立法院法制局專題研究報告　　編號：1733

本報告僅供委員參考

因應量子科技發展之網路安全相關法制研析

法制局 陳育靖 撰

中華民國 113 年 11 月

因應量子科技發展之網路安全相關法制研析

目 次

摘　要

量子科技之發展將對產業發生重大變革，而聯合國認為該項科技亦將協助解決永續發展問題，並已將 2025 年定為「國際量子科技年」，世界先進國家除關注相關技術與應用之研究，並紛紛投入大量資源外，美國因觀察到量子運算技術可能帶來之網路安全問題，於 2016 年起進行後量子密碼標準建立，並陸續制定國家量子倡議法、量子運算網路安全準備法，於提升該國量子科技研發能量、取得該領域領導地位之同時，亦依據相關規定評估、規劃網路系統移轉至後量子密碼之時程；歐盟雖尚未制定相關法律，惟自 2018 年起陸續發布「歐洲量子技術旗艦計畫」及「歐洲量子技術宣言」，亦觀察到量子運算技術發展成熟後對網路安全之衝擊，提出「歐洲量子通訊基礎設施倡議」及「執委會關於移轉至後量子密碼之協調實施路徑圖建議」等，作為歐盟對量子科技發展之衝擊因應措施。

觀察我國目前針對量子科技，似僅關注技術面之研究發展，除欠缺整體規劃外，對於量子科技發展對於網路安全之衝擊，更缺乏相關因應措施與機制，本報告主要參考美國量子科技相關立法例，進而探討我國發展現況與問題，並提出法制方向建議，俾供本院委員問政及審查法案參考。

因應量子科技發展之網路安全相關法制研析

壹、前言

隨著人工智慧（Artificial Intelligence）之發展，量子力學（Quantum mechanics）、量子電腦（Quantum computer）、量子運算（Quantum computing）等領域亦成為科技界關注之焦點。量子力學除了是物理學之重要基礎外，其理論亦廣泛應用於各項領域並發展為多樣化之量子科技，早期各國多著重於促進該項科技之發展，近期則逐漸轉為關切量子科技可能產生之風險議題[1]。

美國早在本世紀初期即將量子電腦之相關研究列入國家科技戰略目標，在相關因應措施法制化方面，於 2018 年[2]美國國會通過國家量子倡議法（National Quantum Initiative Act）、2022 年美國國會通過量子運算網路安全準備法（Quantum Computing Cybersecurity Preparedness Act）[3]；歐盟於 2016 年依據荷蘭數位經濟與社會委員會主委及荷蘭經濟部長之倡議提出量子宣言（Quantum Manifesto），以因應第二次量子革命[4]，並依該宣言於 2018 年設定歐洲量子技術旗艦計畫（Quantum Technologies Flagship）[5]，嗣後並於 2023 年發布歐洲量子技術宣言（European Declaration on Quantum Technologies）、2024 年正式由歐盟成員國簽署量子公約（Quantum Pact），承諾共同合作推動歐洲成為世界量子谷（Quantum Valley）[6]；韓國則在 2014 年制定量子資通訊中長期戰略[7]，並在 2020 年

---

[1] 吳佳琳，淺論量子科技法制規範，科技法律透析，第 33 卷第 12 期，2021 年 12 月，頁 23。

[2] 本報告有關年分之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。

[3] 阮韻蒨，探析美國因應量子技術所生資安風險之政策發展，科技法律透析，第 35 卷第 3 期，2023 年 3 月，頁 42、44、47。

[4] European Commission, Quantum Manifesto for Quantum Technologies, Website：https://ec.europa.eu/futurium/en/content/quantum-manifesto-quantum-technologies.html, last visited at：2024.9.3。

[5] 科技產業資訊室，主要 16 國家量子科技政策 預算超過 246 億美元，2021 年 5 月 14 日，網址：https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=17799，最後瀏覽日期：113 年 9 月 3 日。

[6] 陳冠榮，推動歐洲轉型「量子谷」，歐盟成員國簽署量子公約，2024 年 3 月 25 日，網址：https://technews.tw/2024/03/25/eu-leaders-sign-declaration-on-quantum-technologies/，最後瀏覽日期：113 年 9 月 3 日。

