

我國資通安全戰略及體系評估 —兼論資通安全管理法草案

張書瑋

政治大學國家發展研究所博士生

摘 要

現今許多專家及專業機構均將非傳統安全中的網路安全、資安風險所衍生之威脅視為全球各國所面臨最重大全球風險之一，從網路安全漏洞、智慧財產權剽竊、個資竊取、網路犯罪、個人國家間的網路攻擊及駭客中繼站竊取資料等各種資安問題已日益嚴重且棘手難以解決。網路威脅的攻擊對象，已不斷擴及到世界各國，包括地方、區域和國家層級的政府機關、私人企業及跨國企業及個人領域，而其威脅的層面亦遍布各種生活型態。本文首先檢視資安總體趨勢及各國網路安全政策；再次說明我國資通安全戰略及體系，以瞭解我國資安體系運作情況；另就資通安全管理法草案提出評估；最終提出建議事項供參研之用。

關鍵詞：非傳統安全、網路安全、資安風險、資通安全管理法草案

An Evaluation on Information and Communication Security Strategy and System in Taiwan: Focus on the Draft of the Information Communication Security Management Act

Shu-Wei Chang

Doctoral Student
Graduate Institute of Development Studies
National Chengchi University

abstract

Today, many experts and professional organizations assess the threat of cybersecurity and rank information security risk as one of the most significant global risks. From the network security loopholes, plagiarism of intellectual property rights, personal information theft, cybercrime, cyber attacks between individual and countries, and theft of information by command and control servers have become increasingly serious and difficult to solve. The target of cyber attacks has been spread worldwide, including government agencies, private enterprises, multinational corporations, and individuals. The threat level also spreads across various life forms. This article firstly examines the overall trend of cybersecurity and national cybersecurity policies; secondly, this article will explain our country's information and communication security strategy and system to understand the operation of our country's information and communication system; thirdly, an evaluation on draft cybersecurity management law will be elaborated; finally, the recommendations for the policymaker will be deduced according to the previous works.

Keywords : Non-traditional security, Cybersecurity, Information security risk, the Draft of the Information Communication Security Management Act

壹、前言

現今許多專家、專業機構評估非傳統安全中的網路安全、資安風險所衍生之威脅視為今日全球各國所面臨最重大全球風險之一，從網路安全漏洞、智慧財產權剽竊、個資竊取、網路犯罪、個人國家間的網路攻擊及駭客中繼站竊取資料等各種資安問題已日益嚴重且棘手難以解決。網路威脅的攻擊對象，已不斷擴及到世界各國，包括地方、區域和國家層級的政府機關、私人企業及跨國企業及個人領域，而其威脅的層面亦遍布各種生活型態。當世界各國日益重視網路等非實體領域的趨勢下，造成現今網路威脅層次日益擴大，各國亦將資安視為國安，而政府與民間如何合作，共同維護網路安全，亦是亟待解決問題。

2016 年 12 月 1 日總統蔡英文出席「第十二屆臺灣駭客年會 HITCON Pacific 2016」會議中，說明政府強化資安管理制度的努力與決心，並期盼在資安領域裡，政府能與駭客社群保持對話，相互交流，為整個政府體系帶來跳脫傳統、挑戰現況的新氣象。並提及民進黨執政半年以來，積極將「資安就是國安」的觀念帶入政府的組織文化，同時行政院也在 2016 年 8 月成立「資通安全處」，並推動臺灣第一部資通安全管理法，將針對政府機關及部分民間企業，提出明確的資安規範。同時，行政部門也有了共識，要建構關鍵基礎設施和民間產業的資安防護體系，以確保公共服務的運作及商業活動不受外來侵擾；¹2017 年 9 月 27 日總統蔡英文接見「2017 年駭客大賽世界盃 DEF CON CTF」競賽選手，對於「HITCON 戰隊」獲得全球第二名的佳績甚表肯定，並重申「資安就是國安」，政府會投入資源來提升本土關鍵資安技術。另表示 2017 年 6 月國

¹ 總統府，〈資安就是國安 政府將不斷投入資源 提升本土關鍵資安技術〉，《總統府》，2016 年 12 月 1 日，<<http://www.president.gov.tw/NEWS/20926>>（2017 年 12 月 3 日查詢）。

軍就成立資通電軍指揮部，她請同樣來自民間的高手，國安會諮詢委員李德財及行政院政務委員唐鳳秉持跳脫科層的透明精神，連結政府和民間的力量一同發展資安。此外提及經濟部和教育部分也要持續在人才培育上與時俱進，才能跟上資通安全產業一日千里的快速變化。²另 2017 年 4 月 27 日行政院會通過行政院資通安全處擬具的資通安全管理法草案，將送請立法院審議，會議中前行政院長林全表示，資通安全在維護國家安全和公共利益上是非常重要和需要面對的課題，請行政院資通安全處積極與立法院朝野各黨團溝通協調，早日完成立法程序。³

上述全球資安趨勢及臺灣重要領導人均表示資安議題非常重要，為解決資安問題，政府在戰略面、組織面及法制面做出不少變革，因此本文首先檢視資安總體趨勢及各國網路安全政策；再次說明我國資通安全戰略及體系，以瞭解我國資安體系運作情況；另就資通安全管理法草案提出評估；最終提出建議事項供參研之用。

貳、資安總體趨勢

世界經濟論壇（World Economic Forum）《2017 年全球風險報告》（The Global Risks Report 2017）中提到，現今企業組織面臨最大的風險第一名是環境風險，像全球暖化的議題，其次是社會經濟風險，第三才是科技風險。科技風險在 2008 年以前根本不在前 10 名，但從 2014 年開始則急遽攀升，今年已成為前三大風險之一。其中網路攻擊、資料詐騙與關鍵基礎設

² 彭煒琳，〈資安就是國安 蔡英文允諾投資資源發展產業〉，《中時電子報》，2017 年 9 月 29 日，<<http://www.chinatimes.com/realtimenews/20170929003178-260407>>（2017 年 12 月 3 日查詢）。

³ 行政院新聞傳播處，〈行政院會通過「資通安全管理法」草案〉，《行政院》，2017 年 4 月 27 日，<http://www.ey.gov.tw/News_Content.aspx?n=F8BAEBE9491FC830&s=26B446DFB5C87E70>（2017 年 12 月 3 日查詢）。

施保護這三項就佔科技風險的 80%。⁴ 另一份由英國營運持續協會（Business Continuity Institute）與英國標準協會（Business Standard Institute）所發表的 2017 年地平線掃描報告（Horizon Scan Report 2017）也同樣指出，網路攻擊、資料外洩與無預警資訊與通訊中斷為企業所面臨的前三大威脅，由此看出當前面臨資安攻擊風險所在。⁵ 以下檢視聯合國及區域組織、資安公司所發佈資安趨勢報告以檢視資安總體趨勢概況：

一、聯合國及區域組織

在資安總體趨勢評估層次上，2017 年 7 月 5 日聯合國國際電信聯盟（U.N. International Telecommunication Union, ITU）發表 2017 年全球網路安全指數（Global Cybersecurity Index, GCI），評估數據中新加坡各方面都表現傑出優良，ITU 表示國家的財富會滋生網路犯罪，但是網路安全不會同時生成，而是需要政府帶領、培養公私部門在網路安全的能力、進行適當的計劃和部署，國家網路安全最初的第 1 步，就是要有國家安全戰略，但是據 ITU 調查，還有 5 成的國家沒有相關準備。⁶ GCI 是以法律措施、技術措施、組織措施、能力建設

⁴ World Economic Forum, “The Global Risks Report 2017 12th Edition,” *World Economic Forum Website*, January 2017, < http://www3.weforum.org/docs/GRR17_Report_web.pdf > (2017 年 12 月 3 日查詢)；羅正漢，〈從世界經濟論壇 2017 風險報告書，看企業與政府的資安防禦重點〉，《iThome》，2017 年 3 月 17 日，<<https://www.ithome.com.tw/newstream/112847>> (2017 年 12 月 3 日查詢)。

⁵ Business Continuity Institute, “Horizon Scan Report 2017,” *BSI Website*, February 2017, <<https://www.bsigroup.com/en-ZA/ISO-22301-Business-Continuity/Business-Continuity---Horizon-Scan-Report-2017/>> (2017 年 12 月 3 日查詢)；黃彥棻，〈企業營運十大威脅出爐，前三大都得靠 IT〉，《iThome 網站》，2017 年 5 月 25 日，<<https://www.ithome.com.tw/news/114440>> (2017 年 12 月 3 日查詢)。

⁶ Tom Miles, “U.N. survey finds cybersecurity gaps everywhere except Singapore,” *Reuter Website*, July 5, 2017, <<https://www.reuters.com/article/us-cyber-un/u-n-survey-finds-cybersecurity-gaps-everywhere-except->

和合作 5 大方向來衡量各國的網路安全狀況。調查以線上問卷形式實施，內容包括「是否有網路安全相關法規」、「法規規範的網路行為和內容」、「政府是否有成立各類型網路安全處理小組」、「是否有負責網路安全的政府部門或組織」、「國內是否存在網路安全產業」、「是否存在網路安全相關合作措施」、以及「是否有兒童網路安全保護措施」等。整體評估下，新加坡的評分最高，而過去時常居首的美國則排名第 2，前 10 名的國家有許多開發中或小型的經濟體，包括馬來西亞、阿曼、愛沙尼亞、毛里求斯、澳大利亞、格魯吉亞、法國和加拿大，中國則在 134 國中排在第 34 位。⁷

在區域組織資安層次評估上，2016 年 7 月 8 日北約秘書長 Jens Stoltenberg 特別在國防新聞（Defense News）投書強調北約隨時都在對付來犯的網路攻擊。他表示兩年前網路攻擊曾經癱瘓過北約網站，而最近有一連串的網路攻擊是對德國的國家電腦系統進行入侵，試圖控制發動場等基礎設施。⁸此外，網路攻擊的發起者可能是國家授意或是獨立組織，以實現自己的外交與軍事目的。這些網路攻擊會對社會造成危害，以及軍事行動的困難。因此，北約會確保自身的網路安全與盟友的網路防護機制，並且透過交流、訓練，和持續的投資，以確保真正的網路安全。在華沙舉行的北約高峰會已經確定網路安全是

singapore-idUSKBN19Q19L>（2017 年 12 月 3 日查詢）。

⁷ 黃有容，〈聯合國網路安全調查：新加坡資安第一、小型經濟體不俗〉，《匯流新聞網》，2017 年 7 月 8 日，<<https://cnews.com.tw/%E8%81%AF%E5%90%88%E5%9C%8B%E7%B6%B2%E8%B7%AF%E5%AE%89%E5%85%A8%E8%AA%BF%E6%9F%A5%EF%BC%9A%E6%96%B0%E5%8A%A0%E5%9D%A1%E8%B3%87%E5%AE%89%E7%AC%AC%E4%B8%80%E3%80%81%E5%B0%8F%E5%9E%8B%E7%B6%93%E6%BF%9F/>>（2017 年 12 月 3 日查詢）。

⁸ Jens Stoltenberg, “NATO and Cyber: Time to Raise our Game,” *Defense NEWS Website*, July 8, 2016, <<https://www.defensenews.com/smr/road-to-warsaw/2016/07/08/nato-and-cyber-time-to-raise-our-game/>>（2017 年 12 月 3 日查詢）。

北約防務的優先選項，並會擴及到歐盟這類的友好同伴。而北約投入網路戰爭，是為了建立安全透明的網路空間，也是確保自由、民主、人權、法治等共同價值觀；⁹ 具體實踐上，2017 年 5 月 31 日北約官員在愛沙尼亞塔林舉辦的第 9 屆「國際網路衝突會議」上，表示網路攻擊對國家安全的威脅日增，北約正積極強化制止網攻能力，在面臨針對重要軍事設施與民間基礎建設的網攻時，也可援引北約憲章第 5 條規定，實施集體防禦。¹⁰

