2014 年 5 月 16 日，中國大陸「中央國家機關政府採購中心」（2014）[4] 發出一份重要通知：「要求國家機關進行資訊類協定供貨強制節能產品採購時，所有電腦類產品不允許安裝 Windows 8 作業系統」。雖然通知並未解釋禁止所採購的電腦類產品安裝 Windows 8 作業系統的原因，有評論指出國家資訊安全是其原因之一（董樂，2014），甚至業內專家指稱，網路安全風險才是禁購 Windows 8 作業系統的主要原因之一（王軼駿、薛質、傅卓異，2013），不過，有媒體引述官員的意見，這個通知與網路安全審查制度沒有任何的聯繫，只是個案（劉雪玉，2014）。

2014 年 5 月 22 日，中國大陸國家網際網路資訊[5] 辦公室[6] 發布公告（下稱網信辦公告）：「為維護國家網路安全、保障中國用戶合法利益，中國將推出網路安全審查制度。」「關係國家安全和公共利益的系統使用的、重要資訊技術產品和服務，應通過網路安全審查。」（趙勇，2014）前者為審查目的，後者為審查範圍，根據網信辦公告，網路安全審查係指對關係國家安全和公共利益的系統使用的重要資訊技術產品和服務進行的安全審查，該審查以產品和服務的安全性、可控性為重點，旨在防止產品和服務的提供者非法控制、干擾、中斷用戶系統，非法收集、儲存、處理和利用用戶有關資訊，不符合安全審查要求的產品和服務不得在中國境內使用（楊光，2014）。因此，網信辦公告關於網路安全審查制度的內容，大致如表 1。

表 1　網路安全審查制度的內容

項目	內容
審查範圍	關係國家安全和公共利益的系統使用的重要技術產品和服務。
審查重點	產品的安全性和可控性。
審查目的	防止產品提供者非法控制、干擾、中斷用戶系統，非法收集、儲存、處理和利用用戶有關資訊。
如何管理	對不匹配安全要求的產品和服務，將不得在中國大陸境內使用。

資料來源：作者整理。

2014 年 5 月 23 日，《人民日報》指出當前中國大陸的網路安全問題為：少數國家政府和企業利用產品的單邊壟斷和技術優勢大規模收集敏感資料，以及政府部門、機構、企業、大學及電信主幹網路遭受大規模侵入、監聽（史竟男、白陽、張洋、鄭會燕，2014）。

結合上述事件的時間點，中國大陸當局把禁購 Windows 8 視為國家採取網路安全審查制度的具體體現，可視為推行網路安全審查的前奏。由此可知，中國大陸網路安全審查制度主

[4] 中央國家機關政府採購中心（簡稱：中央政府採購中心），是根據《國務院辦公廳關於印發中央國家機關全面推行政府採購制度實施方案的通知》（國辦發 2002-53 號）和中央機構編制委員辦公室《關於國務院機關事務管理局成立中央國家機關政府採購中心的批復》（中央編辦複字 2002-163 號）的規定，於 2003 年 1 月 10 日正式成立的，是中央國家機關政府集中採購的執行機構，是經註冊的獨立事業法人。

[5] 網際網路在中國大陸稱為互聯網，資訊在中國大陸稱為信息。

[6] 原名為國家互聯網信息辦公室，現已改為中共中央網絡安全和信息化委員會辦公室。

要是與資訊技術相關的產品和服務之審查，著重於「國家安全」和「公共利益」的重要技術產品和服務，審查重點是針對產品的「安全性」和「可控性」（張棉棉，2014），即網路安全審查的核心要求——「自主可控」（倪光南，2018）。換言之，即網路空間能夠自主可控，產品和服務就不存在惡意後門，並可以不斷改進或修補漏洞，網路安全就獲得保護；反之，不能自主可控，就會受制於人，產品和服務容易存在惡意後門，並難以改進或修補漏洞，網路安全就難以獲得保護。

二、理論基礎

網路安全審查的理論基礎是「網路空間主權原則」，網路空間已成為國家繼「陸地、海洋、天空、太空」四個疆域之後的「第五疆域」（劉彥華，2017），與其他疆域一樣，網路空間也需要體現國家主權，保護網路空間也就是保護國家主權。根據網路空間主權理論，國家有權獨立自主地決定並採取一切防衛本國網路安全的正當措施，管理包括網路安全立法在內的一切與本國網路空間有關的事務，歸根究底，該理論為各國提供在激烈的網路空間競爭中，採取有效措施捍衛本國利益的理論依據。

「網路空間主權」是進入網路時代的新生名詞，是國家主權在網路空間的自然延伸，包括四項基本權力：一是網路空間「獨立權」，即一國在網路空間中不受制於任何國家和組織，對其網路系統、資源以及應用技術等獨立自主地進行管理和控制的權力。獨立權的行使以不侵犯他國主權為前提，在當代，各國的主權會體現出一定的相對性，這是各國對主權限制的自願接受，並非是對獨立權的放棄（李營輝，2016），這個規則同樣適用於網路空間，即網路空間獨立權的行使不應侵犯到他國的網路空間主權。二是網路空間「平等權」，即指各國在網路空間主權平等，對於網路空間的管理，主權國應在平等和互相尊重的基礎上進行協商，基於平等方式實現互聯互通，而不能因擁有網路資源的不平等造成主權國家網路空間地位的不平等，或由某一個國家憑藉技術優勢來控制網路空間。三是網路空間「自衛權」，是一國針對域外網路攻擊進行防衛的權力，主權國家可採取必要的措施、手段保護本國網路以及在其中運行的軟、硬體不受攻擊，同時，對外來攻擊可予以反擊。四是網路空間「管轄權」，是一國對其國內網路空間的最高管理權，包括對國內資訊系統的管理和對國土範圍內的一切網路活動。

2016 年 12 月 27 日，經中央網路安全和資訊化領導小組[7]批准，國家互聯網資訊辦公室發布《國家網路空間安全戰略》（中國網信網，2016）指出：「網路空間已經成為與陸地、海洋、天空、太空同等重要的人類活動新領域，國家主權拓展延伸到網路空間，網路空間主權成為國家主權的重要組成部分。尊重網路空間主權，維護網路安全，謀求共治，實現共贏，正在成為國際社會共識。」而針對「網路空間主權原則」，《國家網路空間安全戰略》也指出：「網路空間主權不容侵犯，尊重各國自主選擇發展道路、網路管理模式、網際網路公共政策

[7] 2018 年 3 月，根據中共中央印發《深化黨和國家機構改革方案》，將中央網路安全和資訊化領導小組改為中共中央網路安全和資訊化委員會。

和平等參與國際網路空間治理的權利。各國主權範圍內的網路事務由各國人民自己做主，各國有權根據本國國情，借鑒國際經驗，制定有關網路空間的法律法規，依法採取必要措施，管理本國資訊系統及本國疆域上的網路活動；保護本國資訊系統和資訊資源免受侵入、干擾、攻擊和破壞，保障公民在網路空間的合法權益；防範、阻止和懲治危害國家安全和利益的有害資訊在本國網路傳播，維護網路空間秩序。任何國家都不搞網路霸權、不搞雙重標準，不利用網路干涉他國內政，不從事、縱容或支持危害他國國家安全的網路活動。」

三、法律體系

截至 2013 年底，中國大陸的網路用戶數已經是高居世界第一（高少華、葉健，2014），因此，網路安全審查制度的建立也就刻不容緩，從 2014 年 5 月到 2017 年年底，中國大陸當局積極推動網路安全審查制度的建設，在立法層面取得一定進展，並逐步建構網路安全審查法律體系，按時間先後，分述如下：