[7] 黃品澤、尤俊皓，韓國國家量子科學技術戰略報導，2024 年 3 月 18 日，網址：https://qt.ntu.edu.tw/qoa/202403-korea-quantum-strategy/，最後瀏覽日期：113 年 9 月 3 日。

修正情報通信融合法（정보통신융합법）納入量子科技相關促進措施[8]，2023 年韓國科學技術情報通信部（Ministry of Science and ICT, MSIT）並發布「國家量子科學技術戰略計畫」，目標在 2035 年以前取得世界量子經濟主導權[9]；日本內閣府於 2020 年發布「量子技術創新戰略」，將該技術定位為未來 10 至 20 年國家戰略重要核心，於 2022 年重新修訂後，並區分技術及跨領域等面向，針對量子電腦、量子模擬、量子計算與感測、量子通訊與密碼等規劃路徑圖[10]；2024 年 6 月聯合國更作成一項決議，宣布 2025 年為「國際量子科技年」（International Year of Quantum Science and Technology, IYQST），聯合國認為，量子科技可能在氣候、能源等層面，對於達成聯合國 2030 永續發展目標提供新興解決方案，因此期望各國提升大眾對於量子科技之認識[11]。

我國之高科技產業位居全球領先地位，量子科技研究發展亦屬未來產業躍升之重要關鍵，國家科學及技術委員會（下稱國科會）於 110 年 9 月推動成立跨部會量子系統推動小組，期望自技術研發、國際鏈結、人才培育、產業參與等層面，全面推動我國量子科技發展[12]；而就法制層面部分，本院委員前於 109 年提出「量子科技研究及發展條例草案」，經院會一讀交教育及文化委員會審查[13]，惟因屆期不續審，未進一步完成立法。考量近期國際間針對量子科技相關法制已有所進展，爰擬參考外國立法例，探討相關法制問題並提出建議，俾供本院委員問政及審查法案之參考。

---

[8] 吳佳琳，同註 1，頁 24。

[9] 黃品澤、尤俊皓，同註 7。

[10] 經濟部台日產業合作推動辦公室，日本量子技術創新戰略路線圖(1)，2023 年 2 月 22 日，網址：https://www.tjpo.org.tw/NewsDetail.aspx?id=1096，最後瀏覽日期：113 年 10 月 21 日。

[11] UNESCO, International Year of Quantum Science and Technology, website：https://quantum2025.org/en/, last visit：Sep. 20, 2024.

[12] 量子系統推動小組，網址：https://www.quantumtaiwan.org/tw/modules/cadch/about，最後瀏覽日期：113 年 9 月 4 日。

[13] 立法院第 10 屆第 2 會期第 3 次會議立法院議案關係文書，院總第 1021 號委員提案第 25093 號，109 年 9 月 30 日印發。

貳、量子科技發展現況及影響

一、量子科技發展現況

（一）量子電腦

德國物理學家普朗克於 1900 年首次提出「能量量子化假說」，該假說認為所有物理實體皆可量子化，開啟第一次量子革命，迄 1980 年代止，電晶體、積體電路、雷射、LED 等皆係量子科技之應用成果；其後之第二次量子革命，則是結合資訊科技進一步發展量子通訊、量子計量感測器等新興應用[14]。

傳統電腦係由 0 及 1 組合而成一組訊息之二進制電腦，以電子訊號處理運算[15]，而費曼（Richard Feynman）於 1980 年代提出電腦以量子力學進行運算概念[16]。量子電腦係使用量子位元（Quantum Bit）進行運算，可同時表示 0 與 1 的多種可能組合，因此相較傳統電腦，可同時進行複雜且多元之運算[17]，由於其具備短時間內處理巨量資料之能力，因此就應用面而言，並非取代傳統電腦，而係用於製藥、機器學習、人工智慧等新興應用領域[18]。透過量子電腦運算模擬，將有助於大幅縮短新藥與疫苗開發時程，亦可取代目前機器學習需大規模使用 GPU 運算之缺點[19]。