另 2016 年 2 月 9 日歐盟統計局（Eurostat）公布的網路安全報告指出，2015 年一年中，25% 的歐盟民眾曾經出現電腦病毒感染、個人資料遭駭、財務損失或兒童登錄不當網站等網路安全問題。也因為對網路安全有疑慮，約 19% 的歐洲人不願在網路購物，18% 民眾拒絕使用網路銀行，13% 民眾除了家裡外，會避免在其他地方使用手機上網或是利用其他無線網路。對網路使用最感安心的國家是捷克，只有 10% 的民眾曾經碰過網路安全問題，其次為荷蘭的 11%、斯洛伐克為 13%、愛爾蘭為 14%；排名最後一名的國家是克羅埃西亞，曾經碰過網路安全問題的比率達到 42%，其次為匈牙利的 39%、葡萄牙有 36%、馬爾他 34%，許多國人喜愛的法國也有 33%。¹¹

二、資安公司發佈資安趨勢報告

2017 年 9 月 12 日資安廠商趨勢科技發表《2016 年資訊安全總評：企業威脅刷新紀錄的一年》報告，此報告重點如下：第一勒索病毒大幅成長，過去一年來，勒索病毒家族數量

⁹ 江飛宇，〈北約秘書長強調 網路戰爭的重要性〉，《中時電子報》，2016 年 7 月 10 日，〈<http://www.chinatimes.com/realtimenews/20160710003894-260417>>（2017 年 12 月 3 日查詢）。

¹⁰ 崔敬熙，〈反制網攻 北約擬集體防禦〉，《青年日報》，2017 年 6 月 2 日，〈<http://www.ydn.com.tw/News/238946>>（2017 年 12 月 3 日查詢）。

¹¹ 〈歐盟：1/4 歐洲人曾有網路安全問題〉，《科技新報》，2016 年 2 月 9 日，〈<https://technews.tw/2016/02/09/eurozone-internet-safety/>>（2017 年 12 月 3 日查詢）。

從原本的 29 個增加到 247 個。主要原因之一是勒索病毒的獲利率高。儘管個人或企業都已被建議最好不要支付贖金，還是有許多人屈服於勒索病毒，總損失金額高達十億美金（約新臺幣 300 億元）；第二變臉詐騙日益猖獗，事實證明，變臉詐騙就像勒索病毒一樣能為網路犯罪集團帶來龐大獲利，全球企業平均案例損失金額高達 14 萬美元。此外，這類詐騙也突顯出歹徒誘騙企業上當的社交工程技巧十分有效；第三軟體漏洞層出不窮，趨勢科技和 Zero Day Initiative（ZDI）所發掘的漏洞數量在 2016 年創下新高，其中發現最多的是 Adobe Acrobat Reader DC 的漏洞，為企業用監控與資料擷取（SCADA）系統常用的軟體；第四 Angler 漏洞攻擊套件正式出局，就在 50 名網路犯罪分子遭到逮捕之後，曾經稱霸一時的 Angler 漏洞攻擊套件便逐漸退出江湖，最後銷聲匿跡。雖然沒過多久就有新的漏洞攻擊套件冒出來取代 Angler 的地位，但截至 2016 年底，收錄至漏洞攻擊套件的軟體漏洞數量還是減少了 71%；第五銀行木馬程式和 ATM 惡意程式，網路犯罪集團一直都會利用 ATM 惡意程式、盜拷磁條以及銀行木馬程式來從事犯罪。但近年來隨著犯罪的多元化，歹徒現在也取得了受害者的個人身分資訊和帳號密碼，並藉此入侵企業網路；第六 Mirai 殭屍病毒發動大規模攻擊，2016 年 10 月，有眾多安全防護脆弱的物聯網（IoT）裝置遭到駭客入侵並用於發動分散式阻斷服務（DDoS）攻擊，前後約有 10 萬臺 IoT 裝置遭到入侵，並且導致 Twitter、Reddit、Spotify 等知名網站斷線數個小時；第七 Yahoo 發生史上最大宗資料外洩，2013 年 8 月 Yahoo 發生了有史以來最大的一宗資料外洩，高達 10 億個帳號的使用者資料遭到外洩。然而該事件卻直到 2016 年 9 月該公司又再發生另一起資料外洩才連帶曝光，這一次又有 5 億個帳號受害。兩起案例再度掀起有關廠商資訊揭露義務以及客戶資料安全責任的

討論。¹²

而 2017 年 9 月 12 日資安廠商趨勢科技另總結 2017 上半年資安趨勢發表「2017 上半年資安總評：駭客入侵的代價」研究報告，指出 2017 上半年企業依然不斷遭遇營運中斷與資安上的挑戰，面臨日益增加的勒索病毒、變臉詐騙（Business Email Compromise, BEC）以及物聯網（Internet of Things, IoT）相關攻擊。除此之外，一種新的威脅「網路宣傳」（Cyber Propaganda）對企業商譽的影響力也不容小覷。2017 年 5 月和 6 月分別爆發了 WannaCry 和 Petya 勒索病毒，據估計該攻擊在全球所造成的損失，包括生產力損失及災害控制成本，共計高達 40 億美元。而根據美國聯邦調查局的資料，2017 上半年變臉詐騙所造成的全球損失也高達 53 億美元。截至 2017 上半年為止，趨勢科技共偵測到近 8,300 萬個勒索病毒威脅，以及 3,000 次變臉詐騙嘗試攻擊，另 2017 年 1 月至 6 月物聯網攻擊數量不斷攀升，網路宣傳活動也持續擴散。根據趨勢科技和資安廠商 Politecnico di Milano（POLIMI）合作的研究顯示，工業機器人同樣也可能遭駭客入侵，並且帶來嚴重的財務與生產力損失，智慧工廠¹³千萬不能輕忽這類連網裝置的安全性。¹⁴

2017 年 8 月 7 日卡巴斯基實驗室發佈最新 DDoS 趨勢報告，此報告指出 2017 年第二季有 86 個國家遭受分散式阻斷服務攻擊（distributed denial-of-service attack, DDoS）。DDoS 攻

¹² 〈2016 年資訊安全總評：企業威脅刷新紀錄的一年〉，《趨勢科技》，2017 年 3 月 7 日，<http://www.trendmicro.tw/cloud-content/tw/pdfs/security-intelligence/reports/trendlabs_2016_annual_information_security_review.pdf>（2017 年 12 月 3 日查詢）。

¹³ 智慧工廠是推動工業 4.0 的重要引擎，藉由物聯網、機器人、大數據、人工智慧等技術，不僅可藉此提高生產力與製造效率，更同時也成為驅動全球經濟的一股力量。

¹⁴ 〈今年上半年資安報告 勒索病毒等三大攻擊續增〉，《蘋果日報》，2017 年 9 月 12 日，<<http://www.appledaily.com.tw/realtime/news/article/new/20170912/1202118/>>（2017 年 12 月 3 日查詢）。

擊，比第一季增加了 14 個受害國家，而且約半數（47.42%）攻擊目標特別鎖定中國，其次是韓國、美國，而攻擊來源國家也是相同名次。另外今季發生的 DDoS 攻擊，時間最長達 277 個小時，比上一季 120 小時增加了 157 個小時，也破了 DDoS 攻擊時間的最長紀錄。另報告指出勒索 DDoS 攻擊還分成兩種，一是攻擊者同時發動 DDoS 攻擊和發送勒索信，以恐嚇受害公司，若未支付贖金，攻擊者確實有能力發動下一波 DDoS 攻擊，另一種情況，攻擊者向受害公司發送勒索信，雖然多半只是威脅而不會實際發動攻擊，但目的是為了吸引其他攻擊者執行進一步攻擊。2017 年 6 月駭客集團 Armada Collective 針對韓國 7 家銀行發動勒索 DDoS 攻擊，威脅 7 家銀行需支付贖金 31 萬美元才願意停止攻擊，而 Armada Collective 也是攻擊臺灣證券商的駭客組織。不只勒索 DDoS 攻擊，研究人員也強調，DDoS 越來越常被利用作為政治鬥爭工具。卡巴斯基實驗室也指出今（2017）年 5 月半島電視臺與國營新聞通訊社的網站遭 DDoS 攻擊，雖然無法得知攻擊來源，以及實際攻擊目的，但明顯造成卡達與周邊阿拉伯國家的外交關係緊張。¹⁵

參、美、日、歐盟網路安全政策

一、美國

近年來，特別是在歐巴馬總統任期內，網路空間成為美國政府最重要的政策議程，2009 年 2 月，歐巴馬政府公佈了《網路空間政策評估—保障可信和強健的資訊和通信基礎設施》報告，報告中提到對於網路空間政策所提出的問題，包含了現階段環境因素與未來面臨問題的應對做法，包含以下四點：1、網路安全委員會曾在 2008 年 12 月對第 44 屆總統提出一份報告指出，目前新政府面臨到最緊迫的國家安全問題是未能夠有

¹⁵ 黃泓瑜，〈卡巴斯基實驗室最新 DDoS 趨勢報告：勒索型 DDoS 攻擊越來越盛行〉，《iThome》，2017 年 8 月 7 日，<<https://www.ithome.com.tw/news/116107>>（2017 年 12 月 3 日查詢）。

效保護網路空間。2、聯邦部門和各機構之間對於網路安全負有重大責任，但是常有造成機構職權重疊情況，或因為決定權不足情形造成未能有效行動處理問題。3、政府應制定新的政策，確定事件處理流程，加強人員的要求以及技術的精進，來達到降低網路安全的風險。4、網路安全問題亦需要公共部門與私營部門齊力合作，形成夥伴關係，還有在國際間進行合作與規範。¹⁶ 綜觀此報告將網路空間安全威脅定位為舉國面臨的最嚴重的國家經濟和國家安全挑戰之一，並宣佈關鍵基礎設施將被視為國家戰略資產，保護這一基礎設施將成為國家安全的優先事項，全面規劃保衛網路空間的戰略措施。

2011年5月，美國白宮發佈了美國《網路空間國際戰略》(International Strategy for Cyberspace)，其戰略意圖明顯，指出美國將與國際社會合作，促進開放、互通、安全和可靠的資訊與通訊基礎設施，支援國際貿易與商務，加強國際安全，促進自由表達和創新；¹⁷ 同年7月，美國國防部發佈《網路空間行動戰略》，提出5大戰略措施，用於捍衛美國在網路空間的利益，使得美國及其盟國和國際合作夥伴可以繼續從資訊時代的創新中獲益，根據美國國防部公開之文件內容所提及之戰略五大措施包含：1、將網路空間視為一作戰領域，對美軍進行組織、訓練和武裝，進而獲得網路空間的全面性優勢。2、導入新型防衛作戰概念以維護國防部之網路和系統。3、加強國防部與國土安全部及其他公、私部門之間的合作，確保政府整體的網路安全。4、建立美國與其盟友在網路空間領域的國際合作。5、

¹⁶ The White House, "Cyber Space Policy Review 2009," *Department of Homeland Security Website*, March 2009, <https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf> (2017年12月3日查詢)。

¹⁷ The White House, "International Strategy for Cyberspace," *The White House Website*, May 2011, <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> (2017年12月3日查詢)。

重視高科技人才培育並提升技術創新能力。¹⁸

2013 年 2 月，歐巴馬發佈第 13636 號行政命令《增強關鍵基礎設施網路安全》，明確指出該政策作用為提升國家關鍵基礎設施並維護環境安全與恢復能力；¹⁹2014 年美國通過《聯邦資訊安全現代化法》（Federal Information Security Modernization Act of 2014, FISMA 2014），2014 年修正的《聯邦資訊安全現代化法》納入美國國土安全部為管理角色之一，並要求對資安事件進行通報，相關修正之重點包括第一賦予國土安全部長監督管理之權責²⁰；第二增加資安事件通報之要求與相關規定及第三調整各機關提出年度報告之內容。²¹2015 年以來，歐巴馬政府逐步從「稜鏡門事件」²²影響中走出，美國

¹⁸ US Department of Defense, “Department of Defense Strategy for Operating in Cyberspace,” *Department of Homeland Security Website*, July 2011, <<https://www.hsdn.org/?view&did=489296>> (2017 年 12 月 3 日查詢)。

¹⁹ The White House, “Executive Order 13636: Improving Critical Infrastructure Cybersecurity,” *The White House Website*, February 2013, <<https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>> (2017 年 12 月 3 日查詢)。

²⁰ FISMA 2002 原本所授權之管理角色為美國管理及預算局（Office of Management and Budget, OMB）局長，其監督聯邦各機關之資安政策與其實施。而 FISMA 2014 則新增授權美國國土安全部部長，使其協助預算局局長共同進行各機關之監督管理。