（一）國家安全法

2015 年 7 月 1 日，《國家安全法》公布施行，立法中首次出現網路安全審查的相關內容，雖僅有幾字描述，例如第 25 條：「國家建設網路與資訊安全保障體系，提升網路與資訊安全保護能力，加強網路和資訊技術的創新研究和開發應用，實現網路和資訊核心技術、關鍵基礎設施和重要領域資訊系統及資料的安全可控；加強網路管理，防範、制止和依法懲治網路攻擊、網路入侵、網路竊密、散布違法有害資訊等網路違法犯罪行為，維護國家網路空間主權、安全和發展利益。」第 59 條：「國家建立國家安全審查和監管的制度和機制，對影響或者可能影響國家安全的外商投資、特定物項和關鍵技術、網路資訊技術產品和服務、涉及國家安全事項的建設項目，以及其他重大事項和活動，進行國家安全審查，有效預防和化解國家安全風險。」（《中華人民共和國國家安全法》，2015）

《國家安全法》提升網路與資訊安全保護能力，加強網路和資訊技術的創新研究和開發應用，實現網路和資訊核心技術、關鍵基礎設施和重要領域資訊系統及資料的安全可控。此外，《國家安全法》加強網路管理，防範、制止和依法懲治網路攻擊、網路入侵、網路竊密、散布違法有害資訊等網路違法犯罪行為，維護國家網路空間主權、安全和發展利益，尤其是為該制度的構建奠定了法律基礎，確立國家網路與資訊安全保障體系。

（二）網路安全法

2016 年 11 月 7 日，《網路安全法》公布施行，部分條文對構建網路安全審查制度有著重要的啟發和參考價值，其明確關鍵基礎資訊基礎設施中可能影響國家安全的網路產品和服務，應當通過網路安全審查。《網路安全法》是中國大陸網路安全領域中的基本法，雖然該法涉及網路安全審查的內容有限，例如，第 35 條：「關鍵資訊基礎設施的運營者採購網路產品和服務，可能影響國家安全的，應當通過國家網信部門會同國務院有關部門組織的國家安全審查。」第 65 條：「關鍵資訊基礎設施的運營者違反本法第 35 條規定，使用未經安全審查或者安全審查未通過的網路產品或者服務的，由有關主管部門責令停止使用，處採購金額一倍以上十倍以下罰款；對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元

以下罰款。」（《中華人民共和國網絡安全法》，2016）該法是構建網路安全審查制度的法律基礎，換言之，中國大陸網路安全審查制度必須體現網路安全法的法律精神，與該法形成呼應。

（三）國家網路空間安全戰略

2016 年 12 月 27 日，《國家網路空間安全戰略》發布，主要針對保護關鍵資訊基礎設施進行規範，內容主要分為四個部分：

第一，強調國家關鍵資訊基礎設施是指關係國家安全、國計民生，一旦資料洩露、遭到破壞或者喪失功能可能嚴重危害國家安全、公共利益的資訊設施，包括但不限於提供公共通信、廣播電視傳輸等服務的基礎資訊網路，能源、金融、交通、教育、科研、水利、工業製造、醫療衛生、社會保障、公用事業等領域和國家機關的重要資訊系統，重要互聯網應用系統等。

第二，採取一切必要措施保護關鍵資訊基礎設施及其重要資料不受攻擊破壞。堅持技術和管理並重、保護和震懾並舉，著眼識別、防護、檢測、預警、回應、處置等環節，建立實施關鍵資訊基礎設施保護制度，從管理、技術、人才、資金等方面加大投入，依法綜合施策，切實加強關鍵資訊基礎設施安全防護。而關鍵資訊基礎設施保護是政府、企業和全社會的共同責任，主管、運營單位和組織要按照法律法規、制度標準的要求，採取必要措施保障關鍵資訊基礎設施安全，逐步實現先評估後使用。

第三，加強關鍵資訊基礎設施風險評估。一是加強黨政機關以及重點領域網站的安全防護，基層黨政機關網站要按集約化模式建設運行和管理。二是建立政府、行業與企業的網路安全資訊有序共用機制，充分發揮企業在保護關鍵資訊基礎設施中的重要作用，堅持對外開放，立足開放環境下維護網路安全。

第四，建立實施網路安全審查制度，加強供應鏈安全管理，對黨政機關、重點行業採購使用的重要資訊技術產品和服務開展安全審查，提高產品和服務的安全性和可控性，防止產品服務提供者和其他組織利用資訊技術優勢實施不正當競爭或損害用戶利益。

從上述可知，《國家網路空間安全戰略》將實施網路安全審查作為保護關鍵資訊基礎設施的重要舉措，要求對「黨政機關」、「重點行業」採購使用的重要資訊技術產品和服務進行安全審查，並要求強化對供應鏈的安全管理，提高產品和服務的安全性和可控性。《國家網路空間安全戰略》作為網路安全審查體系中的重要組成部分，這些內容必然構成網路安全審查立法的基本精神，要求網路安全審查能夠在開放的網路環境下積極對抗網路竊密、洩密等安全風險，成為有效的安全防禦手段，從而更好地維護國家安全、捍衛網路空間主權。同時，《國家網路空間安全戰略》在網路安全基礎戰略任務中，提出加強認證認可標準化工作，做好等級保護、風險評估、漏洞發現等基礎性工作的要求，網路安全審查立法也應對此予以體現。

（四）網路產品和服務安全審查辦法（試行）

2017 年 5 月 2 日，《網路產品和服務安全審查辦法（試行）》公布施行，這為有關部門進行網路安全審查工作提供具體實施規則，且在同年 6 月 1 日起在中國大陸國境內實施。

《網路產品和服務安全審查辦法（試行）》使得網路安全審查立法內容得到細化，增強其針對性和可操作性，根據第 1 條規定，該辦法是基於《國家安全法》、《網路安全法》等法律法規為依據，一共十六個條文，是當前中國大陸網路安全審查的具體實施規則，將網路安全審查的核心內容明確規範，包括：審查對象、審查方式、審查內容、審查機構、審查程序及審查監督等。審查辦法已經建構起中國大陸網路安全審查制度的基本框架，也是落實《國家安全法》第 25 條和《網路安全法》第 35 條的重要措施，預示著中國大陸在網路管理方式已經由表層化向深層化發展，範圍由黨政軍的重要資訊系統擴大至關係國家安全的所有網路及資訊系統。同時，《網路產品和服務安全審查辦法（試行）》也標誌著中國大陸決心改變資訊技術產品和服務受制於外國的局面，並邁出實質性的步伐（張莉，2017）。

四、機構改革

2018 年 3 月，根據中共中央印發的〈深化黨和國家機構改革方案〉（新華社，2018），該方案加強中共中央對涉及黨和國家事業全局的重大工作的集中統一領導，強化決策和統籌協調職責，將中央全面深化改革領導小組、中央網路安全和資訊化領導小組、中央財經領導小組、中央外事工作領導小組分別改為中央全面深化改革委員會、中央網路安全和資訊化委員會、中央財經委員會、中央外事工作委員會，負責相關領域重大工作的頂層設計、總體布局、統籌協調、整體推進及督促落實。