（二）量子通訊

傳統上加密通訊技術係透過加密密鑰，由通訊之一方單向傳遞給

---

[14] 柴惠珍，量子運算技術的競賽與威脅，展望與探索，第 20 卷第 10 期，2022 年 10 月，頁 65、66。

[15] 劉江龍，量子計算對當代密碼系統之威脅及對策，前瞻科技與管理，9 卷 1/2 期，2019 年 11 月，頁 6。

[16] 李永悌，為量子網際網路預作準備，國防譯粹，第 49 卷第 8 期，2022 年 8 月，頁 5。

[17] 柴惠珍，同註 14，頁 66。

[18] 壽邇琪，下一世代運算工具-淺談量子電腦（Quantum Computer）（上），2022 年 9 月 16 日，網址：https://www.find.org.tw/index/tech_obser/browse/85207d3a92f8ce9dbce6349b56839f47/，最後瀏覽日期：113 年 9 月 4 日。

[19] 壽邇琪，下一世代運算工具-量子電腦（Quantum Computer）淺談（下）—潛力應用市場領域，2022 年 11 月 30 日，網址：https://www.find.org.tw/index/tech_obser/browse/c12263f48d1375a035e8e2b339106b9c/，最後瀏覽日期：113 年 9 月 4 日。

他方，透過此種雙方事先約定之加密、解密方式共享密鑰，以避免遭任意第三方破解[20]，惟量子電腦的出現，降低此種傳統加密方式之安全性；然而，量子科技同時也促進新型態加密通訊技術發展，藉由量子態的不確定性及不可複製性發展之「量子密鑰分發」（Quantum Key Distribution, QKD）技術，因為量子態於被測量時始會確定，倘若第三方以不正確方式測量，則會發生錯誤，從而使通訊雙方知悉有第三方介入，而不可複製性則可避免密鑰遭竊取；「量子隱形傳遞」（Quantum Teleportation）則係將一對具有量子糾纏態之量子由通訊雙方個別持有，當其中一個量子發生變化，另一方所持之量子亦將同時、瞬間發生變化，達成傳遞訊息之效果，此為運用量子糾纏原理之新型態通訊技術，論者認此種始為真正量子通訊[21]。

（三）後量子密碼

由於「量子密鑰分發」在功能面及技術成熟度的限制，在具體實踐上尚有困難[22]，為因應量子時代之加密需求，各國競相發展有助於對抗量子電腦之密碼，其中「後量子密碼」（Post-Quantum Cryptography, PQC）係以量子運算不擅長之數學領域為基礎進行密碼建構[23]。美國自 2016 年起由國家標準暨技術研究院（National Institute of Standards and Technology, NIST）提出 PQC 標準化計畫，透過全球性之公開競賽開發、甄選[24]。

二、量子科技發展之影響

（一）網路安全

---

[20] 陳繹安、廖家興，量子科技專利趨勢分析—量子通訊與後量子密碼，智慧財產權月刊，第 283 期，2022 年 7 月，頁 38。

[21] 柴惠珍，同註 14，頁 68、71-72。NEXT FORUM，精進量子密鑰分發技術，加速實現量子通訊未來，2022 年 12 月 31 日，網址：https://edge.aif.tw/hhri-221212-yuhrenn-wu/，最後瀏覽日期：113 年 9 月 19 日。

[22] 劉江龍，本局 113 年 10 月 18 日召開之「因應量子科技發展之網路安全相關法制研析」專題研究報告（初稿）座談會發言內容。

[23] 柴惠珍，同註 14，頁 68。

[24] 阮韻蒨，同註 3，頁 42、45。

各國爭相投入量子科技發展下，有論者認，2030 年全球即將進入量子時代，由於量子電腦之強大運算力將可輕易破解密碼、金鑰，將使現今所有需要使用密碼之系統（例如：網路銀行、電子商務等）面臨嚴重威脅[25]，雖然目前已針對後量子密碼進行加速研究，惟從目前加密方式進展到後量子密碼仍須有一段長達數年的過渡期，如何確保政府機關及各項產業得以及時、順利轉換至後量子密碼，是維護網路安全刻不容緩的問題[26]。