²¹ 蘇柏毓，〈資訊安全法規國際最新發展舉隅〉，《科技法律透析》，第 27 卷第 6 期（2015 年 6 月），頁 28-29。

²² 「稜鏡門事件」指的是一項由美國國家安全局自 2007 年開始實施的絕密級電子監聽計劃。該計劃的正式名稱為「US-984XN」，媒體稱稜鏡計劃（英語名稱 PRISM）。根據報導，泄露的文件中描述 PRISM 計劃能夠對即時通信和既存資料進行深度的監聽。許可的監聽對象包括任何在美國以外地區使用參與計劃公司服務的客戶，或是任何與國外人士通信的美國公民。國家安全局在 PRISM 計劃中可以獲得的數據電子郵件、視訊和語音交談、影片、照片、交談內容、檔案傳輸、登入通知，以及社交網路細節。綜合情報文件《總統每日簡報》中在 2012 年內在 1,477 個計劃使用了來自稜鏡計劃的資料。關於 PRISM 的報道，是在美國政府持續秘密要求威訊向國家安全局提供所有客戶每日電話記錄的消息曝光後

白宮發佈《美國 2015 年國家安全戰略》，提出美國在國際秩序中的領導角色以及對應的領導力模型，該戰略針對網路空間安全明確提出：美國是互聯網的發源地，有責任領導網路世界，除了保障美國本國關鍵基礎設施和對抗網路攻擊，還包括參與協助其他國家基礎設施保障法律以及國際行為準則的制定。²³

而在歐巴馬執政後期，2016 年 2 月 9 日歐巴馬宣布一項預算高達 190 億美元的全國性資安計畫，此為《國家資安行動計畫》（Cybersecurity National Action Plan），用以強化政府以及私部門的資安能力。《國家資安行動計畫》包括建立聯邦政府的資安協調機制、全面檢修過時的電腦系統、簡化聯邦網絡並提升效率、認證聯網設備、投資資安研究、培育資安人才，還將聘雇一位資訊安全長（Chief Information Security Officer, CISO），並設立「強化國家資安委員會」負責這項計畫。²⁴ 而川普執政後，於 2017 年 5 月 11 日簽署一項網路安全行政命令，期望能藉此改善美國的網路安全現況。該行政命令列出了美國網路安全領域的三個優先事項：保護聯邦網路、關鍵基礎設施網路和美國大眾網路使用。²⁵ 從上述美國資安法制得知，

不久出現的。洩露這些絕密文件的是國家安全局合約外包商員工愛德華·斯諾登，於 2013 年 6 月 6 日在英國《衛報》和美國《華盛頓郵報》公開。

²³ The White House, "Fact Sheet: The 2015 National Security Strategy," *The White House Website*, February 2015, <https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf> (2017 年 12 月 3 日查詢)。

²⁴ 呂紹玉，〈視駭客為國家威脅！歐巴馬宣布 190 億美元的資安計畫〉，《科技新報》，2016 年 2 月 16 日，<<https://technews.tw/2016/02/12/obama-unveils-19-billion-cybersecurity-plan/>> (2017 年 12 月 3 日查詢)。

²⁵ The White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," *The White House Website*, May 11, 2017, <<https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>> (2017 年 12 月 3 日查詢)；〈川普簽署網路安全行政命令則〉，《行政院國家資通安全會報技術服務中心》，2017 年 5 月 17 日，<<https://www.nccst.nat.gov.tw/>>

美國從戰略面、組織面、通報機制、人才及資源均不斷在網安領域充實更新，並參與國際建置在網安領域處於領導協調地位。

二、日本

日本是傳統的資訊大國，早在 1999 年就開始研議網安政策，但其在具體作為措施上卻是相對落後。由於日本的法規傾向較為保守，加上資訊化的程度相當高，便成為與資訊犯罪的溫床。根據日本政府資料，2013 年內部網路遭受駭客攻擊的次數是 2011 年的八倍，而且攻擊對象擴展到關鍵基礎設施等。2015 年 10 月，日本將針對國民正式核發社會保障卡，整合健康保險證、護理保險證和年金手冊相關的功能在同一張 IC 卡上，這也代表日本必須更加重視網安議題以確保個資。²⁶

在 2005 年日本設立國家資訊安全中心（National Information Security Center, NISC）與資訊安全政策委員會（Information Security Policy Council, ISPC），負責統籌制定關鍵資訊基礎建設防護之相關政策，這兩者皆隸屬在 IT 戰略總部（IT Strategy Headquarter）之下。但 2014 年前日本的網安政策其實是相當混亂的，這也與其內閣自 2006 年到 2013 年前頻繁的替換首相有關，以致於在資安管理政策上一直有著許多漏洞，直到 2014 年 5 月根據《國家資安策略》（National Security Strategy）內容發佈《關鍵資訊基礎建設保護政策》（The Basic Policy of CIIP），日本的資安策略才開始逐漸步上軌道。²⁷

NewsRSSDetail?lang=zh&RSSType=news&seq=15956>（2017 年 12 月 3 日查詢）。

²⁶ 林穎佑，〈急起直追：日本的網安策略〉，《觀策站》，2016 年 7 月 19 日，<<http://www.viewpointtaiwan.com/columnist/%E6%80%A5%E8%B5%B7%E7%9B%B4%E8%BF%BD%EF%BC%9A%E6%97%A5%E6%9C%AC%E7%9A%84%E7%B6%B2%E5%AE%89%E7%AD%96%E7%95%A5/>>（2017 年 12 月 3 日查詢）。

²⁷ 林穎佑，〈急起直追：日本的網安策略〉，《觀策站》，2016 年 7 月 19 日，<<http://www.viewpointtaiwan.com/columnist/%E6%80%A5%E8%B5%B7%E7%9B%B4%E8%BF%BD%EF%BC%9A%E6%97%A5%E6%9C%AC%E7%9A%84%E7%B6%B2%E5%AE%89%E7%AD%96%E7%95%A5/>>（2017 年 12 月 3 日查詢）。

後日本政府為了提升資安層級，於 2015 年正式推動《網路安全基本法》（Basic Act on Cybersecurity）。《網路安全基本法》最主要的核心目標就是制定資安相關決策，指定由誰來負責，這些單位又要做哪些決策，將任務劃分清楚。在《網路安全基本法》上路後，原本隸屬於 IT 戰略總部的 NISC，改為直屬於內閣管轄，並將名稱變成國家資安事件整備與戰略中心（National Center of Incident Readiness and Strategy for Cybersecurity, NISC），成為一個獨立運作的內閣單位。另提升 ISPC 層級，將原本由 IT 戰略總部管轄的資訊安全政策委員會，提升為網路安全戰略總部並直屬內閣管轄，和其他 IT 戰略總部及國家安全諮詢委員會彼此協同作業。²⁸

除了組織上的調整，網路安全基本法也將網路安全戰略總部的權限大幅提升，在法案推動之前，所有網路資安的運行，要通過政府各單位的同意，並且採自律方式進行審核，無法準確落實。現在則是強制各政府單位要向總部稟報資安相關問題，總部也會向各單位送出正式的資安建議。NISC 則要協助各政府單位落實網路安全的審核，也要在發生重大資安事件時，第一時間介入調查，相較過去協助調查的角色，NISC 權限大幅提昇。²⁹ 最重要的是，日本在網路資安策略的落實，有顯著的效益。過去資安策略只有綁定 ISPC 委員會成員，也無

E7%9B%B4%E8%BF%BD%EF%BC%9A%E6%97%A5%E6%9C%AC%E7%9A%84%E7%B6%B2%E5%AE%89%E7%AD%96%E7%95%A5/ > (2017 年 12 月 3 日查詢)。

²⁸ 日本「網路安全基本法」條文內容請參閱：

<http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&vm=02&id=2760> (2017 年 12 月 3 日查詢)；沈庭安，〈日本要用 3 大資安對策迎戰 2020 奧運會〉，《iThome》，2016 年 7 月 19 日，<<https://www.ithome.com.tw/news/110717>> (2017 年 12 月 3 日查詢)。

²⁹ 沈庭安，〈日本要用 3 大資安對策迎戰 2020 奧運會〉，《iThome》，2016 年 7 月 19 日，<<https://www.ithome.com.tw/news/110717>> (2017 年 12 月 3 日查詢)。

任何強制的執行力，但在網路安全基本法後，所有的網路資安策略是屬於內閣的命令，因此可以將權力拓展到各個政府單位，以確保行政機關及關鍵基礎設施業者之網路安全。此外，該法也直接的探討物聯網安全政策、日本的資安人才培育計畫、促進民間企業與教育研究機關自願參與、資安產業振興強化國際競爭力、推動技術研究開發、公司合作與國際合作等相關基本政策規範。³⁰

三、歐盟

鑒於網路安全威脅所帶來的衝擊效應已漸受重視，2013 年歐盟執行委員會（European Commission）與歐盟外交暨安全政策高級代表（High Representative of the Union for Foreign Affairs and Security Policy）共同發佈歐盟網路安全策略（Cybersecurity Strategy of the European Union）。新的歐盟網路安全策略以「開放、安全與可靠網路空間」（An Open, Safe and Secure Cyberspace）為主軸，對應所面臨的網路安全威脅，提出五項重要策略：³¹

1、實現網路韌力（achieving cyber resilience）：推動政府與私有企業建立資安防禦機制與有效互助合作。包含建立最低網路安全要求準則，建置整體網路安全預防、偵測、處理及回應機制，建置各界網路安全資訊分享與互助合作方式，提升整體網路安全認知能量。

³⁰ 蘇柏毓，〈資訊安全法規國際最新發展舉隅〉，頁 31-32。

³¹ EUROPEAN COMMISSION, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” *EUROPEAN COMMISSION Website*, February 7, 2013, < http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf >（2017 年 12 月 3 日查詢）；王家宜，〈歐盟網路安全策略（Cybersecurity Strategy of the European Union）〉，《行政院國家資通安全會報技術服務中心》，2014 年 12 月 5 日，< <https://www.nccst.nat.gov.tw/ArticlesDetail?lang=zh&seq=1361> >（2017 年 12 月 4 日查詢）。

2、徹底減少網路犯罪（drastically reducing cybercrime）：建立有效及重罰法則為第一要務。

3、針對一般安全暨防禦政策，發展網路防禦政策和能力（developing cyber defense policy and capabilities related to the Common Security and Defense Policy）：歐盟與北大西洋公約組織（NATO）整合雙方的安全政策及資安防禦機制，朝一致化目標前進。

4、建立網路安全之企業和技術性資源（developing the industrial and technological resources for cyber-security）：歐盟希望能儘量使用歐盟國家所生產的網路及資安設備，針對其他地區的資安與設備業者，也能訂出一套監督與治理規則。

5、為歐盟建立一個完整的國際網路空間政策與促進歐盟核心價值（establishing a coherent international cyberspace policy for the European Union and promoting core EU values）：國際資安組織、相關合作夥伴、政府機關與私人企業進行溝通及建立共識，以利建置及推動網路安全政策及更緊密的策略合作。

並推動以下三大相關措施以確保歐盟各會員國間的網路與資訊安全能到達相同的水平。第一會員國至少應該建立以下基本的國家資安能量：建立國家資安主管部門，建立功能完善的計算機應急反應小組並通過國家資訊安全策略和國家資安合作計劃；第二會員國之資安主管部門將進行資安訊息的交換和合作，以防禦資安威脅和事件；第三要求關鍵基礎設施的運營商（如能源、交通、銀行、證券交易所與醫療），主要的網路服務推動者（電子商務平臺、社交網路等）以及公共管理部門必須評估他們所面臨的風險，並採取適當和適度的措施，確保國家資訊安全。同時也被要求必須向其主管部門報告有關影響到核心服務的重要事故。

2016年5月歐洲理事會（European Council）核定的《網路安全準則》（Network and Information Security Directive, NIS

Directive)，7 月 6 日在歐洲議會（European Parliament）正式通過，該準則於 2016 年 8 月生效，各會員國將有 21 個月的時間把該準則嵌入當地法令中，並在之後的 6 個月確認各個基礎營運商的導入狀況。NIS Directive 是歐盟首個網路安全法令，歐盟期望能於歐盟各會員國內建立統一之網路安全準則，向強化歐盟網路安全與法制化跨出成功一步。³²