在網路空間管理方面，將原本的「中共中央網路安全和資訊化領導小組」改為「中共中央網路安全和資訊化委員會」，[8] 並以「中共中央網路安全和資訊化委員會辦公室」作為辦事機構，強化其職責，並將國家電腦網路與資訊安全管理中心由工業和資訊化部管理調整為由中央網路安全和資訊化委員會辦公室管理，原本的工業和資訊化部仍負責協調電信網、網際網路、專用通信網的建設，組織、指導通信行業技術創新和技術進步，對國家電腦網路與資訊安全管理中心基礎設施建設、技術創新提供保障，在各省（自治區、直轄市）設置的通信管理局管理體制、主要職責、人員編制維持不變（新華社，2018）。從上述「領導小組」、「委員會」及「辦公室」可以得知，中國大陸當局為維護國家網路空間安全和利益，已經將網路安全審查的行政級別提升到國家機關級別，更將國家安全作為網路安全審查的首要目標。

五、制度評析

網路安全審查是國家安全的重要舉措，而中國大陸網路安全審查制度主要針對兩大類風險：一類是針對重要、關鍵資訊系統的安全風險，主要表現為資訊系統被他人控制、干擾、破壞等，該類風險一旦發展到嚴重程度，將導致中國大陸重要行業和領域的運行出現癱瘓；

[8] 該方案稱：為加強黨中央對涉及黨和國家事業全局的重大工作的集中統一領導，強化決策和統籌協調職責，將中央全面深化改革領導小組、中央網路安全和資訊化領導小組、中央財經領導小組、中央外事工作領導小組分別改為中央全面深化改革委員會、中央網路安全和資訊化委員會、中央財經委員會、中央外事工作委員會，負責相關領域重大工作的頂層設計、總體布局、統籌協調、整體推進及督促落實。

另一類是針對儲存或運行於資訊系統中的資訊的安全風險，簡單說，主要是竊密和資訊洩露風險，這些資訊必然有一部分是國家各方面運行的資料和國家秘密，一旦被洩露和利用，將嚴重威脅國家安全。需要進一步說明的是，網路安全審查是一項對網路產品和服務進行包括但不限於技術安全審查的綜合性安全風險審查措施，隨著各國在網路空間的競爭不斷升級，構成網路安全威脅的因素不僅有來自技術方面的風險，還有很多非技術方面的隱形風險，因此，開展網路安全審查，不僅要審查技術，還應對產品和服務背後的隱藏性風險進行審查，例如對供應鏈、對核心技術人員的背景等進行審查，以此增強產品、服務的安全性和可控性（左曉棟，2015）。但是需要明確的是，雖然網路安全審查係指對重要資訊技術產品和服務進行的安全審查，未來可能擴大到儲存在產品、服務系統中的資料和資訊等內容。

當前中國大陸核心技術和關鍵設備依然處於追趕狀態，部分高端產品和核心部件仍然依賴國外，導致美國制裁中興事件的發生。2018 年 4 月 16 日，美國商務部於宣布 7 年內禁止美國企業向中國的電信設備製造商中興通訊公司銷售零件及其後續事件，隨即讓這家電信大廠進入「休克狀態」，在中國大陸掀起軒然大波，由此可知，中國大陸網路基礎設施供應鏈安全問題不斷凸顯，為提升網路產品和服務的安全性、可行性，防範供應鏈安全風險。2018 年 4 月 21 日，中國大陸國家主席習近平出席「全國網絡安全和信息化工作會議」，指出「核心技術」是國之重器，要下定決心、保持恆心、找準重心，加速推動資訊領域核心技術突破（風傳媒國際中心，2018）。

參、網路安全審查制度的主要內容

網路安全審查制度的核心內容就是提供足夠的保障能力，而保障能力也是判斷網路安全審查法律體系實施效果的判斷標準（馬民虎，2007）。當前，《國家安全法》、《網路安全法》、《國家網路空間安全戰略》及《網路產品和服務安全審查辦法（試行）》等已經公布施行或發布，從立法功能上來看，它們應當具備保障網路安全審查持續、穩定運行，有效防禦網路安全風險和威脅的能力；從立法形式上來看，它們應同時包含實體性法律規範和程序性法律規範。然而，就當前立法內容來看，網路安全審查實體性法律規範內容仍存在不足，程序性法律規範內容也較為薄弱，可操作性有待加強。對此，本文從審查重點、審查標準、網路清理、資訊儲存、企業配合及審查機構等方面，針對現有的條文內容，提出完善建議，以促進既有立法內容進一步深化。

一、審查重點

（一）審查目標

網路安全審查目標是「國家安全」，根據《國家安全法》第 59 條：「國家建立國家安全審查和監管的制度和機制，對影響或者可能影響國家安全的外商投資、特定物項和關鍵技術、網路資訊技術產品和服務、涉及國家安全事項的建設項目，以及其他重大事項和活動，進行國家安全審查，有效預防和化解國家安全風險。」（《中華人民共和國國家安全法》，

2015）根據《網路安全法》第 35 條：「關鍵資訊基礎設施的運營者採購網路產品和服務，可能影響國家安全的，應當通過國家網信部門會同國務院有關部門組織的國家安全審查。」（《中華人民共和國網絡安全法》，2016）根據《網路產品和服務安全審查辦法（試行）》（2017）第 2 條：「關係國家安全的網路和資訊系統採購的重要網路產品和服務，應當經過網路安全審查。」

（二）審查內容

網路安全審查目標是網路產品和服務，根據《網路產品和服務安全審查辦法（試行）》第 4 條，網路安全審查重點審查網路產品和服務的安全性、可控性，主要包括以下五種內容：一是產品和服務自身的安全風險，以及被非法控制、干擾和中斷運行的風險；二是產品及關鍵部件生產、測試、交付、技術支援過程中的供應鏈安全風險；三是產品和服務提供者利用提供產品和服務的便利條件非法收集、存儲、處理、使用用戶相關資訊的風險；四是產品和服務提供者利用用戶對產品和服務的依賴，損害網路安全和用戶利益的風險；五是其他可能危害國家安全的風險。

（三）審查對象

網路安全審查對象，根據《網路安全法》第 35 條的規定是「關鍵資訊基礎設施」，根據中國大陸當前對「關鍵資訊基礎設施」的界定，從字面意思理解，它是屬於「關係國家安全和公共利益的系統」，再根據《網路安全法》第 31 條，關鍵資訊基礎設施應當「實行重點保護」，可知關鍵資訊基礎設施是網路安全審查的重點領域。不過，《網路產品和服務安全審查辦法（試行）》第 2 條規定並未用「關鍵資訊基礎設施」一詞，而是用「關係國家安全的網路和資訊系統採購的重要網路產品和服務」，本文以為，後者的內涵其實就是「關鍵資訊基礎設施」。

（四）供應鏈安全管理

網路產品和服務本身就具有複雜性，其中的後門和漏洞已經對國家網路安全產生巨大威脅，網路基礎設施供應鏈安全管理，將為提升網路產品和服務的安全性、可行性，防範供應鏈安全風險。在貿易全球化、網路無國界的背景下，其供應鏈在世界範圍延伸、流轉，鏈條變得更加脆弱，這就進一步加劇網路安全威脅。供應鏈上存在諸多脆弱節點，其中任何節點都有被利用的可能性，一旦被中斷或受到攻擊，都將導致一國資訊被竊取或資訊及資訊系統被破壞，帶來嚴重損失和後果（馮琳，2015）。在此情況下，加強網路產品和服務供應鏈的安全審查已成為保障國家網路安全的重要舉措，例如美國政府審計署（The Government Accountability Office, GAO）曾明確指出：「通過全球供應鏈提供的網路產品和服務存在危及聯邦資訊安全的威脅，聯邦機構須識別和防範該類供應鏈風險」（馬民虎、馬寧，2014）。而中國大陸《國家網路空間安全戰略》（中國網信網，2016）也明確指出：「建立實施網路安全審查制度，加強供應鏈安全管理，……提高產品和服務的安全性和可控性，防止產品服務提供者和其他組織利用資訊技術優勢實施不正當競爭或損害用戶利益。」