（二）個人隱私

由於量子電腦具有強大的破密能力，現行加密技術恐無法抵擋量子電腦之攻擊，因此將使得保有大量個人資料之政府機關、產業界面臨個人資料外洩之高度風險[27]。目前高度仰賴公鑰加密關鍵協定之金融與通訊產業，該公鑰主要在於提供身分驗證，具有量子技術能力之駭客可能可以透過偽造數位簽名，輕易存取大量銀行帳戶資料，此外，如比特幣、以太幣等以區塊鏈技術為基礎之數位資產，亦可能被駭客竊取[28]；尤其量子相關技術與人工智慧配合運用時，更將產生乘數效應，其影響非僅限於個人隱私資料外流，更可能因個人身分遭竊取而成為犯罪團體或恐怖主義者逃避追查之工具[29]。

參、美國因應量子科技發展之相關法制

美國政府於 2000 年即將量子電腦相關研究納入國家科技戰略目標，自 2016 年起由 NIST 提出 PQC 標準化計畫，該計畫迄今仍持續進行中[30]，為彰顯促進量子科技發展之決心，2018 年 12 月美國通過國家量子倡議

---

[25] 蘇純儀，量子時代預計 2030 年到來恐引發網路安全危機，2024 年 1 月 30 日，網址：https://www.digitimes.com.tw/tech/dt/n/shwnws.asp?CnlID=1&id=683630&query=%E9%87%8F%E5%AD%90，最後瀏覽日期：113 年 9 月 27 日。

[26] 林祉均，量子駭客防禦術：後量子密碼學的現在進行式，2023 年 6 月 9 日，網址：https://www.charmingscitech.nat.gov.tw/post/research10-pqc，最後瀏覽日期：113 年 9 月 30 日；劉江龍，同註 22。

[27] Anat Lior, A QUANTUM OF PRIVACY, March 19, 2024, Nevada Law Journal, Vol. 25, 2024, P. 15, SSRN：https://ssrn.com/abstract=4764111, last visited on Sept. 27, 2024.

[28] Anat Lior, *Supra* note, p.17.

[29] Anat Lior, *Supra* note 27.

[30] 阮韻蒨，同註 3，頁 42、45。

法，為因應量子運算可能帶來之網路安全問題，2022 年除頒布行政命令及「促進美國在量子運算領域之領導地位，同時降低密碼系統受攻擊風險之國家安全備忘錄」（National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems，下稱國家安全備忘錄），推動相關措施外[31]，同年 12 月並針對因應量子運算之網路安全相關事宜予以法制化，制定量子運算網路安全準備法[32]，相關法規範堪稱完備。爰就美國政府有關促進量子科技發展，及因應量子科技發展所涉網路安全相關法制作法說明如下：

一、國家量子倡議法[33]

2018 年 12 月 21 日美國國會通過國家量子倡議法，其目的在於透過支持量子科技之研發與應用、培訓與提升大學以上相關研發與教育人力、改善各聯邦機關間相關研發之協調合作、提升聯邦政府量子科技相關計畫之有效性、推動國際標準之制定等方式，確保美國在量子科技應用方面的持續領導地位[34]。

該法要求總統應提出「國家量子倡議計畫」（National Quantum Initiative Program，下稱倡議計畫），規劃未來 10 年美國推動量子科技之優先事項及進程[35]，並應設立以下機關或單位以推動相關工作：

（一）量子資訊科學次級委員會（Subcommittee on Quantum Information Science）[36]：

該次級委員會係在國家科學技術委員會（National Science and Technology Council）下，成員包括 NIST、國家科學基金（National

[31] 韓佳盈，美國推動量子運算技術，並維護網路安全發展，科技法律透析，第 34 卷第 9 期，2022 年 9 月，頁 9。
[32] 阮韻蒨，同註 3，頁 42。
[33] National Quantum Initiative Act, website：https://www.congress.gov/bill/115th-congress/house-bill/6227/text, last visited on Sept. 24, 2024.
[34] National Quantum Initiative Act Sec. 3.
[35] National Quantum Initiative Act Sec.101.
[36] National Quantum Initiative Act Sec.103

Science Foundation）、能源部、國防部、國家情報總監辦公室（Office of the Director of National Intelligence）、預算及管理辦公室（Office of Management and Budget, OMB）、科技政策辦公室（Office of Science and Technology Policy）及總統認為適當之聯邦政府機關等，該次級委員會主要工作為，確定倡議計畫之目標與優先事項、評估倡議計畫所需之基礎建設並提出建議、評估相關研發人力、評估國際發展趨勢、尋求國際合作機會等，並須於國家量子倡議法公布後 1 年內制定 5 年策略計畫，該法公布後 6 年內制定下一個 5 年策略計畫。