NIS Directive 要求仰賴資訊與通訊技術的基礎服務必須重視資安問題，涵蓋能源、運輸、水力、金融、健康醫療與數位基礎建設等領域，業者必須採取適當的安全措施，並在發生重大資安事故時通報有關單位。除了上述的基礎服務營運商之外，NIS Directive 還適用於諸如搜尋引擎、雲端運算服務及線上市集等數位服務供應商。歐盟將會設立一個合作組織，以推動會員國在資安上的策略合作及資訊交換，亦將建立電腦安全事件回應小組（Computer Security Incident Response Team, CSIRT）的分享網路。某些重大基礎設施領域的維運者（金融服務、交通、能源或醫療）、資訊社會服務的推動者（APP 商店電子商務平臺、線上支付、雲端運算、搜尋引擎、社群網路）和公家行政部門必須在其核心服務上，進行風險管理及通報重大網路安全事故並做成報告。³³ 從最新頒布的歐盟網路安全策略和執委會頒佈的 NIS 指令可以發現，歐盟對於新世代的網路

³² 陳曉莉，〈歐盟通過首個網路安全準則〉，《iThome》，2016 年 7 月 7 日，<<https://www.ithome.com.tw/news/107004>>（2017 年 12 月 4 日查詢）；Danielle Kriz, “Passage of EU NIS Directive Is a Milestone, But Next Steps Matter Even More,” *CSO Perspective Website*, July 6, 2016, <<https://researchcenter.paloaltonetworks.com/2016/07/passage-of-eu-nis-directive-is-a-milestone-but-next-steps-matter-even-more/>>（2017 年 12 月 4 日查詢）。

³³ 〈歐盟通過首個網路安全準則〉，《行政院國家資通安全會報技術服務中心》，2016 年 7 月 18 日，<<https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=15667>>（2017 年 12 月 4 日查詢）；完整條文請參閱 <[http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016AG0010\(01\)&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016AG0010(01)&from=EN)>（2017 年 12 月 4 日查詢）。

安全風險及威脅，已經有完整的預見與具體的因應措施。

四、國外網路安全政策趨勢

綜觀上述各國網路安全政策，美國之各時期戰略報告著重將網路安全納入國家安全戰略一環，而《聯邦資訊安全現代化法》將納入美國國土安全部為管理角色之一，並要求對資安事件進行通報，《國家資安行動計畫》用以強化政府以及私部門的資安能力；日本之《網路安全基本法》則是將主管資安層級機關位階提高並賦予相當職權；歐盟之《網路安全準則》確保歐盟各會員國間的網路與資訊安全能到達相同的水平並進行合作，以下綜整各國資安發展趨勢均重視以下幾點：³⁴

1、網路安全納入國家安全戰略一環：網路是全新的技術空間，全球駭客持續入侵各國相關資訊系統，非法及破壞事件有日益頻繁而嚴重的情形，網軍專門偷竊他國各類情報，並破壞他國的電腦系統，已然對國家安全造成了威脅，傳統上國家安全戰略重視軍事、外交等層面，但現今許多國家以將「第五空域（網際空域）」納入國家安全戰略層次，除美國發布多部安全戰略報告外，近期如 2016 年 11 月 1 日英國財務大臣 Mr. Philip Hammond 宣布英國投資 19 億英鎊來推動英國國家網路安全戰略，從防禦、嚇阻和發展這三個核心上建立；³⁵ 新加坡

³⁴ 蘇柏毓，〈資訊安全法規國際最新發展舉隅〉，頁 33-34。

³⁵ 英國已在過去 5 年投資 8.6 億英鎊，提升政府網路的防護能量，強化對於網路攻擊和網路犯罪的應變能力。同時也建立了一個網路委員會（Cyber Committee），成員來自外交部（Foreign Office）、國防部（Ministry of Defence）、內政部（Home Office）等相關部門部長，共同合作研議解決英國目前面對的網路威脅。企業方面，政府也鞏固了與企業之間的合作夥伴關係，密集關注到網路風險的議題。研發方面，英國建立了 13 個專門探討網路安全研究和創新的學術中心（Academic Centres of Excellence）。〈英國政府推動國家網路安全戰略〉，《行政院國家資通安全會報技術服務中心》，2016 年 11 月 30 日，〈<https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=15815>〉（2017 年 12 月 4 日查詢）；完整版英國國家網路安全戰略請參閱：〈https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/〉

總理李顯龍在 2016 年 10 月中旬，以國家最高領導人總理身份參加國際網路節，同時揭櫫攸關未來新加坡網路安全局所擬制的最高資安指導原則《新加坡國家網路安全戰略》。³⁶ 此都顯示網路安全已佔據國家安全重要角色地位。

2、建立專責機關強化職權職能：由於資安問題已屬於需投入一定資源、人力與技術，方能因應之問題，故推動公私部門落實資安要求一事，目前常有以法規授權專責機關負責，並提供該機關充足之權能與資源之方式進行。且如上述法規介紹所示，尚會依據行政與法制體系之需求規定妥適權責，並適時強化其權能，如賦予其對相關公私機關進行資安之監督權責等。

3、關鍵基礎設施納入法律規範管理：因關鍵基礎設施乃維持民生、經濟與政府等相關運作而提供之基本設施與服務，故若其發生資安方面的問題，導致無法或錯誤運作，便很有可能造成重大的生命、身體或財產的損失。故明確以法律規定，要求其採行適當之資安措施，或進一步落實相關之資安標準，乃有其必要，且應由相關政府主管機關加以持續監督稽核。

4、建立通報因應機制強化公私合作：無論資安管理之落實程度如何，仍無法百分之百避免資安事件之發生，因此建立資安事件之通報與因應機制，即成為降低風險與損害之重要措施。而公私合作主要強化公部門與關鍵基礎設施業者間管理與合作之關係，通過資安事件通報與資安情資分享，以及專責機

national_cyber_security_strategy_2016.pdf> (2017 年 12 月 4 日查詢)。

³⁶ 李顯龍在新加坡網路安全節的演講致詞時對外宣示，國家級網路安全戰略有 4 個重要的支柱，分別是：建置彈性關鍵資訊基礎設施，創造安全網路空間，發展具有活力網路安全生態系統，以及強化網路安全相關的國際合作關係。黃彥棻，〈新加坡用總理高度揭露國家資安戰略，臺灣呢？〉，《iThome》，2016 年 10 月 19 日，<<https://www.ithome.com.tw/news/109141>> (2017 年 12 月 4 日查詢)；黃彥棻，〈新加坡大砸 40 億元推動國家級網路安全戰略〉，《iThome》，2016 年 10 月 13 日，<<https://www.ithome.com.tw/news/109011>> (2017 年 12 月 4 日查詢)。

關與國際間相關資安專責機關之合作，希望能達成共同打擊網路犯罪與因應資安事件之目標。此外，亦持續研發資安標準與技術，以建立堅實之資訊系統環境，乃為資訊安全之基石。

肆、我國資通安全戰略及體系檢測

一、我國資通安全戰略

在我國國家安全戰略上將資訊安全納入可參見由我國國家安全會議於 2006 年 5 月 20 日出版的《2006 國家安全報告》，在其報告書的第三部分「國家安全的內外威脅上」臚列九項威脅，其中在第八項威脅點出資訊安全威脅，在其內容上說明「隨著資訊系統之運用的普及化，資訊及網路安全已成為日趨重要的國家安全課題。現今無論是軍事、金融、交通管理、電力調度乃至國家行政體系，都相當依賴資訊系統來進行作業處理與訊息管理。因此，資訊、網路系統與設施已經成為關鍵性的基礎設施之一。」其後更分點列出一般資訊安全威脅、戰略資訊戰的威脅及中國強化資訊戰對我之安全威脅。³⁷ 在第四部分國家安全策略第八項建議構築資訊時代的資訊安全體系，包括第一以新思維強化資訊安全的三項策略，包括以彈性化人事任用制度，擴大引進民間資安人才、增設專責單位，提升整體資安維護之能量及訂定具體戰略及政策指導，強化資安因應措施；第二強化資訊安全的具體措施計有 6 項，包括建立資安預警暨分享機制、依法建立內部稽核、建立資安標準作業程序、優化系統架構、增加資訊安全投資及加速完成《個人資料保護法》及《電子交易法》之立法。³⁸ 在 2008 年《2006 國家安全報告（2008 年修訂版）》中，其中資訊安全威脅與 2006 年版本一致，而在具體因應策略上則增加強化使用者端的資安防護、

³⁷ 國家安全會議，《2006 國家安全報告》，（臺北：國家安全會議，2006 年），頁 72-76。

³⁸ 國家安全會議，《2006 國家安全報告》，頁 133-136。

加強關鍵基礎設施的資安防護及加強軟體安全。³⁹ 往後我國就無國家安全報告，但此兩版本的國家安全報告對於我國的資安戰略有其一定程度說明，但缺陷在於往後無更新版本，雖馬英九政府及現今蔡英文政府國家安全會議皆有設置資訊專長的諮詢委員，但上位階層戰略具有延續政策及檢討改進作用，以避免人事更迭而政策無法延續之現象。

另從新政府負責資安政策人事戰略規劃觀察，2017 年 3 月 15 日第三屆臺灣資安大會（Taiwan Cyber Security Summit 2017）上，制訂國家資安發展方針的國家安全會議諮詢委員李德財表示要落實「資安即國安」的政策方針，就必須要做到確保數位國家安全，並且加速數位經濟發展，所以政府透過推動 3x3x3 國家級資安戰略，做到面對資安威脅可以超前部署、預置兵力。李德財進一步解釋 3x3x3 國家級資安戰略，就是政府必須要做到包括資安人力資源、前瞻的科研資源以及產業資源的三大跨域整合，並且提升基礎整備、產業能量和數位防衛等三大面向的能力，進而做到政府預期達成的三大目標，首先是打造國家級的資安機制；其次，要建立國家級的資安團隊以確保數位國土安全；最後，則是要推動國防資安自主研發，強化產業發展。⁴⁰

³⁹ 國家安全會議，《2006 國家安全報告（2008 年修訂版）》，（臺北：國家安全會議，2008 年），頁 79-83、143-147。

⁴⁰ 此 3x3x3 國家級資安戰略構想擬定於 2016 年 8 月 27、28 日由國安會與政院十多個相關部會共同召開擴大資安會議，此會議討論「資安即國安機制與策略」、「國家層級資安團隊發展策略」、「國防資安產業發展策略」等三大議題。參與會議討論的單位包括國安局、內政部、國防部、科技部、法務部、經濟部、交通部、國發會、教育部、主計總處與人事總處等，政府部門參與人士包括行政院科技政委吳政忠、國安會諮委李德財、行政院科技會報執行秘書郭耀煌、行政院資通安全處處長簡宏偉等人。黃彥棻，〈國安會諮詢委員李德財：推動國家級資安戰略，捍衛數位國土安全〉，《iThome》，2017 年 3 月 16 日，< <https://www.ithome.com.tw/news/109141> >（2017 年 12 月 4 日查詢）；〈資安即國安 府院今明擴大資安會議〉，《自由電子報》，2016 年 8 月 27 日，

而在臺灣在國家資安政策綱領的制定上，在 2001 年～2004 年就通過《建立我國資通訊基礎建設安全機制計畫》，除了推動資訊安全管理系統（ISMS），並制定資安責任等級分級以及落實資安演練，也在 2001 年 1 月成立行政院國家資通安全會報，並於同年 3 月規畫成立國家資通安全技術服務中心（簡稱技服中心），藉此建構資安防護體系。從 2005 年～2008 年，臺灣政府則制定《建立我國資通訊基礎建設安全機制計畫》，目的在健全資安防護能力，除了推動資訊安全長的責任制度外，也打造國家資通安全防護管理平臺，制定資安關鍵指標和落實資安內稽，更重要的是，實體隔離的政策也在此階段推動；自 2009 年～2012 年則通過《第三期發展方案：國家資通訊安全發展方案》，目的是要打造安心信賴的智慧臺灣，也要讓民眾可以過安心優質的數位生活，這期間，主要是落實關鍵資訊基礎設施的防護（CIIP），強化緊急應變與復原能力，政府也特別要求電子商務業者的資訊安全，也制定資訊系統分級分類，希望可以真正落實資安治理；從 2013 年～2016 年則是《第四期發展方案：國家資通運安全發展方案》，目的是希望可以建構安全資安環境、邁向優質網路社會，期間除了推動功能性資安組織（106 年 5 月 3 日遭到立法院廢止資安科技中心），也希望可以完備相關的資安管理法規（行政院近期推動的資通安全管理法），可以促進產官學研的合作交流，更希望建構資安專案管理（PMO）機制，落實資安防護二級制並推動政府資訊安全組態基準設定（參閱圖 1）。⁴¹