二、審查標準

關於審查標準，法律法規體系中的四部法規都有提及，例如《國家安全法》第 72 條：「應當按照國家有關規定和標準對國家安全物資進行收儲、保管和維護」（《中華人民共和國國家安全法》，2015）。《網路安全法》第 7 條：「國家積極開展網路空間治理、網路技術研發和標準制定」。第 10 條：「建設、運營網路或者通過網路提供服務，應當依照法律、行政法規的規定和國家標準的強制性要求，採取技術措施和其他必要措施，保障網路安全、穩定運行，有效應對網路安全事件，防範網路違法犯罪活動，維護網路資料的完整性、保密性和可用性。」第 15 條：「國家建立和完善網路安全標準體系。」（《中華人民共和國網絡安全法》，2016）《國家網路空間安全戰略》更在多處提到標準一詞，例如資訊技術標準、標準規範逐步建立、不搞雙重標準制度、標準的要求、加強網路安全標準化和認證認可工作、標準規範等，而《網路產品和服務安全審查辦法（試行）》（2017）第 11 條也提到：「承擔網路安全審查的第三方機構，應當堅持客觀、公正、公平的原則，按照國家有關規定，參照有關標準，重點從產品和服務及其供應鏈的安全性、可控性，安全機制和技術的透明性等方面進行評價，並對評價結果負責。」

不過，當前的法律體系僅提到「審查標準」，卻並沒有規範「具體細目」，導致無法為審查活動提供有效依據和行使界限，這容易造成主管機關的恣意和濫權，假網路安全審查之名，行國家監控之實，對此，中國大陸網路安全審查制度的立法完善，必須要加快審查標準中「具體細目」的建設工作。

三、網路清理

《網路安全法》針對網路空間中容易流傳許多違法資訊，要求網路運營者必須自我審查網路的內容，網路運營者應當加強對其用戶發布的資訊的管理，發現法律、行政法規禁止發布或者傳輸的資訊的，應當立即停止傳輸該資訊，採取消除等處置措施，防止資訊擴散，保存有關記錄，並向有關主管部門報告。

所謂發現法律、行政法規禁止發布或者傳輸的資訊，一般係指《網路安全法》第 12 條第 2 項的違法資訊，包括：危害國家安全、榮譽和利益，煽動顛覆國家政權、推翻社會主義制度，煽動分裂國家、破壞國家統一，宣揚恐怖主義、極端主義，宣揚民族仇恨、民族歧視，傳播暴力、淫穢色情資訊，編造、傳播虛假資訊擾亂經濟秩序和社會秩序，以及侵害他人名譽、隱私、智慧財產權和其他合法權益等活動。可以發現，同性戀題材並不在違法資訊所包括的範圍之內，我們有理由相信，微博絕對不會是單一個案，未來網路運營者將不斷進行自我審查並自行擴張對違法資訊的範圍，可見網路安全法所引發的「寒蟬效應」（鄺承華，2002）。

2018 年 4 月 13 日，微博宣布為遵循《網路安全法》第 47 條的要求，展開為期 3 個月的清理行動，對象包括涉黃的、宣揚血腥暴力、同性戀題材的漫畫及圖文短視頻內容，以及含有暴力內容的違法遊戲，將關閉違規嚴重的帳號，以及存在違規內容的話題，還鼓勵社群依《網路安全法》第 49 條進行舉報。此舉引起廣大同性戀用戶及同性戀支持社群的反彈，

大量的「＃我是同性戀＃」、「＃我是同性戀的朋友＃」、「＃我是同性戀，我拒絕被清查＃」等支援同性戀的相關標籤紛紛出現於微博上。同性戀支持者抗議微博將同性戀與涉黃、暴力畫上等號，也呼籲微博應尊重多元文化，2018 年 4 月 16 日，微博清理政策急轉彎，宣布清理對象將排除同性戀內容（陳曉莉，2018）。

四、資訊儲存

資訊儲存所規範的包括關鍵資訊基礎設施和關鍵資訊基礎設施的運營者。首先，關鍵資訊基礎設施，根據《網路安全法》第 31 條規定，係指公共通信和資訊服務、能源、交通、水利、金融、公共服務、電子政務等的產業，會特別實行重點保護，原因在於其一旦遭到破壞、喪失功能或者資料洩露，可能嚴重危害國家安全、國計民生及公共利益等。其次，關鍵資訊基礎設施的運營者，根據《網路安全法》第 37 條規定，要求關鍵資訊基礎設施的運營者在中國大陸境內運營中收集和產生的個人資訊和重要資訊應當在中國大陸境內儲存（《中華人民共和國網絡安全法》，2016）。當某企業被認定為關鍵資訊基礎設施的運營者，尤其是雲端運算企業，主管機關會將其列入專門的管制對象，此舉將在一定程度上避免大量的個人資訊和國家的敏感資訊流通到境外。在此之前，在重點領域的資訊科技產品中，境外產品占有較大分額，該項制度的實施會讓這種趨勢得以緩解，並對境內雲端運算企業影響，這也是中國大陸對境內的雲端運算服務相關企業的政策性扶持。

應該注意的是，《網路安全法》第 37 條規定並非要求所有網路運營者收集的個人資訊都要儲存在中國大陸境內，而僅限於關鍵資訊基礎設施運營者在其在中國大陸境內的運營活動中收集和產生的個人資訊。換言之，一旦落入關鍵資訊基礎設施的運營者範疇，該法將直接影響到其將在中國大陸境內運營過程中收集和產生的個人資訊和業務資料向境外傳輸的行為。當前全球市場已經深度融合，中資企業想要走出去、外資企業想要走進來的大背景下，以企業為主體的業務資訊跨境流動已經十分普遍，特別是透過網路提供資訊服務的企業而言更是如此。因此，關鍵資訊基礎設施的範圍及其帶來的資料傳輸限制，對部分企業的業務正常開展，可能會產生根本性影響，甚或造成實質性阻礙，形成貿易壁壘，限制外國企業和技術產品進入中國大陸市場，也難怪在 2016 年 8 月，46 家在華國際企業團體為此聯名致函國務院總理李克強，抗議《網路安全法》部分條文對資訊的限制，已經違反世界貿易組織的規則（海彥，2016）。

五、企業配合

《網路安全法》第 28 條規定，網路運營者在維護國家安全或調查犯罪應與中國大陸當局（主要是公安機關、國家安全機關）密切合作，在需要時為政府部門提供技術支持和協助，因此，在推動網路安全治理工作，必須確保做到以下具體措施：一是自覺淨化網路空間。網信企業[9]應自覺遵守國家法律、法規和政策，堅守職業道德，自覺抵制不法行為。二是做

[9] 網信企業，即網路資訊企業，由於中國大陸將資訊稱為信息，因此簡稱網信企業。

好客戶教育培訓。網信企業要把先進的網路安全技術產品與以客戶為導向的優質服務充分結合起來，讓客戶能夠非常清晰、直觀地瞭解到網路安全保障的產品功能、服務內容與價值，從而建立起信任。三是積極參與網路安全公眾宣傳教育。網信企業應當積極參與國家和地方的網路安全宣傳活動、暢通公眾投訴舉報管道，提高有害資訊發現和處置能力，並激發民眾參與的積極性、提升民眾的安全意識。四是成為貫徹落實網路安全相關法規的典範。網信企業應當自覺加強網路安全保護意識，建立嚴格的內部管理體系，不僅強化對自身資訊系統、敏感資料的保護，同時向客戶交付高品質的產品和服務，保障客戶資料資產的安全和隱私。五是培養網路安全領域合格人才。要根據網路安全市場人才的實際需求，對網路安全領域人才進行有目標的培養。六是做好技術與服務保障。在網路安全治理工作中，網路安全企業要提供多方面的網路安全保障，包括網路安全技術與產品、安全運維及安全事件回應與處置等（陳興躍，2017）。