（二）國家量子倡議諮詢委員會（National Quantum Initiative Advisory Committee）[37]

該委員會成員係由總統指定具有量子科技研發、標準、教育、應用、國安等領域專業之產業界、學術界、聯邦實驗室等代表擔任，其主要任務在於向總統及次級委員會提出建議，並應定期、獨立地評估量子科技發展趨勢、倡議計畫之執行進度及其優先事項是否確有助於美國於量子科技之領導地位、倡議計畫是否需調整修正、及國家安全、社會、經濟、法規、人力等領域問題是否已確實為倡議計畫所涵蓋等事項。

（三）國家量子協調辦公室（National Quantum Coordination Office）[38]

提供「國家量子倡議諮詢委員會」相關技術及行政支援，負責聯邦政府各機關、地方政府、產學界間之協調聯繫工作，並監督倡議計畫之執行。

此外，依據國家量子倡議法，美國國家科學基金應提出量子資訊科學與工程之基礎研究及教育計畫，並透過捐助高等教育機構或非營利組織設立 2 個以上、不超過 5 個之多學科量子研究和教育中心（Multidisciplinary Centers for Quantum Research and Education），以辦理相關教育、培訓工作[39]；能源部應提出量子資訊科學研究計畫，並

[37] National Quantum Initiative Act Sec.104.
[38] National Quantum Initiative Act Sec.102.
[39] National Quantum Initiative Act Sec.302.

藉由公開競爭、績效審查等適當方式，於國家實驗室、高等教育機構或研究機構等之申請中，擇優設立 2 個以上、不超過 5 個之國家量子資訊科學研究中心（National Quantum Information Science Research Centers），以進行加速量子資訊科技突破之基礎性研究[40]。

二、因應量子科技發展之網路安全相關法制

（一）PQC 標準化計畫

為因應量子運算可能帶來之網路安全問題，NIST 於 2016 年提出 PQC 標準化計畫，該計畫係透過公開競爭方式，邀請全球之密碼學專家集思廣益，研發得以對抗量子運算之加密技術[41]，共有 25 個國家之專家計提交 82 個演算法方案，經多輪比較篩選後，2022 年 NIST 已提出 4 項候選方案，並再次對外徵求新方案[42]，2024 年 8 月 NIST 公布已完成 3 項得以因應量子運算威脅之加密演算法之標準化作業，分別是以加密金鑰封裝機制發展用於存取安全網站之「ML-KEM」、以點陣演算法機制發展用於通用數位簽章協議之「ML-DSA」，及以無狀態雜湊發展用於數位簽章之「SLH-DSA」，此亦為第一套針對量子運算風險管理之機制[43]。「ML-KEM」主要用於通用加密（General encryption），亦即保護於公共網路上交換之資訊，而「ML-DSA」及「SLH-DSA」則是用於身分認證之數位簽章，NIST 預計於 2024 年底將公布另一項標準，PQC 標準化計畫尚在持續進行中[44]。

---

[40] National Quantum Initiative Act Sec.402.

[41] 阮韻蒨，同註 3，頁 45。

[42] 羅正漢，NIST 正式發布 3 款 PQC 標準，鼓勵各界盡快轉換以因應量子破密威脅，2024 年 8 月 14 日，網址：https://www.ithome.com.tw/news/164456，最後瀏覽日期：113 年 9 月 24 日。

[43] 黃松勳，美國 NIST 發布後量子密碼標準 積極應對量子運算威脅，2024 年 8 月 15 日，網址：https://iknow.stpi.narl.org.tw/post/Read.aspx?PostID=21003，最後瀏覽日期：113 年 9 月 19 日。

[44] 羅正漢，同註 42。

（二）國家安全備忘錄[45]