<<http://news.ltn.com.tw/news/politics/paper/1025776>>（2017 年 12 月 4 日查詢）。

⁴¹ 行政院國家資通安全會報，〈我國重大資安政策進程〉，《行政院國家資通安全會報網站》，2014 年 2 月 25 日，<http://www.nicst.gov.tw/News_Content3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF&s=1ACE1B808B9444DF>（2017 年 12 月 4 日查詢）。

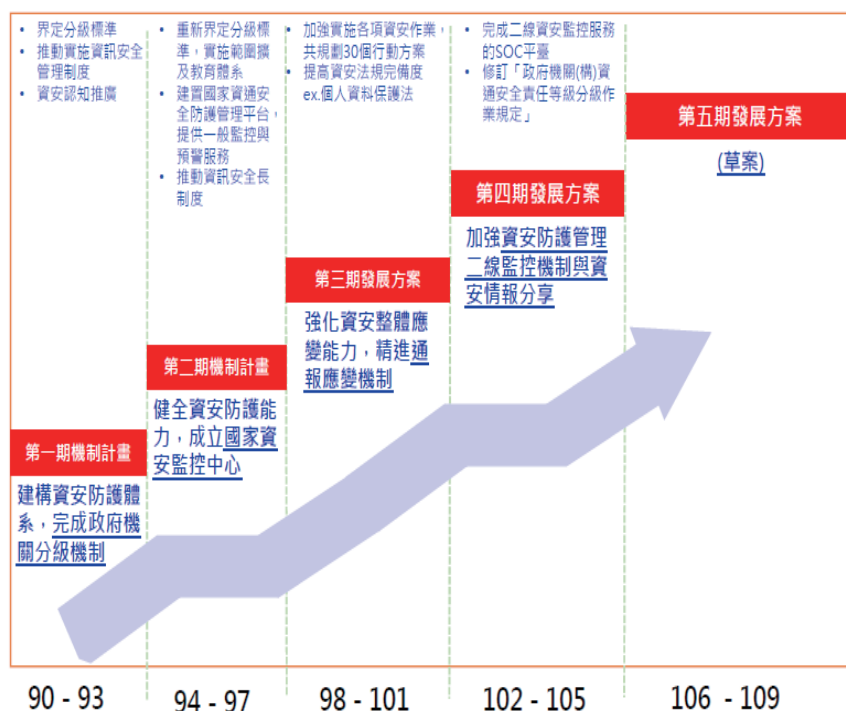


圖 1 我國資安推動歷程

資料來源：簡宏偉，〈資通安全管理法與發展藍圖〉，《iThome》，2017 年 9 月 22 日），〈<http://s.ithome.com.tw/egov/2017/A-1320.pdf>〉（2017 年 12 月 4 日查詢）。

從臺灣過往四個階段的資安發展方案來看，臺灣雖然起步早，但歷年資安政策都偏向政府體系中的各種防護作為，缺乏與民間企業甚至是國際合作的方向，且直到 2016 年 8 月 1 日才有專門的資安組織，但仍設下在行政院，偏重的仍是政府應該有的資安作為；若要真正落實資安等於國安的政策方針，從既有的各種政策高度來看，仍然不到國家安全的政策高度。另行政院資安處正在著手進行第五期國家資通訊安全發展方案草案，預計從國家安全、資安管理、產業發展、科技研發和人才培育等 5 個面向進行研議，相關的政策計畫也正在評估中，預

算初步估計也有 10 多億元（參閱圖 2），⁴² 但最終政策高度到哪裡，相關的資安人力是否足夠因應未來資安事件、資安專案是否仍淪為資安廠商的設備採購和系統建置費用，以及能否提供區域性的、全球性的，更為宏觀的資安政策願景等需進一步以時間檢視。

二、我國資通安全體系

（一）組織機制

現階段政府執行資通訊安全工作之主要依據為 2013 年 12 月起之《第四期發展方案：國家資通運安全發展方案》（102 年至 105 年）。該期間於行政院設「國家資通安全會報」及「資通安全辦公室」，下設相關分組處理有關業務，業務推動重點包括資安責任等級分級、資通安全管理與維護責任、資通安全長之設置、資通安全維護計畫之制定與實施、資通安全查核、年度資通安全報告之提出、資通安全事件預防通報及應變等。⁴³ 因資安會報、資安辦公室人員係為臨時任務編組，角色與責任之分工容易混淆，永續性較為不足，每一資安事件發生後，就屢受批評；於是 2015 年 10 月，行政院首度提出資通安全管理法草案，將該方案進行之組織架構及主要事項納入立法，並提出《國家資通安全科技中心設置條例》立法通過；但後因政府政黨輪替，該法未通過，而國家資通安全科技中心亦遭撤除。政黨輪替後，行政院設置「資通安全處」院內單位，迄今除資通安全處為正式院內單位外，其他資安會報等組織架構皆

⁴² 簡宏偉，〈當前資安情勢與未來推動重點〉，《行政院》，2016 年 9 月 22 日），<<http://www.ey.gov.tw/DL.ashx?u=%2FUpload%2FRelFile%2F19%2F741464%2F1ea97c3e-c045-4352-b500-dd9b7cc4fd97.pdf>>（2017 年 12 月 4 日查詢）。

⁴³ 行政院國家資通安全會報，〈行政院國家資通安全會報組織架構〉，《行政院國家資通安全會報》，2016 年 8 月 1 日，<<http://www.nicst.ey.gov.tw/cp.aspx?n=F1FB6AFC30C728EC&s=FABA959E6E602DA3>>（2017 年 12 月 4 日查詢）。

第五期國家資通訊安全發展方案(草案)



圖 2 行政院資安處第五期國家資通訊安全發展方案（草案）

資料來源：簡宏偉，〈當前資安情勢與未來推動重點〉，《行政院》，2016 年 9 月 22 日），<<http://www.ey.gov.tw/DL.ashx?u=%2FUpload%2FRelFile%2F19%2F741464%2F1ea97c3e-c045-4352-b500-dd9b7cc4fd97.pdf>>（2017 年 12 月 4 日查詢）。

尚未處理。而一個轄屬於院內的組織，是否適合擔負國家整體資安政策及推動工作，乃是值得更進一步檢討之重要議題。

除設立專責資安機構行政院資安處外，國安會負責資安諮詢委員李德財組建資安鐵三角架構，以落實「資安即國安」戰略高度，包括成立國安會資通安全辦公室與行政院資安處以及國家通訊傳播委員會成立資安鐵三角。國安會資通安全辦公室為國家資通安全政策幕僚單位，且要執行國安會國家資通安全指導小組相關決議事項，其不僅與行政院資安處採聯合作業方式，統合政府各機關全面推動國家資通安全工作，真正發揮政府一體的資通安全功能外，也和監管電信網路安全的國家通訊傳播委員會密切合作配合。在運作機制上，李德財指派現任

國發會管制考核處處長何全德兼任國安會資通安全辦公室主任一職，國防部和國安局也個別指派一位副主任，與行政院資安處處長簡宏偉聯繫配合。⁴⁴ 此聯繫機制立意良好，總統府可以執行資安戰略高度直接統籌指揮行政院資安處合作配合執行政策，但因國安會資通安全辦公室為初始成立之組織，其可發揮多大綜效值得後續觀察。

（二）會報機制

有別於馬政府時期在政院成立的「資安辦公室」是任務編組，行政院資安處擴編原有資安辦的組織規模，並將原先的資安管理三級制調整為二級制，由資安處直接指揮行政院國家資通安全會報技術服務中心（National Center for Cyber Security Technology, NCCST），不需透過科技部，以強化資安通報應變效率。目前國內資安事件通報管理以行政院資安處為對口，統一作為關鍵基礎設施的主管機關，並分為來自民間與政府機構的兩大通報管道，民間通報統籌由臺灣電腦網路危機處理暨協調中心（Taiwan Computer Emergency Response Team/Coordination Center, TWCERT/CC）彙整，而政府機構則統一彙報到行政院國家資通安全會報技術服務中心，此二管道都會直接連接到行政院資通安全處，並視重要性與實質的需要而投入包括軍方與民間等重要的機構協助解決。

另新政府在資安通報規劃作為上，建構國家級的整體資安聯防機制，已經涵蓋包括能源、水資源、政府機構、通訊傳播、高科技園區、交通運輸、緊急醫療與銀行金融機構，並整合六個直轄市的聯防，另因資安層面影響非常的寬廣，民間企業也應納入聯防體系，並由 TWCERT/CC 負責推動。TWCERT/CC 為了有效與國際聯防組織情資交換需要，將建置自動化的情資

⁴⁴ 黃彥棻，〈國安會資通安全辦公室正式成立，國發會管制考核處處長何全德接任主任一職〉，《iThome》，2016年8月5日，<<https://www.ithome.com.tw/news/107527>>（2017年12月4日查詢）。

分享機制，來統籌與推動民間企業導入資安聯防機制。⁴⁵

（三）評估作為

從新政府規劃的組織及會報機制上，在組織機制上成立資安專責單位行政院資安處，並與國安會資通安全辦公室與及國家通訊傳播委員會成立資安鐵三角，此組織架構有朝先進國家資安體系學習，但遭詬病的是專責人力不足之問題，從國安會諮委李德財的資安戰略規劃中，可以明顯看出第一步是先完善政府資安組織機制，後再擴充資安人力，最後則是公私結合帶動資安產業發展，此戰略構想立意良好，但也有論者指出行政院在 2016 年 8 月 1 日成立的「資通安全處」，目前僅有 21 人，包括正式人員 16 人，其中 6 人為行政院員額，10 人自科技部移撥，另從其他部會借調 5 人，資安處首任處長由國發會資訊處長簡宏偉接任，並由科技政委吳政忠督導資安處相關業務，在此人力架構下是否有能力規劃國家資安戰略，⁴⁶ 此外目前政府盤點中央與地方等三、四千個各級公務機關均面臨資安人力都是兼職，不少部會都向政院反映專責資安人力不足，遑論各地方政府及其下轄的各機關，推估全國由中央到地方的專責資安人力缺口至少 1000 人以上，而行政院資安處建議短期以約聘僱方式攬才，或考慮資安暫時委外辦理，而此項資安專職人員不足缺陷將直接影響國家資安戰略之推行。⁴⁷

⁴⁵ 劉念祖，〈政府與民間合力搭建資安通報應變與聯防機制〉，《Digitimes》，2017 年 9 月 25 日，<http://www.digitimes.com.tw/tech/dt/n/shwnws.asp?id=0000513432_ZFQ3WGXN4YWZKE1E8ZTB8>（2017 年 12 月 4 日查詢）。

⁴⁶ 〈政院資安處 8.1 掛牌 21 人成軍〉，《自由電子報》，2016 年 7 月 24 日，<<http://news.ltn.com.tw/news/focus/paper/1014161>>（2017 年 12 月 4 日查詢）。

⁴⁷ 李欣芳，〈建構國家資安 尚缺千餘人力〉，《自由電子報》，2017 年 1 月 17 日，<<http://news.ltn.com.tw/news/focus/paper/1071736>>（2017 年 12 月 4 日查詢）；王君瑋，〈公部門資安人力短缺 資安處：短期內以約聘、委外方式處理〉，《風傳媒》，2017 年 1 月 17 日，<<http://www.storm>

另有論者建議將廢止的國家資通安全科技中心重新立法設立，以補足目前行政院資安處人力不足現況，且行政院國家資通安全會報技術服務中心人員具備專業技能，如轉型行政法人，其資安人力具備準公務人員身分，在處理資安事件上較具適法資格，⁴⁸ 但此面臨政治質疑，因而立法院在 2016 年 5 月 3 日的院會中，通過由時代力量提案廢止「國家資通安全科技中心設置條例」，後在 106 年 5 月 25 日總統公告廢止，讓 2016 年 4 月 1 日正式掛牌的國家資通安全科技中心，回復到原本委由資策會技服中心負責政府資安委外的作法。而目前新政府資安組織架構重新調整，更應思考行政院國家資通安全會報技術服務中心未來定位問題。