六、審查機構

網路安全審查不是行政審批，主要對重要網路產品和服務採取的事中和事後監管，堅持實驗室檢測、現場檢查、線上監測和背景調查相結合的原則（楊茸，2017）。為保證審查順利開展，《網路產品和服務安全審查辦法（試行）》提出設立四個機構，一是國家網路安全審查委員會，由國家網路資訊辦公室會同有關部門成立，負責審議相關政策及協調重要問題；二是網路安全審查辦公室，主要負責安全審查的具體組織實施；三是網路安全審查專家委員會，主要對網路產品和服務的安全風險及其提供者的安全可信狀況進行綜合評估；四是第三方機構，由國家依法認定，具體承擔網路安全審查中的第三方評價工作（張莉，2017）。

值得注意的是國家網路安全審查委員會，2017 年 2 月 4 日，由國家網路資訊辦公室會同有關部門所成立的，負責審議網路安全審查的重要政策，統一組織網路安全審查工作，協調網路安全審查相關重要問題。網路安全審查委員會將聘請相關專家組成網路安全審查專家委員會，在第三方評價基礎上，對網路產品和服務的安全風險及其提供者的安全可信狀況進行綜合評估。另外，由國家統一認定網路安全審查第三方機構，將承擔網路安全審查中的第三方評價工作（李丹丹，2017）。

肆、網路安全審查制度的缺失探討

一、立法內容表述的不一致

中國大陸網路安全審查制度的首要缺失，就是立法內容表述的不一致，不同法律規範、文件對審查對象表述不統一，將給制度的實施帶來不確定性，從而影響實施效果，而完善網路安全審查制度的首要工作，就是要釐清這幾個不同表述的關係，這可以從以下兩個方面來談：

第一，就網路安全審查目標來看，根據上述，網路安全審查目標是「國家安全」，在根據上述網信辦公告的審查範圍的表述為：「關係國家安全和公共利益的系統使用的、重要資訊技術產品和服務，應通過網路安全審查。」由此可知，網信辦公告和法律體系三部法規對審查範圍的表述並不同，網信辦公告強調「國家安全和公共利益」，網路安全審查法律體系的三部法規刪掉「公共利益」，只強調「國家安全」。從字面上看，似乎對網路安全審查的對象範圍進行限縮，限制網路安全審查的作用發揮。本文以為，公共利益的涵義十分廣泛，凡涉及多數人的利益都可以被納入公共利益的範疇，這就在無形中將網路安全審查的適用範圍擴大，極容易造成該涵義（公共利益）與其他相似涵義（國家安全）的重疊。另外，網路安全審查法律體系的三部法規都只強調「國家安全」，進一步說明中國大陸網路安全審查制度是以「維護國家安全」為目標，且立法對「國家安全」的解釋，例如《國家安全法》第2條：「國家安全係指國家政權、主權、統一和領土完整、人民福祉、經濟社會可持續發展和國家其他重大利益相對處於沒有危險和不受內外威脅的狀態，以及保障持續安全狀態的能力。」（《中華人民共和國國家安全法》，2015）條文中的「人民福祉、社會可持續發展」均可以體現「公共利益」。所以，網路安全審查法律體系的三部法規對審查對象的範圍並沒有背離網信辦公告，而是強化網路安全審查制度的「國家安全」屬性，實質上是更有利於該制度的作用發揮的。

第二，就網路安全審查對象來看，表述並不一致，在《國家安全法》中被表述為「影響或者可能影響國家安全的網路資訊技術產品和服務」，在《網路安全法》中體現為「關鍵資訊基礎設施的運營者採購網路產品和服務，可能影響國家安全的，應當進行網路安全審查」，在《國家網路空間安全戰略》中表現為「對黨政機關、重點行業採購使用的重要網路產品和服務開展安全審查」，而《網路產品和服務安全審查辦法（試行）》將網路安全審查的對象表述為「關係國家安全的網路和資訊系統採購的重要網路產品和服務」，同時也專門規定「關鍵資訊基礎設施的運營者採購網路產品和服務，可能影響國家安全的，應當進行網路安全審查」。

由此可見，當前法律體系對審查對象的表述並不完全一致，在理解時會產生迷惑，例如「網路資訊技術產品和服務」（國家安全法）、「網路產品和服務」（網路安全法）及「重要網路產品和服務」（國家網路空間安全戰略和網路產品和服務安全審查辦法（試行））等，這三個概念的差別為何？本文認為，這三個概念僅是從不同觀點去表述而已，網路安全審查對象重點還是「關鍵資訊基礎設施」。另外，「關鍵資訊基礎設施」與「黨政機關、重點行業」是什麼關係？依中國大陸的現況，關鍵資訊基礎設施廣泛分布在黨政機關、重點行業，因此，應該將黨政機關、重點行業視為一個「行為主體」，由兩者負責運營和維護，兩者即是法律體系中所說的「關鍵資訊基礎設施的運營者」，否則在理解上會產生歧義，難以釐清兩者間關係。

二、立法內容的可操作性較差

《國家安全法》和《網路安全法》僅對網路安全審查作出原則性規定，並沒有設置能夠指導網路安全審查實施的具體內容，這是立法內容缺乏可操作性的典型表現。隨後，《網路

產品和服務安全審查辦法（試行）》作為以上法律的配套規則，該審查辦法細化其中的原則性規定，為網路安全審查提供具體的實施規則，但立法內容仍存在可操作性較差的問題，以下條文仍待改進：

第一，第 3 條指出要「堅持企業承諾與社會監督相結合的方式」進行網路安全審查，但後文並沒有體現「企業承諾」的內容，企業要如何進行承諾無從知曉。

第二，第 7 條涉及第三方審查機構的認定，指出「國家依法認定網路安全審查第三方機構」，但並沒有說明該依「何法」進行認定，條文中也沒有指導國家進行第三方機構認定的具體規則。

第三，第 11 條是第三方機構的行為規則，指出第三方機構應「按照國家有關規定，參照有關標準」進行網路安全審查，但該辦法同樣沒有說明審查標準是什麼。當前網路安全審查立法內容仍很不完善，需要進一步細化，以增強可操作性，否則將難以保證審查的透明性與公正性，將嚴重影響網路安全審查的實施效果。

第四，第 4 條（二）和第 11 條的供應鏈安全管理。第 4 條（二）「產品及關鍵部件生產、測試、交付、技術支援過程中的供應鏈安全風險」和第 11 條「承擔網路安全審查的第三方機構，應當堅持客觀、公正、公平的原則，按照國家有關規定，參照有關標準，重點從產品和服務及其供應鏈的安全性、可控性，安全機制和技術的透明性等方面進行評價，並對評價結果負責。」雖然這兩條分別提到要對供應鏈進行審查，但並沒有相對應的措施。本文認為，有必要對供應鏈的審查方式進行明確和細化，以支持此項審查有效開展，而實施供應鏈安全審查，意味著中國大陸網路安全審查不僅要對終端產品和服務進行技術審查，也要對隱藏在終端產品和服務背後的軟性安全風險進行審查。