2022 年 5 月 4 日美國總統簽署國家安全備忘錄，確立保持美國在量子運算及量子科技方面之競爭優勢，及減輕量子電腦對網路、經濟與國家安全風險之關鍵步驟，並導引相關機構採取具體行動，將易受攻擊之電腦系統轉移到後量子密碼。該備忘錄指出，由於密碼分析相關量子電腦（cryptanalytically relevant quantum computer, CRQC）具有破解美國及全世界數位系統所使用之多數公鑰密碼之可能性，倘若 CRQC 技術成熟，民用及軍事通訊系統、關鍵基礎設施之監督及控制系統，與大多數基於互聯網的金融交易安全協議皆可能遭受破壞[46]。備忘錄指出之主要作法如下：

1、提升美國在量子科技之領導地位

備忘錄指出，應將量子相關科技與網路安全原則納入各級學校課程，以培養更多量子科技相關領域科學家、工程師，並鼓勵量子科技及新興應用之研發。因此，於備忘錄發布日起 90 天內，資助量子電腦研究、開發或採購之機關應指定聯絡人與科學技術政策辦公室主任（Director of the Office of Science and Technology Policy）協調，以確保國家戰略之一致性，相關協調應依據國家量子促進法第 102 條(b)(3)及國防授權法（National Defense Authorization Act）第 6606 條規定辦理，並與業界、學界推動聯合研發計畫，簡化產業和政府間之技術轉移機制，及促進與海外盟友和合作夥伴的專業和學術合作[47]。

2、降低加密風險[48]

美國應以 2035 年以前盡可能減輕量子風險為目標，從政府到關

[45] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (hereinafter NSM), website：https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/, last visited on Sept. 23, 2024.

[46] NSM Sec 1.

[47] NSM Sec 2.

[48] MSN Sec 3.

鍵基礎設施、商業服務到雲端供應商，以及其他使用易受攻擊之公鑰加密技術者，優先考慮及時、公平地將密碼系統過渡到後量子密碼。

（1）針對非國安系統（non-National Security Systems, non-NSS）：

於備忘錄發布日起 90 天內，商務部及 NIST 應與業界共同成立工作小組，透過經驗分享協助 NIST 後續建立後量子密碼相關指引或標準，該小組並定期將工作成果提供 OMB、總統國家安全事務助理（Assistant to the President for National Security Affairs, APNSA）及國家網路主任（National Cyber Director），此外，商務部應透過 NIST 在國家網路安全卓越中心（National Cybersecurity Center of Excellence）建立「後量子密碼轉移計畫」（Migration to Post-Quantum Cryptography Project），與私部門合作開發程式，以發現與修復不使用後量子密碼或仍依賴易受攻擊系統之系統。

於備忘錄發布之日起 180 天內，OMB 應與網路與基礎建設安全局（Cybersecurity and Infrastructure Security Agency, CISA）、NIST、國家網路主任及 NSA 協商、清點所有當前之加密系統，包括關鍵資訊技術資產清單、過渡時期衡量基準（interim benchmarks）及用於評估 IT 系統中後量子加密轉移進度之通用（最好是自動化）評估流程，後續並每年提出相關評估報告。

（2）針對國安系統（National Security Systems, NSS）

於備忘錄發布之日起一年內，國家安全局經諮詢國防部與國家情報總監，應就國安系統之後量子密碼移轉、執行與監督提供技術指導，負責維運 NSS 者並應持續識別並記錄 NSS 使用量子脆弱（quantum-vulnerable）加密技術的所有情形，並向其管理機關報告；於後量子密碼標準發布後 180 天內，管理機關應定期發布 NSS 停用易受攻擊加密技術之官方時間表，而負責維運 NSS 者每年應提出 NSS 移轉計畫，包括時間表、權限、障礙、資金需求和例外情況。至 2023 年 12 月 31 日，負責維運 NSS 者應執行如：高保證網路協定加密器

（High Assurance Internet Protocol Encryptor）等措施，為易受量子攻擊的金鑰交換提供額外的保護；而國防部亦應向總統國家安全事務助理及 OMB 提交量子運算對國防工業基地與國防供應鏈的風險評估，以及與業界合作升級 IT 系統以實現量子抗性之計畫。

3、保護美國量子技術及智慧財產權[49]