在會報機制上，原則上公部門會報機制具強制性，且由行政院國家資通安全會報技術服務中心彙整並通報行政院資安處，但在這匯報管道上，參考外國作法，資安情資分享至為重要，各國多設有資安情資分享平臺，我國可參考應用；另私部門通報機制上，TWCERT/CC 負責民間企業的資安通報與應變，目前協助政府進行相關資安通報應變準則（Guideline）的規劃，界定通報的方式與訊息管道的傳遞方式，讓民間組織有所依循，並配合政府部門自建的各種 ISAC（資安資訊分享與分析平臺）或者是 SOC（資安監控中心）、CERT（網路危機處理中心）以及 CSIRT（網路危機處理應變中心）等，形成資安情資分享網路。⁴⁹ 但私部門通報機制無強制力，且一般私部門企業多存有資安由企業自行處理完畢即可，不需要由國家力

mg/article/213972>（2017 年 12 月 4 日查詢）。

⁴⁸ 黃彥棻，〈立院通過廢止資安科技中心設置條例，贊成者：正確第一步，反對者：親痛仇快〉，《iThome》，2016 年 5 月 4 日，<<https://www.ithome.com.tw/news/105714>>（2017 年 12 月 4 日查詢）。

⁴⁹ 黃彥棻，〈臺灣 TWCERT/CC 負責哪些資安任務？〉，《iThome》，2016 年 9 月 4 日，<<https://www.ithome.com.tw/news/108002>>（2017 年 12 月 4 日查詢）。

量介入，TWCERT/CC 如何建構公私協力平臺及取得私部門信任，渠部門推廣業務是另一挑戰。

伍、資通安全管理法草案評析

一、資通安全管理法草案架構及內容

2017 年 4 月 27 日行政院為推動國家資通安全法制化，通過資通安全管理法草案，在草案說明上明確指出「隨著網際網路及其他資通科技之快速發展與普及，資通科技相關應用，已被世界各國視為協助產業經濟轉型及有效解決社會發展議題之關鍵，各國亦紛紛致力於資通政策之規劃，期能建構公開、有效率之數位環境，並希望藉由科技化服務，提升民眾生活品質、維護公共利益、帶動產業發展及國家整體競爭力」，並希望藉由資安法制化帶動整體資安產業的發展。⁵⁰

在草案架構上包括 5 個章節，分別為第一章總則（第一條至第八條）、第二章公務機關資通安全管理（第九條至第十四條）、第三章非公務機關資通安全管理（第十五條至第十八條）、第四章罰則（第十九條至第二十一條）及第五章附則（第二十二條至第二十三條）（參閱圖 3）。⁵¹ 其中草案內容適用對象有 3 類，第一類是政府部會、地方政府等公務機關；第二類為能源、水資源、交通運輸、金融、資通訊、緊急醫療、中央與地方政府及高科技園區等 8 大關鍵基礎設施提供者，由中央部會提出清單納管；第三類為非關鍵基礎設施的公營事業及政府捐補助財團法人。較重要部分包括明定行政院應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及

⁵⁰ 〈資通安全管理法草案總說明〉，《行政院》，2017 年 4 月 27 日，
<http://www.ey.gov.tw/News_Content4.aspx?n=D0675BEBB0C613C7&sms=1B6A34286EEBCD4C&s=79472F6EDE25F136>（2017 年 12 月 4 日查詢）。

⁵¹ 簡宏偉，〈資通安全管理法與發展藍圖〉，《iThome》，2017 年 9 月 22 日，
<<http://s.itho.me/egov/2017/A-1320.pdf>>（2017 年 12 月 4 日查詢）。

資通安全整體防護等相關事宜，並應定期公布國家資通安全情勢報告及資通安全發展方案；公務機關應稽核其所屬或監督公務機關的資通安全維護計畫實施情形。受查核機關的資通安全維護計畫實施有缺失或待改善者，應提出改善報告。至於公務機關為因應資通安全事件，應訂定通報及應變機制。公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報行政院；無上級機關者，應通報行政院；在非公務機關部分，草案明定關鍵基礎設施提供者、公營事業以及政府捐助的財團法人，要向中央主管機關或縣市政府提出資通安全維護計畫實施情形，而為因應資安事件，應訂定通報及應變機制，違反者可要求限期改正，屆期未改正者，按次處罰 10 萬元以上、100 萬元以下罰鍰。⁵²



圖 3 資通安全管理法草案架構

資料來源：簡宏偉，〈資通安全管理法與發展藍圖〉，《iThome》，2017 年 9 月 22 日，<<http://s.ithome.com.tw/news/politics/breakingnews/2049801>>（2017 年 12 月 4 日查詢）。

⁵² 李欣芳，〈防止駭客攻擊 政院端出國家首部資通安全法〉，《自由電子報》，2017 年 4 月 27 日，<<http://news.ltn.com.tw/news/politics/breakingnews/2049801>>（2017 年 12 月 4 日查詢）。

二、資通安全管理法草案建議事項

(一) 產官學界對於草案建議

行政院資安處為儘快能夠完成資通安全管理法草案三讀，在 2016 年 8 月底完成法案初稿，並一連舉辦 6 場法案座談會，不只找來政府機關資訊與資安業務相關的主管參與，也照例向法界和資訊界學者請益，還特別舉辦 2 場向民間意見領袖和業界資訊、資安主管請教，2016 年 9 月底更進一步將法案草案上網公開向全民徵求意見，期間草案內容獲得產官學界許多建議，以下就各界意見整理如次：⁵³

1、政府機關建言⁵⁴

- (1) 考量政府機關資安人力不足或專業不足，建議減少例行文書作業，如免定資通安全維護計畫，或是明文列出應投入適當資安資源的規定，以充裕各機關資安預算及人力；
- (2) 電子商務業者資安防護不足，建議也納入規範；
- (3) 行政檢查作業面上，一來因無急迫危急人身安全，建議刪除警察陪同，改有危害才報警，另可增加遭遇大規模攻擊時，可尋求國軍支援的項目；
- (4) 草案第八條規定政府採購需特別考量資安需求，恐與現行採購法規定採整體評選作法衝突需解決；
- (5) 未來訂定通報應變辦法時，應納入證據保全程序。資安通報可以和法務部調查局現行通報整合來簡化

⁵³ 黃彥霖，〈產官學 3 方資安管理法建言大整理〉，《iThome》，2016 年 10 月 10 日，〈<https://www.ithome.com.tw/news/108920>〉（2017 年 12 月 4 日查詢）。

⁵⁴ 〈「資通安全管理法(草案)」政府機關座談會紀錄〉，《公共政策網絡參與平臺》，2016 年 9 月 6 日，〈<https://join.gov.tw/attachments/9a07113a-f916-4e61-8a33-5625e2805029/download/1050906%E6%94%BF%E5%BA%9C%E6%A9%9F%E9%97%9C%E5%BA%A7%E8%AB%87%E6%9C%83.odt>〉（2017 年 12 月 4 日查詢）。

程序；

- (6) 產業權責主管機關除中央目的事業主管機關之外，可以增列管轄機關；
- (7) 草案獎少懲罰多，建議調整比例。

2、民間團體建言⁵⁵

- (1) 應釐清所有納管產業的主管機關並統一權責單位，並訂定業者遵循標準，以利衡量是否善盡責任，或提供完整資安維護範本；
- (2) 關鍵基礎設施定義需更清楚，如通訊軟體是否納入？高科技園區內企業是否納入？也應明訂重大資通安全事件之定義。或是限縮非公務機關規範範圍，排除與關鍵基礎設施無關之企業；
- (3) 委外監督應訂標準，並限縮於受委託範圍；
- (4) 罰則較重，應提供更多獎勵和輔導措施，例如將資安投資納入投資抵免範疇。也建議採比例原則，先輔導改善再課罰；
- (5) 資安事件往往事後才能發現，規定未通報就開罰恐對業者負擔過大。另外，企業通報後，應可獲得政府部門支援來改善；
- (6) 政府應保障相關預算和人力，並提供資安人才培育機制；
- (7) 政府應建立整體資安防護系統，抵抗境外攻擊；
- (8) 不宜增加國軍介入的項目；
- (9) 不需訂定行政檢查，或刪除司法警察陪同之條文；
- (10) 資安維護規定與現有法律多有重疊，應進一步調

⁵⁵ 〈「資通安全管理法(草案)」民間團體座談會紀錄〉，《公共政策網絡參與平臺》，2016年9月8日，<<https://join.gov.tw/attachments/d1f218e5-e599-441a-95f6-a2a51c366669/download/1050908%E6%B0%91%E9%96%93%E5%9C%98%E9%AB%94%E5%BA%A7%E8%AB%87%E6%9C%83.odt>> (2017年12月4日查詢)。

整，避免提高企業法尊成本或一事多罰；

(11) 應釐清境外單位是否納管，尤其協助外商遵守本法；

3、學者專家建言⁵⁶

(1) 立法目的、達成實際作法、私部門規範之必要應有更詳細說明，例如納入資安預防、資安保護、證據保全與專業鑑識，或適度納入管理、技術、稽核及風險評估等面向，草案架構可考慮部分內容分開立法；

(2) 建議法條先以政府機關規範為主，不列入民間企業；

(3) 行政院應籌組諮詢委員會，協助政府掌握資安高速變動；

(4) 應釐清資訊和資安業務各自的主管機關；

(5) 關鍵基礎設施指定若有爭議，行政院應增設爭議協調機制；

(6) 主管機關可指定納管企業的範圍過廣。關鍵基礎設施提供者之界定應有一套判別基準，而非只由主管機關指定，或統一由行政院公告訂定關鍵基礎設施定義；

(7) 加強對非公務機關之義務規範，包括通知當事人義務、目的外利用或再識別行為；

(8) 對企業罰則強度不足，罰則額度小於個資法，難發揮效果。建議可增加，對其他之事業、機關或個人之資料安全、財產、生命或其他之資訊運作有重大影響者，主管機關得要求停止全部或部分業務的營業。也可要求負責人應接受教育講習；

⁵⁶ 〈「資通安全管理法(草案)」學者專家座談會紀錄〉，《公共政策網絡參與平臺》，2016年9月13日，<<https://join.gov.tw/attachments/d5fbeat9-02ff-4fde-b34d-59f29f36987d/download/1050913%E5%AD%B8%E8%80%85%E5%B0%88%E5%AE%B6%E5%BA%A7%E8%AB%87%E6%9C%83.odt>>（2017年12月4日查詢）。

- (9) 罰則應涵蓋公務機關，另避免圖利資安業者；
- (10) 建議對民間資安投資可給予租稅優惠；
- (11) 應設立國家級資安長，另對各級機關資安長，可訂定符合資格條件來遴選；
- (12) 建議將定期稽核、檢查、復原及動員計畫納入草案；
- (13) 可訂定日出條款，逐步納入不同規範對象；
- (14) 行政檢查發動時機的合宜性需考慮。

而在 2017 年 4 月 27 日行政院通過資通安全管理法草案，更陸續在 8 月 10 日、11 日舉辦座談會，其中行政院資安處確立多項爭議問題，包括：⁵⁷

- 1、關鍵基礎設施的定義、對象，目前不包括網站、電商；
- 2、由政府補捐助超過 50% 的財團法人是列管對象，但標準會再衡量；
- 3、為什麼對公務機關依據公務人員考績法、公務員懲戒法進行相關的獎懲（第十四條），但對非公務機關卻只有處罰（第十九條～第二十一條）說明；
- 4、各機關都需要提出各自的資通安全維護計畫，行政院會提供參考的範本；
- 5、模糊解釋了負責委外稽核的對象、有誰具有相關的權限。
- 6、對非公務機關的通報來說，資安處只對中央目的事業主管機關、地方政府，也就是非公務機關無法直接向資安處通報或請求協助。

（二）對於草案內容之評估

本次提出之資安法草案內容，綜觀產官學界較重視非公

⁵⁷ 行政院國家資通安全會報，〈「資通安全管理法草案」說明會會議紀錄〉，《行政院國家資通安全會報》，2017 年 8 月 31 日，<http://www.nicst.gov.tw/News_Content.aspx?n=7D08312E0E5D8F33&sms=04631FAE19EA7CCA&s=BDF4D0DD8763E82C>（2017 年 12 月 4 日查詢）。