三、審查標準不明確

當前的法律體系僅提到「審查標準」，卻並沒有規範「具體標準」，無法為審查活動提供有效依據，這容易造成主管機關的恣意和濫權。審查標準，是判斷網路產品與服務是否安全、可控的依據，是審查主體得出審查結果的根據，應當是網路安全審查制度中必備的因素，正如美國的資訊技術採購安全保障制度，各類安全標準構成了安全審查工作有效運行的基礎。缺乏審查標準的審查制度，對產品和服務的「提供者」以及審查主體而言，都無法提供明確的審查指引，因而無法稱之為「可期待規範」，只能淪為「政策工具」，中國大陸在提出建立網路安全審查制度之初就聲明，網路安全審查制度是防禦網路安全風險的主動保障措施，將對國內外提供者一視同仁，若缺失審查標準，那麼該制度的正當性和有效性都會存疑（馬寧，2016）。

在制定審查標準時，應將以下三點納入考慮範圍：一是對它的設計既要確保產品和服務安全性和可控性，不能過分干預到企業的商業機密，不能阻礙引進先進產品和服務的空間，達成協同「安全」和「發展」理念的具體體現；二是基於對審查效率與效果的考慮，制定審查標準時不可採取單一標準的做法，應當基於分級審查的規制，針對不同領域中不同安全等級的產品和服務設計有區別的審查標準，例如對涉密系統，應根據《國家保密法》的要求，

設計出較為嚴格的標準，尤其是對於關鍵資訊基礎設施中的資訊系統，應當體現出「重點保護」的要求等；三是審查標準是確保審查公正、無國別的依據，它顯示出對「技術」的尊重，體現公平性，即遵循「技術中立」原則。

四、審查集中於採購環節

《網路安全法》第 36 條：「關鍵資訊基礎設施的運營者採購網路產品和服務，應當按照規定與提供者簽訂安全保密協定，明確安全和保密義務與責任。」（《中華人民共和國國家安全法》，2015）《網路產品和服務安全審查辦法（試行）》（2017）第 2 條：「關係國家安全的網路和資訊系統採購的重要網路產品和服務，應當經過網路安全審查。」第 10 條：「公共通信和資訊服務、能源、交通、水利、金融、公共服務、電子政務等重要行業和領域，以及其他關鍵資訊基礎設施的運營者採購網路產品和服務，可能影響國家安全的，應當通過網路安全審查。產品和服務是否影響國家安全由關鍵資訊基礎設施保護工作部門確定。」

由此可知，無論是《網路安全法》第 36 條，還是《網路產品和服務安全審查辦法（試行）》第 2 條和第 10 條，都只強調在「採購」環節進行網路安全審查，並未提及在「使用」中實施網路安全審查，這是典型的「節點控制」模式。網路產品和服務並非完全安全可控，其中的安全風險是持續存在且無法被避免的，僅在採購時對其進行安全審查，雖然可以篩檢出一部分後門和漏洞，起到風險防禦的作用，但不可否認的是，網路產品和服務在使用過程中仍可能會給網路和資訊系統帶來不安全的風險，即採購環節的審查並不能保證網路產品和服務在後續使用過程中是絕對安全可控的，可見，「節點控制」的審查模式並未能很好地契合網路安全風險的特點，無法實現積極防禦，將嚴重限制網路安全審查的作用發揮。

因此，法律體系在網路安全審查集中均只突出「採購」環節，而沒有體現「使用」，為避免理解上產生偏差，降低實踐中的不確定性，進一步強化網路安全審查的作用發揮，本文認為，應完善網路安全審查的活動從「採購」環節擴展至「使用」。

五、缺少分級規則

中國大陸網路安全審查立法中缺少分級規則，應當建立分級規則。首先，在網路安全審查針對的風險中，有一類是關於資訊管理的安全風險，當這些「資訊」涉及「國家秘密」時，網路安全審查必須要符合《國家保密法》中的分級管理和保護要求，即將國家秘密分為「絕密」、「機密」和「秘密」三級，而對涉密系統也要進行分級保護，且要求嚴格，但當不涉及國家秘密時，網路安全審查就沒有了分級管理和保護的依據，這就在一個制度中形成兩套規則，容易造成混亂。其次，依據《網路安全法》，應當將關鍵資訊基礎設施作為網路安全審查的重點領域，然而當前立法內容並不能回答如何區分重點領域與普通領域、如何保證重點領域的審查效果等問題。最後，需要進行網路安全審查的網路產品和服務數量龐大，且不同的網路和資訊系統對不同的網路產品和服務的安全可控水準要求不同，若不對審查活動予以區分，平均分配審查資源，必然會影響審查的效率和品質。本文認為，缺少分級審查規則將影響網路安全審查的實施效果，應在中國大陸網路安全審查立法中填補這個空白。

六、審查結果的公布與通報

審查結果是網路安全審查的最終結論，關係到產品和服務提供者的利益，也關係到資訊系統的安全穩定性，應謹慎對待審查結果。《網路產品和服務安全審查辦法（試行）》第 8 條指出網路安全審查辦公室發布並在一定範圍內通報審查結果，本文認為，此條規定過於寬泛，應當進一步完善。首先，應當對「發布」和「通報」的情形分別作出規定，本文認為，對涉及國家秘密的審查結果可以採用「在一定範圍內通報」的形式，其他審查結果可採用發布的形式。其次，應對「一定範圍」作出進一步的解釋，另外，還應當改進公布與通報的方式與內容，本文認為，若產品和服務未能通過安全審查，除要將該結果進行公布或通報，還應告知提供者未通過審查的原因；若產品和服務通過安全審查，則應將該產品和服務置於「採購安全目錄」，同時詳細登記其各項審查內容的評價結果，從而避免重複審查，造成資源浪費。本文認為，通過以上方式完善審查結果的公布與通報環節，能夠體現審查工作的公正性和透明性，可有效避免網路安全審查成為阻攔外國產品和服務進入中國大陸市場的「政策性工具」。

伍、網路安全審查制度的改進之處

當前中國大陸網路安全審查立法尚不完備，當前仍以積極防禦原則為指導，進一步充實立法內容，針對網路安全風險無時不在的特點，以及數量龐大且情況複雜的現狀，為建立起更加完整和周密的網路安全審查制度。對此，應該建立動態審查模式，實現對安全風險的即時監測和應對。同時，建立分級審查規則，以提高審查資源的利用率，強化網路安全審查效果。最後，由第三方機構針對各項基礎資料進行評價，並在其基礎上，對網路產品和服務的安全風險及其提供者的安全可信狀況進行綜合評估。

一、動態審查模式

廣泛隱藏在網路產品和服務中的後門、漏洞無法被完全避免，使得網路安全風險呈現出「泛在化」[10] 的特點，由此，不得不默認任何網路產品和服務的引入與部署都存在風險，並且在現實中，通過審查活動實現絕對的風險排除是不可能實現的，即無論何種審查方式、無論審查措施多麼嚴密，始終都會存在「風險殘餘」問題，即使網路產品和服務在被使用前已

[10] 泛在化，意指使電腦融入人的生活空間，形成一個「無時不在、無處不在而又不可見」的計算環境。在這樣的環境中，計算不再局限於桌面，用戶可以通過手持設備、可穿戴設備或其他常規、非常規計算設備，無障礙地享用計算能力和資訊資源。所謂泛在（Ubiquitous）概念源於 20 世紀 90 年代，首先由美國加州 Xerox（施樂）公司 Palo Alto 研究中心首席科學家 Mark Weiser 博士在 1991 年提出。“Ubiquitous” 原為拉丁文，意思是神無所不在。它被用於形容網路無所不在是源於電腦技術的進展，電腦已全面融入人們的生活之中，無所不在地為人們提供各種服務。要推動 Ubiquitous Society，一般認為有三個普及任務，包括電腦的普及、連結網路的普及、服務享受的普及等。以泛在／適計算為背景的研究計畫是從 20 世紀 90 年代中後期廣泛開展的，絕大多數美國和歐洲的知名大學和研究所都啟動了相關的計畫，如美國的 MIT、CMU、Stanford、UC Berkeley；德國的 GMD、University of Karlsruhe；英國的 Cambridge、Lancaster 等都開展相關的研究。

經通過安全審查，但仍不能排除其在使用過程中的安全風險，這就要求必須以動態、即時的方式對安全風險進行感知並及時採取應對措施（馬民虎、馬寧，2016），惟有如此，才能減少網路安全風險的威脅。目前《網路安全法》和審查辦法對網路安全審查採用的均是「節點控制」模式，即在「採購」環節進行審查，而忽略使用階段的安全審查，但基於對網路安全風險「泛在化」的認識，本文認為，有效的網路安全審查應當覆蓋網路產品和服務的整個生命週期，體現動態的風險感知和應對，即「動態審查」模式，相較於「節點控制」，該模式防禦網路安全風險的有效性更高，其所帶來的效果將更加符合中國大陸推行網路安全審查的預期。本文認為，應對「節點控制」模式進行補強，將網路安全審查設置為「動態審查」模式，明確規定「在採購環節和使用過程中」實施網路安全審查，即將審查階段分為採購階段和使用階段兩個基本階段，在採購環節進行一次網路安全審查，在使用階段也要進行階段性安全審查，可以採用每年「定期檢查」、「專項檢查」和「抽查」等方式，實現持續性的動態風險監測和應對，強化網路安全防禦。

二、分級審查規則

中國大陸網路安全審查以「關係國家安全的網路和資訊系統中的重要網路產品和服務」為審查對象，這個範圍是十分廣泛的，然而，隨著國家建設、社會發展的資訊化程度越來越高，在現有基礎上會有更多的資訊系統被劃入這個範圍，面對如此龐大的審查範圍，國家是否有能力開展有效的安全審查成為疑問。同時，中央網路安全和資訊化領導小組關於加強資訊安全保障工作的意見指出要「優化資訊安全資源的配置，確保重點」，但是，在網路安全審查領域中，如何分配審查資源，如何開展重點領域的審查，如何保障重點領域的審查效果等等，都成為需要解決的具體問題。若要解決上述問題，實現資源的有效配置，提高效率，保障審查效果，建立分級審查的規則就變得十分重要。

網路分級審查規則的法律依據有三：一是《網路安全法》，該法實行網路安全等級保護制度與對關鍵資訊基礎設施進行重點保護的規定；二是《保守國家秘密法》及實施條例，該法對國家秘密及涉密系統的分級管理和保護要求；三是《資訊安全等級保護管理辦法（試行）》，[11] 該法根據損害的嚴重程度將中國大陸的資訊系統分為五個安全等級的規定，例如第 7 條：「資訊系統的安全保護等級分為以下五級：第一級，資訊系統受到破壞後，會對公民、法人和其他組織的合法權益造成損害，但不損害國家安全、社會秩序和公共利益。第二級，資訊系統受到破壞後，會對公民、法人和其他組織的合法權益產生嚴重損害，或者對社會秩序和公共利益造成損害，但不損害國家安全。第三級，資訊系統受到破壞後，會對社會秩序和公共利益造成嚴重損害，或者對國家安全造成損害。第四級，資訊系統受到破壞後，會對社會秩序和公共利益造成特別嚴重損害，或者對國家安全造成嚴重損害。第五級，資訊系統受到破壞後，會對國家安全造成特別嚴重損害。」

[11]《資訊安全等級保護管理辦法（試行）》由公安部、國家保密局、國家密碼管理局、國務院資訊化工作辦公室於 2006 年 1 月 17 日發布，2006 年 3 月 1 日實施。

不過，《網路產品和服務安全審查辦法（試行）》對分級標準的規定過於模糊，指導意義有限，但仍為建立網路分級審查的規則提供依據和參考，因此，中國大陸網路安全審查制度的下一步，應該根據現有資訊安全等級保護制度的框架和對涉密系統的分級管理要求，進一步細化分級標準，這可以參考美國聯邦資訊和資訊系統安全分類標準，按照保密性、完整性、可用性及其各自的影響度劃分資訊系統的安全類型，確定各系統的安全等級（馬寧，2016），並以此為基礎，制定與各等級相對應的審查標準和審查事項，從而形成井然有序的網路安全審查的對象範圍，確保資源的有效利用，實現重點領域重點保護和網路安全防禦效果的最大化。

三、第三方機構認定

根據當前立法內容，網路安全審查第三方機構是具體的評價機構，其為網路安全審查的最終結果提供各項基礎資料，在網路安全審查組織體系中占據重要地位，然而，對於這樣重要的審查主體，關於其資格認定，《網路產品和服務安全審查辦法（試行）》第 7 條中僅有原則性描述，即「國家依法認定網路安全審查第三方機構」，此條內容明顯缺乏可操作性，無法支援第三方機構認定工作有效開展。

在完善網路安全審查制度時，應當添加第三方機構的認定規則，至少應包含以下三個方面：一是什麼樣的機構能夠成為網路安全審查第三方機構的問題，即要明確規定第三方機構的資質，設置第三方機構的門檻，應指出其在信用、技術、人員構成、資金等方面所要具備的基本條件，這是認證規則的核心內容，直接關係網路安全審查的品質。二是如何進行認定的問題，即要明確規定認定程序，該部分應具備認定申請、資格審查、公布結果等環節，要突出認定過程的公平與公正，以選拔出品質過硬的網路安全審查評價機構為目標，這是確保網路安全審查公正性與透明性的前提基礎。三是如何管理第三方機構的問題，即要對第三方機構進行持續性管理，一方面要監督第三方機構嚴格依法進行網路安全審查具體評價工作，另一方面要督促第三方機構不斷升級審查技術，從而保障網路安全審查基礎評價品質。

陸、結論

自中國共產黨第十八屆中央委員會第四次全體會議以來，中國大陸網路空間法制化進程加快，《國家安全法》、《網路安全法》、《國家網路空間安全戰略》及《網路產品和服務安全審查辦法（試行）》相繼公布施行或發布。中國大陸實施網路安全審查制度是落實國家安全的重要舉措，將進一步規範和提升關係國家安全和公共利益的資訊系統使用的重要網路產品和服務的安全性、可控性，從而更好地維護和保障國家安全和公共利益。不過，中國大陸核心技術和關鍵設備依然處於追趕狀態，部分高端產品和核心部件仍然依賴國外，尤其是 2018 年 4 月所發生的「中興事件」，凸顯中國大陸在「核心技術」的自主性仍然不足。