務機關如何界定、非公務機關中行政檢查適法性以及公務非公務機關如何進行資安通報相關細節等問題上，因本身較重視整合，尤其近期資安已和國土安全、保防法制化議題有所關聯重疊，因此必須要有整合或協調機制，但現今資通安全管理法草案看起來是大致延續過去臨時任務編組之作法，但卻未見統籌整合機制，比較大的突破為首度把非政府機關之關鍵資訊基礎設施（Critical Information Infrastructure，下簡稱 CII）納入，並提出行政檢查及罰責，但如何強化部門間聯繫配合、公私治理關係落實則需從磨合合作中累積。筆者整理資安專業人士及法界人士就資通安全管理法草案評估如下：⁵⁸

1、整體國家安全與資通安全框架定位不明

- (1) 資通安全涵蓋之關鍵基礎設施即所謂 CII，需與更上位之國家安全之關鍵基礎設施（Critical Infrastructure, CI）防護接軌。法規草案中所指之 CII 實為國家 CI 範圍內之項目，CI 為 CII 之上位層次，CII 之規範理應與 CI 要求一致，在 CI 未有明確規範前，就談 CII 似乎缺乏穩固之基礎，且亦未盡完整之思維邏輯。（目前草案中未敘明）
- (2) 草案與其他主管部門相關法規之關係尚待釐清，包括與通訊傳播基本法、電信法、個資法、金融保險、醫療衛生等相關法規，是否有重疊競合或衝突之處。
- (3) 資通安全之範圍包括跨中央各部會、跨中央與地方、跨公部門與私部門，條文中之中央目的事業主管機關要做很多事情，如應指定 CI 清單、核定及查核 CI 資通安全維護計畫、遇重大資安事件之行政檢查及罰則執行等，其機制屬由各目的事業主管機關分

⁵⁸ Vincent Chen，〈從歐盟資安運作法規與架構，談我國的資安法規課題〉，《火箭科技評論》，2016 年 10 月 4 日，<<https://rocket.cafe/talks/79619>>（2017 年 12 月 4 日查詢）。

散自行處理方式，屆時各部會步調、品質要求不一，全國資安保護成效，即會受到很大影響。因此建議全國資安政策及推動，應有統籌整合、協調及管理之明確權責設計。（目前草案中未敘明）

2、未融入治理機制設計及強化公私協作夥伴關係

我國 CI、CII 及資通訊安全之相關推動工作，都尚能隨世界各國發展趨勢迅速開展，但法規及持續治理機制之建立，始終不甚理想。一般治理之範圍包括建立政策、策略、方針，確保遵循政策、標準及程序，及執行策略及管理風險等。資安法草案第一條之定位為推動國家資通安全政策，加速建構國家資通安全環境，但後續條文對達成上述目標之良好治理核心要素，如歸責、透明、多方參與、即時回應、效率、合法框架等諸多項目，皆尚未能明確設計涵蓋，仍以完全由上而下之管理角度出發，較不符合新型態之治理法規機制規劃。

利害關係人公私協作夥伴在關鍵資訊基礎設施安全防護（Critical Information Infrastructure Protection, CIIP）機制中，被認為是一項比較有效的重要機制之一，應設計如何協助私部門提升資安能量及強化公私協作夥伴之相關誘因機制（如芬蘭對公司投入購置資安設施享有減稅優惠）。

3、未強化網路危機管理機制與風險評鑑與管理

草案中有敘明因應資通安全事件應向中央目的主管機關通報及應變機制，必要時得執行必要行政檢查等。惟如遭受全國性大規模網路攻擊事件，涉及跨中央目的主管機關需有之明確、快速因應之緊急動員機制，目前草案中並未敘明。另執行國家層級、部門層級之資安風險評鑑、因應措施及安全稽核作業，被認為是良好 CIIP 實務原則之一，目前草案中未敘明，建議應至少將進行國家層級之資安風險評鑑納入，以作為 CIIP 提供者之認定及資安防護項目之依據。

4、行政檢查及罰責之依據有適法性之疑義

草案中對於非公務機關 CII 提供者強制規定有訂定資安維護計畫及通報應變的責任，包括中央目的事業主管機關之行政檢查及罰則執行等，雖於草案說明中多次引用日本《網路資訊安全基本法》第十五條第二項「政府為促進民間業者採取自發性措施，得採取必要措施」，本條應是著重協助及輔導，而非直接對 CIIP 提供者進行行政檢查與罰則。另亦引用歐盟 2016《網路與資訊系統安全指令》第二十一條，要求針對違反國家法規之行為制定有效罰則；但歐盟最新對 CIIP 檢討報告及最佳實務運作建議中，並未包括罰則部分，足見行政檢查及罰則並非 CIIP 之有效性及急迫性手段。而且草案中要求非公務機關部分之相關配套措施仍較為不足，至少應對 CIIP 提供者提供資安防護相關技術與制度建立之協助與輔導，並至少訂定一段過渡緩衝之日出條款（2 年後實施）等。

另有法界學者對於行政檢查提出疑義，諸多學者為文，認為本條抵觸諸多憲法原理原則，包括授權明確性、平等原則、比例原則等，條文中還有不少「不確定法律概念」，可能被行政權濫用等等，尤其，非公務機關的電腦機房，屬人民財產，卻賦予相關機關（包括地方政府），無須向法院申請搜索票，即可進入機房檢查資通安全設備，容有違憲之虞，甚至學者吳威志對其批評是「白色恐怖」復辟。行政院資通安全處對此僅回應說明：「行政檢查目的在協助組織釐清資通安全事件，或是阻止資通安全事件進一步擴大。為避免影響民間業者正常運作，對此訂定二項要件，因查核資通安全維護情形發現重大缺失，或發生重大資通安全事件時，必須符合二項要件之一，方可進入非公務機關執行檢查，同時，參與檢查人員也應負保密義務。倘若涉及犯罪並經報案，即由警調單位執行調查進入司法程序。」對此學者盧映潔所主張：「行政檢查程序倘無法於本法中為細部規範，亦應另訂專法明文規範為宜，而非全面授

權行政機關以法規命令決定，方合於法治國原則之基本要求。」⁵⁹

5、本法排除軍事機關及情報機關容待商榷

本法考量軍事機關及情報機關之性質特殊，認其資通安全管理宜由該等機關另行規定，故將「軍事機關及情報機關」排除於本法適用之外，此一立法政策是否正確，容待商榷。蓋其一，關於重要的法案，例如個人資料保護法、通訊保障及監察法等涉及重要法案，從未因「情報機關」具有特殊性而完全排除於適用之外，至多僅於特殊考量上予以例外規定；其二，本法已於第一條開宗明義謂係為「維護國家安全」而制定，殊難想像，竟將「國安（情報）機關」排除在外？情報機關包括甚廣，不僅有國家安全局、軍事情報局、電訊發展室、軍事安全總隊隊，且包括海岸巡防署、政治作戰局、憲兵指揮部、警政署、移民署及調查局等視同情報機關；甚至依《國家情報工作法》第十六條，國安局關於密碼管制（即同法第三條所稱之安全管制）與空間情報所統合指導之機關為各級「政府機關」，而這些機關所掌理者均屬涉及國家安全之重要資通安全，如將其排外適用，究竟將來這部法案還能維護多少國家安全，恐令人存疑？另外，國安會雖非「情報機關」，但其許多資訊系統均由國安局規劃、提供，且於實際作業上又與國安局密切往來，究竟其能否列入本法規範，將來豈非爭議。⁶⁰

⁵⁹ 「行政檢查」的部分，政府機關建議為：行政檢查作業面上，一來因無急迫危急人身安全，建議刪除警察陪同，改有危害才報警，另可增加遭遇大規模攻擊時，可尋求國軍支援的項目；民間團體建議為：不宜增加國軍介入的項目；學者建議為：行政檢查發動時機的合宜性需考慮；而行政院資安處 2017 年 4 月 27 日所確認之資料，對此卻未表示意見。但最後行政院的版本第 18 條則設仍設有「行政檢查」權，但無「警察陪同」及「國軍支援」之規定。吳威志，〈資通安全法 白色恐怖復辟〉，《中時電子報》，2017 年 11 月 7 日，<<http://opinion.chinatimes.com/20171107005674-262105>>（2017 年 12 月 4 日查詢）；盧映潔，〈盧映潔觀點：「資通安全管理法草案」之修正建議〉，《風傳媒》，2017 年 5 月 15 日，<<http://www.storm.mg/article/264648>>（2017 年 12 月 4 日查詢）。

⁶⁰ 呂啟元，〈掛羊頭賣狗肉的資通安全管理法〉，《國家政策研究基金會》，

陸、建議事項

從非傳統安全趨勢觀察，網路安全佔據地位角色日益重要，許多國際報告與非政府組織報告也一再警告政府與企業，資安風險對於國家安全與財產產生嚴重威脅，從分析各國網路安全政策上觀察，重點包括網路安全納入國家安全戰略一環、建立專責機關強化職權職能、關鍵基礎設施納入法律規範管理及建立通報因應機制強化公私合作等面向，而我國經歷政黨輪替後，在戰略面、組織通報機制面及法制面皆有朝國際重要國家網路安全政策學習方向，但現今在這三大面向上也產生包括戰略面面臨是否政策高度不足問題；組織通報機制面臨新組織架構磨合期、編制資安人力不足及情資分享平臺運作問題；而法制面則有整體國家安全與資通安全框架定位不明、未融入治理機制設計及強化公私協作夥伴關係、未強化網路危機管理機制與風險評鑑與管理及行政調查合法性問題，上述皆需經由政策執行時一一檢視，且需政府投入人力及資源補足缺陷，以下提出建議事項供參考：

（一）法制整合

目前國家安全納入資安不容疑義，而其中資安法制 CII 涉及到國土安全法制 CI，目前國土安全法制由行政院國土安全辦公室研擬國家關鍵基礎設施安全防護法草案，而資安檢查與保防措施有密切關連，此部份由法務部調查局研擬國家關鍵基礎設施安全防護法草案，目前國家關鍵基礎設施安全防護法草案、國家保防工作法草案立法進度較資通安全管理法草案落後，決策者可思考三法制整合工作，不只在專有名詞定義上的整合，在法制面的執行層面也可朝向整合，避免公務機關及非公務機關面臨三種行政檢查浪費時間及資源之困境。

2017 年 11 月 17 日，<<http://www.npf.org.tw/1/17709>>（2017 年 12 月 4 日查詢）。

（二）資源整合

依現行資安決策支援體系，行政院資安處囿於人力編制，渠部門業務著重在計畫、法制規劃督導上，屬於幕僚層，而其所屬行政院國家資通安全會報技術服務中心人員雖人力較為充足，但也是偏向幕僚層且不具備公務人員身分，在執行資安業務有其適法性問題。目前法務部調查局在與 CI 及重要企業進行交流宣導時多會強調資安業務，且多是站在協助角色，獲得不少贊同與肯定，在政府資安人力未補足前，建議運用法務部調查局資安人力進行資源整合配合推廣資安業務。

（三）公私整合

現行政府推動資安政策公部門整合已有初步成效，然與民間私部門整合仍遭遇窒礙，建議初期不要強調處罰面，對非公務機關及 CIIP 提供者提供資安防護相關技術與制度建立之協助與輔導，並至少訂定一段過渡緩衝之日出條款，藉由初期協助輔導與非公務機關建立良好互動關係，以公司治理角度，在互助、互惠及互利原則下，逐步落實建構資安領域的公私整合協力夥伴關係。

（收件：2017 年 11 月 1 日、第一次修正：2017 年 12 月 4 日、第二次修正：2017 年 12 月 12 日、接受：2017 年 12 月 15 日）

參考文獻

一、中文部分

(一) 專書

國家安全會議，2006。《2006 國家安全報告》，臺北：國家安全會議。

國家安全會議，2008。《2006 國家安全報告（2008 年修訂版）》，臺北：國家安全會議。

(二) 期刊論文

蘇柏毓，2015/6。〈資訊安全法規國際最新發展舉隅〉，《科技法律透析》，第 27 卷第 6 期，頁 28-29。

(三) 網際網路

2016/9/8。〈「資通安全管理法(草案)」民間團體座談會紀錄〉，《公共政策網絡參與平臺》，<<https://join.gov.tw/attachments/d1f218e5-e599-441a-95f6-a2a51c366669/download/1050908%E6%B0%91%E9%96%93%E5%9C%98%E9%AB%94%E5%BA%A7%E8%AB%87%E6%9C%83.odt>>。