當前，網路空間已經成為國家之間網路戰、情報戰的主戰場，尤其是網路攻防對抗日趨激烈，導致關鍵資訊基礎設施所面臨的網路安全威脅更加嚴峻複雜。網路產品和服務是構建

關鍵資訊基礎設施的基礎，其安全性、可控性直接影響關鍵資訊基礎設施的安全穩定運行，關係用戶利益，關係國家安全。縱觀全球，世界主要國家均將網路安全威脅視為國家安全和經濟社會發展面臨的嚴重挑戰，普遍針對資訊技術產品和提供者開展不同形式的安全審查，網路產品和服務安全審查已經成為國際慣例。例如，美國國家資訊安全保障採購政策等規定優先採購通過評估的產品，美國國防部針對資訊技術產品實施供應鏈安全審查等；英國要求國外通信設備供應商簽訂書面協定，進行專門的測試評估、人員審查等。國家的網路安全審查工作呈現審查範圍逐步擴大、審查內容不斷擴展、審查形式趨向豐富、審查層次上升至國家安全高度等特徵。

參考文獻

中央國家機關政府採購中心，〈關於進行信息類協定供貨強制節能產品補充招標的通知〉，2014 年 5 月 16 日，《中央政府採購網》，http://www.zycg.gov.cn/article/show/242846（瀏覽日期：2018 年 8 月 24 日）。

中國網信網，2016 年 12 月 27 日，〈《國家網路空間安全戰略》全文〉，《新華網》，http://www.xinhuanet.com/politics/2016-12/27/c_1120196479.htm（瀏覽日期，2018 年 8 月 24 日）。

《中華人民共和國國家安全法》，2015 年 7 月 1 日，http://www.xinhuanet.com/legal/2015-07/01/c_1115787801.htm（瀏覽日期，2018 年 8 月 24 日）。

《中華人民共和國網絡安全法》，2016 年 11 月 7 日，http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm（瀏覽日期，2018 年 8 月 24 日）。

史竟男、白陽、張洋、鄭會燕，2014 年 5 月 23 日，〈網絡安全審查乃順勢而為〉，《人民日報》，版 4。

左曉棟，2015，〈以務實態度對待網絡安全審查制度〉，《中國信息安全》，2015（5），頁 88-89。doi:10.3969/j.issn.1674-7844.2015.05.050

李丹丹，2017 年 2 月 4 日，〈中國將成立網路安全審查委員會　由第三方機構評估〉，《網易新聞》，http://news.163.com/17/0204/13/CCEFM1EA000187VE.html（瀏覽日期：2018 年 8 月 24 日）。

李營輝，2016，《我國關鍵信息基礎設施立法保護研究》，北京交通大學法學院碩士論文。

汪莉絹，2018 年 5 月 30 日，〈陸強化網絡監控，兩大網站用黨精神自律〉，《聯合報》，版 8。

風傳媒國際中心，2018 年 4 月 22 日，〈「中興事件」震撼中國　習近平宣示：核心技術是國之重器，加速推動突破〉，《風傳媒》，http://www.storm.mg/article/427926（瀏覽日期：2018 年 8 月 24 日）。

高少華、葉健，2014 年 4 月 20 日，〈網絡經濟規模逾 6,000 億　互聯網思維改變經濟格局〉，《新浪財經》，http://finance.sina.com.cn/chanjing/cyxw/20140420/155418857057.shtml（瀏覽日期：2018 年 8 月 24 日）。

馬民虎，2007，〈信息安全法律體系：靈魂與重心〉，《信息網絡安全》，2007（1），頁 13-15。doi:10.3969/j.issn.1671-1122.2007.01.007

馬民虎、馬寧，2014，〈IT 供應鏈安全：國家安全審查的範圍和中國大陸應對〉，《蘇州大學學報（哲學社會科學版）》，35（1），頁 90-95。

馬民虎、馬寧，2016，〈威脅態勢感知視域下國家網絡安全審查法律制度的塑造〉，《西安交通大學學報（社會科學版）》，35（2），頁 65-72。doi:10.15896/j.xjtuskxb.201602010

馬寧，2016，〈國家網絡安全審查制度的保障功能及其實現路徑〉，《環球法律評論》，38（5），頁 134-150。doi:10.3969/j.issn.1009-6728.2016.05.009

倪光南，2018，〈自主可控是保障網絡安全的一個必要條件〉，《信息安全研究》，4（1），頁 6-7。

海彥，2016 年 8 月 14 日，〈全球數十商業團體促中國修改《網路安全法》〉，《美國之音》，https://www.voachinese.com/a/global-g20-20160814/3463595.html（瀏覽日期：2018 年 8 月 24 日）。

張莉，2017，〈《網絡產品和服務安全審查辦法（試行）》為網絡安全構築銅牆鐵壁〉，《保密工作》，2017（11），頁 51。

張棉棉，2014 年 5 月 22 日，〈中國將推出網絡安全審查制度　外企入華門檻或提高〉，《網易新聞》，http://news.163.com/14/0522/19/9SSFSPSF00014JB5.html（瀏覽日期：2018 年 8 月 24 日）。

陳曉莉，2018 年 4 月 16 日，〈微博依《網絡安全法》大力整頓，掃盪同性戀內容引發反彈，急踩煞車〉，《iThome》，https://www.ithome.com.tw/news/122465（瀏覽日期：2018 年 8 月 24 日）。

陳興躍，2017 年 11 月 16 日，〈凝聚各方力量，維護網絡安全〉，《光明網》，http://theory.gmw.cn/2017-11/16/content_26810348.htm（瀏覽日期：2018 年 8 月 24 日）。

傅卓異、王軼駿、薛質，2013，〈Windows 8 安全改進及缺陷研究〉，《信息安全與通信保密》，239，頁 75-79。doi:10.3969/j.issn.1009-8054.2013.11.012

馮琳，2015，《IT 供應鏈與國家安全法律問題研究》，西南交通大學公共管理與政法學院碩士論文。

楊光，2014，〈我國將出臺網絡安全審查制度〉，《計算機與網絡》，40（10），頁 6。doi:10.3969/j.issn.1006-3366.2014.06.044

楊茸，2017，〈網絡安全審查委員會將成立〉，《計算機與網絡》，43（4），頁 14。doi:10.3969/j.issn.1008-1739.2017.04.013

新華社，〈中共中央印發「深化黨和國家機構改革方案」〉，2018 年 3 月 21 日，《人民網》，http://politics.people.com.cn/n1/2018/0321/c1001-29881261.html（瀏覽日期：2018 年 8 月 24 日）。

董樂，2014 年 5 月 20 日，〈中國下令政府機關電腦禁用視窗 8〉，《BBC 中文網》，http://www.bbc.com/zhongwen/trad/science/2014/05/140520_china_windows_8（瀏覽日期：2018 年 8 月 24 日）。

趙勇，2014，〈經濟學視角下的網路安全審查制度〉，《中國資訊安全》，2014（8），頁 74-77。

《網路產品和服務安全審查辦法（試行）》，2017 年 5 月 2 日，http://www.cac.gov.cn/2017-05/02/c_1120904567.htm（瀏覽日期，2018 年 8 月 24 日）。

劉彥華，2017，〈2017 中國平安小康指數：82.3「第五疆域」急需安全屏障〉，《小康》，2017（19），頁 48-53。doi:10.3969/j.issn.1672-4879.2017.07.017

劉思琦編，2017 年 5 月 14 日，〈聚焦一帶一路〉，《每經網》，http://www.nbd.com.cn/articles/2017-05-14/1105353.html（瀏覽日期，2018 年 8 月 24 日）。

劉雪玉，2014 年 5 月 23 日，〈我國將出臺網絡安全審查制度，與禁裝 Win8 無關〉，《京華時報》，http://tech.163.com/14/0523/03/9ST9VSVG000915BF.html（瀏覽日期：2018 年 8 月 24 日）。

鄺承華，2002，〈寒蟬效應〉，《新聞評議》，334（11），頁 3。