2016/9/6 日。〈「資通安全管理法(草案)」政府機關座談會紀錄〉，《公共政策網絡參與平臺》，<<https://join.gov.tw/attachments/9a07113a-f916-4e61-8a33-5625e2805029/download/1050906%E6%94%BF%E5%BA%9C%E6%A9%9F%E9%97%9C%E5%BA%A7%E8%AB%87%E6%9C%83.odt>>。

2016/9/13。〈「資通安全管理法(草案)」學者專家座談會紀錄〉，《公共政策網絡參與平臺》，<<https://join.gov.tw/attachments/d5fbeat9-02ff-4fde-b34d-59f29f36987d/download/1050913%E5%AD%B8%E8%80%85%E5%B0%88%E5%AE%B6%E5%BA%A7%E8%AB%87%E6%9C%83.odt>>)。

- 2017/3/7。〈2016 年資訊安全總評：企業威脅刷新紀錄的一年〉，《趨勢科技》，<http://www.trendmicro.tw/cloud-content/tw/pdfs/security-intelligence/reports/trendlabs_2016_annual_information_security_review.pdf>。
- 2017/5/17。〈川普簽署網路安全行政命令則〉，《行政院國家資通安全會報技術服務中心》，<<https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=15956>>。
- 2017/9/12。〈今年上半年資安報告 勒索病毒等三大攻擊續增〉，《蘋果日報》，<<http://www.appledaily.com.tw/realtime/news/article/new/20170912/1202118/>>。
- 2016/7/24。〈政院資安處 8.1 掛牌 21 人成軍〉，《自由電子報》，<<http://news.ltn.com.tw/news/focus/paper/1014161>>。
- 2016/11/30。〈英國政府推動國家網路安全戰略〉，《行政院國家資通安全會報技術服務中心》，<<https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=15815>>。
- 2016/8/27。〈資安即國安 府院今明擴大資安會議〉，《自由電子報》，<<http://news.ltn.com.tw/news/politics/paper/1025776>>。
- 2017/4/27。〈資通安全管理法草案總說明〉，《行政院》，<http://www.ey.gov.tw/News_Content4.aspx?n=D0675BEBB0C613C7&sms=1B6A34286EEBCD4C&s=79472F6EDE25F136>。
- 2016/2/9。〈歐盟：1/4 歐洲人曾有網路安全問題〉，《科技新報》，<<https://technews.tw/2016/02/09/eurozone-internet-safety/>>。
- 2016/7/18。〈歐盟通過首個網路安全準則〉，《行政院國家資通安全會報技術服務中心》，<<https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=15667>>。

Vincent Chen, 2016/10/4。〈從歐盟資安運作法規與架構，談我國的資安法規課題〉，《火箭科技評論》，<<https://rocket.cafe/talks/79619>>。

王君瑋，2017/1/17。〈公部門資安人力短缺 資安處：短期內以約聘、委外方式處理〉，《風傳媒》，<<http://www.storm.mg/article/213972>>。

王家宜，2014/12/5。〈歐盟網路安全策略（Cybersecurity Strategy of the European Union）〉，《行政院國家資通安全會報技術服務中心》，<<https://www.nccst.nat.gov.tw/ArticlesDetail?lang=zh&seq=1361>>。

江飛宇，2016/7/10。〈北約秘書長強調網路戰爭的重要性〉，《中時電子報》，<<http://www.chinatimes.com/realtimenews/20160710003894-260417>>。

行政院國家資通安全會報，2017/8/31。〈「資通安全管理法草案」說明會會議紀錄〉，《行政院國家資通安全會報》，<http://www.nicst ey.gov.tw/News_Content.aspx?n=7D08312E0E5D8F33&sms=04631FAE19EA7CCA&s=BDF4D0DD8763E82C>。

行政院國家資通安全會報，2016/8/1。〈行政院國家資通安全會報組織架構〉，《行政院國家資通安全會報》，<<http://www.nicst ey.gov.tw/cp.aspx?n=F1FB6AFC30C728EC&s=FABA959E6E602DA3>>。

行政院國家資通安全會報，2014/2/25。〈我國重大資安政策進程〉，《行政院國家資通安全會報網站》，<http://www.nicst ey.gov.tw/News_Content3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF&s=1ACE1B808B9444DF>。

行政院新聞傳播處，2017/4/27。〈行政院會通過「資通安全管理法」草案〉，《行政院》，<<http://www.ey.gov.tw/>>。

News_Content.aspx?n=F8BAEBE9491FC830&s=26B446DFB5C87E70>。

吳威志，2017/11/7。〈資通安全法 白色恐怖復辟〉，《中時電子報》，<<http://opinion.chinatimes.com/20171107005674-262105>>。

呂紹玉，2016/2/16。〈視駭客為國家威脅！歐巴馬宣布 190 億美元的資安計畫〉，《科技新報》，<<https://technews.tw/2016/02/12/obama-unveils-19-billion-cybersecurity-plan/>>。

呂啟元，2017/11/7。〈掛羊頭賣狗肉的資通安全管理法〉，《國家政策研究基金會》，<<http://www.npf.org.tw/1/17709>>。

李欣芳，2017/4/27。〈防止駭客攻擊 政院端出國家首部資通安全法〉，《自由電子報》，<<http://news.ltn.com.tw/news/politics/breakingnews/2049801>>。

李欣芳，2017/1/17。〈建構國家資安 尚缺千餘人力〉，《自由電子報》，<<http://news.ltn.com.tw/news/focus/paper/1071736>>。

沈庭安，2016/7/19。〈日本要用 3 大資安對策迎戰 2020 奧運會〉，《iThome》，<<https://www.ithome.com.tw/news/110717>>。

林穎佑，2016/7/19。〈急起直追：日本的網安策略〉，《觀策站》，<<http://www.viewpointtaiwan.com/columnist/%E6%80%A5%E8%B5%B7%E7%9B%B4%E8%BF%BD%EF%BC%9A%E6%97%A5%E6%9C%AC%E7%9A%84%E7%B6%B2%E5%AE%89%E7%AD%96%E7%95%A5/>>。

崔敬熙，2017/6/2。〈反制網攻 北約擬集體防禦〉，《青年日報》，<<http://www.ydn.com.tw/News/238946>>）。

陳曉莉，2016/7/7。〈歐盟通過首個網路安全準則〉，《iThome》，<<https://www.ithome.com.tw/news/107004>>。

彭煒琳，2017/9/29。〈資安就是國安 蔡英文允諾投資資源發展產業〉，《中時電子報》，<<http://www.chinatimes.com/realtimenews/20170929003178-260407>>。

黃有容，2017/7/8。〈聯合國網路安全調查：新加坡資安第一、小型經濟體不俗〉，《匯流新聞網》，<<https://cnews.com.tw/%E8%81%AF%E5%90%88%E5%9C%8B%E7%B6%B2%E8%B7%AF%E5%AE%89%E5%85%A8%E8%AA%BF%E6%9F%A5%EF%BC%9A%E6%96%B0%E5%8A%A0%E5%9D%A1%E8%B3%87%E5%AE%89%E7%AC%AC%E4%B8%80%E3%80%81%E5%B0%8F%E5%9E%8B%E7%B6%93%E6%BF%9F/>>。

黃泓瑜，2017/8/7。〈卡巴斯基實驗室最新 DDoS 趨勢報告：勒索型 DDoS 攻擊越來越盛行〉，《iThome》，<<https://www.ithome.com.tw/news/116107>>。

黃彥桀，2016/5/4。〈立院通過廢止資安科技中心設置條例，贊成者：正確第一步，反對者：親痛仇快〉，《iThome》，<<https://www.ithome.com.tw/news/105714>>。

黃彥桀，2017/5/25。〈企業營運十大威脅出爐，前三大都得靠 IT〉，《iThome 網站》，<<https://www.ithome.com.tw/news/114440>>。

黃彥桀，2016/8/5。〈國安會資通安全辦公室正式成立，國發會管制考核處處長何全德接任主任一職〉，《iThome》，<<https://www.ithome.com.tw/news/107527>>。

黃彥桀，2017/3/16。〈國安會諮詢委員李德財：推動國家級資安戰略，捍衛數位國土安全〉，《iThome》，<<https://www.ithome.com.tw/news/109141>>。

黃彥桀，2016/10/10。〈產官學 3 方資安管理法建言大整理〉，《iThome》，<<https://www.ithome.com.tw/news/108920>>。

黃彥桀，〈新加坡大砸 40 億元推動國家級網路安全戰略〉，

- 《iThome》，2016 年 10 月 13 日，<<https://www.ithome.com.tw/news/109011>>。
- 黃彥棻，2016/10/19。〈新加坡用總理高度揭露國家資安戰略，臺灣呢？〉，《iThome》，<<https://www.ithome.com.tw/news/109141>>。
- 黃彥棻，2016/9/4。〈臺灣 TWCERT/CC 負責哪些資安任務？〉，《iThome》，<<https://www.ithome.com.tw/news/108002>>。
- 劉念祖，2017/9/25。〈政府與民間合力搭建資安通報應變與聯防機制〉，《Digitimes》，<http://www.digitimes.com.tw/tech/dt/n/shwnws.asp?id=0000513432_ZFQ3WGXN4YWZKE1E8ZTB8>。
- 盧映潔，2017/5/15。〈盧映潔觀點：「資通安全管理法草案」之修正建議〉，《風傳媒》，<<http://www.storm.mg/article/264648>>。
- 總統府，2016/12/1。〈資安就是國安 政府將不斷投入資源提升本土關鍵資安技術〉，《總統府》，<<http://www.president.gov.tw/NEWS/20926>>。
- 簡宏偉，2016/9/22。〈當前資安情勢與未來推動重點〉，《行政院》，<<http://www.ey.gov.tw/DL.ashx?u=%2FUpload%2FRelFile%2F19%2F741464%2F1ea97c3e-c045-4352-b500-dd9b7cc4fd97.pdf>>。
- 簡宏偉，2016/9/22。〈資通安全管理法與發展藍圖〉，《iThome》，<<http://s.ithome.com.tw/egov/2017/A-1320.pdf>>。
- 羅正漢，2017/3/17。〈從世界經濟論壇 2017 風險報告書，看企業與政府的資安防禦重點〉，《iThome》，<<https://www.ithome.com.tw/newstream/112847>>。

二、英文部分

Business Continuity Institute, 2017/2. “Horizon Scan Report 2017,” *BSI Website*, <<https://www.bsigroup.com/en-ZA/ISO-22301-Business-Continuity/Business-Continuity---Horizon-Scan-Report-2017/>>.

European Commission, 2013/2/7. “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” *European Commission Website*, <http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf>.

Kriz, Danielle, 2016/7/6. “Passage of EU NIS Directive Is a Milestone, But Next Steps Matter Even More,” *CSO Perspective Website*, <<https://researchcenter.paloaltonetworks.com/2016/07/passage-of-eu-nis-directive-is-a-milestone-but-next-steps-matter-even-more/>>.

Miles, Tom, 2017/7/5. “U.N. survey finds cybersecurity gaps everywhere except Singapore,” *Reuter Website*, <<https://www.reuters.com/article/us-cyber-un/u-n-survey-finds-cybersecurity-gaps-everywhere-except-singapore-idUSKBN19Q19L>>.

Stoltenberg, Jens, 2016/7/8. “NATO and Cyber: Time to Raise our Game,” *Defense News Website*, <<https://www.defensenews.com/smr/road-to-warsaw/2016/07/08/nato-and-cybertime-to-raise-our-game/>>.

US Department of Defense, 2011/7. “Department of Defense Strategy for Operating in Cyberspace,” *Department of Homeland Security Website*, <<https://www.hsdl.org/?view&did=489296>>.

White House, 2009/3. “Cyber Space Policy Review 2009,” *Department of Homeland Security Website*, <https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_

final_0.pdf>.

White House, 2011/5. “International Strategy for Cyberspace,” *White House Website*, <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

White House, 2013/2. “Executive Order 13636: Improving Critical Infrastructure Cybersecurity,” *White House Website*, <<https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>>.

White House, 2015/2. “Fact Sheet: The 2015 National Security Strategy,” *White House Website*, <https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf>.

White House, 2017/5/11. “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” *White House Website*, <<https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>>.

World Economic Forum, 2017/1. “The Global Risks Report 2017, 12th Edition,” *World Economic Forum Website*, <http://www3.weforum.org/docs/GRR17_Report_web.pdf>.