為保護量子研發與相關智慧財產權，美國政府應採取相關保護機制（如：反情報措施、出口管制等），並對產業界與學術界推行有關網路犯罪和智慧財產權盜竊威脅之相關教育，如：合規性、內部威脅偵測和量子技術網路安全計畫之重要性等；聯邦執法機關亦應酌情調查並起訴參與竊取量子商業機密或違反美國出口管制法規之行為人。至 2022 年 12 月 31 日，資助量子電腦或量子科技相關研究、開發或取得該技術之機關（構）應制定全面的技術保護計畫，這些計畫應每年更新並提供給總統國家安全事務助理、OMB 及國家科學技術委員會量子科學經濟與安全影響次級委員會（National Science and Technology Council Subcommittee on Economic and Security Implications of Quantum Science）。

（三）量子運算網路安全準備法[50]

2022 年 12 月 21 日，美國國會通過量子運算網路安全準備法，該法說明密碼學對於美國國家安全與經濟運作至關重要，而目前最廣為使用之加密協定係仰賴傳統電腦之有限運算能力以提供網路安全，但考量量子電腦可能可以突破傳統電腦之運算限制，應防止美國之對手先竊取敏感的加密資料，並待量子電腦發展成熟之後予以解密（亦即資安用語中之「先竊取，後解密（harvest now, decrypt later）」）。因此，有關後量子密碼，政府及產業界應優先開發易於支援加密敏捷

[49] NSM Sec 4.
[50] Quantum Computing Cybersecurity Preparedness Act, Public Law 117–260 117th Congress, website：https://www.congress.gov/117/plaws/publ260/PLAW-117publ260.pdf, last visited on Sept. 24, 2024.

性[51]（cryptographic agility）之應用程式、硬體智慧財產及軟體[52]。相關重點如下：

1、建立資訊技術清單[53]

於該法頒布日起 180 日內，OMB、CISA 與國家網路主任應協調發布將資訊技術[54]移轉至後量子密碼之指引，該指引應包括應優先移轉至後量子密碼之資訊技術項目，建立易被量子電腦解碼之資訊技術清單，並評估其移轉流程。該清單及流程應於該法頒布後 1 年內提出，並定期維護、更新，評估方式以自動化為宜。

2、移轉與評估資訊技術[55]

於 NIST 發布後量子密碼標準後 1 年內，OMB 應發布指引，要求各機關（構）依據前述清單之優先性，訂定將資訊技術移轉至後量子密碼之計畫，OMB 並應確認該清單之優先順序已妥為評估，以確保資訊技術之互通性（interoperability）。

3、提出後量子密碼及資訊技術移轉報告

在該法頒布後 15 個月內，OMB 應與 CISA、國家網路主任諮商後，向參議院國土安全和政府事務委員會，及眾議院監督和改革委員會提交「後量子密碼報告」，內容應包括：因應量子電腦可能導致各機關（構）資訊技術加密弱化之風險的解決策略、防止該項風險之相關預算額度、及制定後量子密碼標準之時間表等[56]。

OMB 發布指引要求各機關（構）訂定資訊技術移轉計畫後 1 年，

---

[51] 加密敏捷性係指得以即時升級應用程式與系統所使用之加密演算法，以降低量子運算風險。參自資安人，Gartner 在資料安全成熟度曲線新增五大新技術，2023 年 9 月 4 日，網址：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10670，最後瀏覽日期：113 年 9 月 24 日。

[52] Quantum Computing Cybersecurity Preparedness Act Sec.2.

[53] Quantum Computing Cybersecurity Preparedness Act Sec.4(a).

[54] 依據 Quantum Computing Cybersecurity Preparedness Act Sec.5 規定，該法不適用於任何國家安全系統。

[55] Quantum Computing Cybersecurity Preparedness Act Sec.4(c)、(d).

[56] Quantum Computing Cybersecurity Preparedness Act Sec.4(e)(1).

至 NIST 發布後量子密碼標準 5 年內，OMB 應與 CISA、國家網路主任諮商後，向參議院國土安全和政府事務委員會，及眾議院監督和改革委員會提交各機關（構）資訊技術移轉至後量子密碼標準之進度報告[57]。

三、小結

觀察美國為提升其於量子科技領域之競爭力，並進一步取得領導地位，從促進量子科技發展之角度，制定國家量子倡議法為基礎架構，除由總統提出未來 10 年之計畫，並成立數個機關以協助跨部會協調、落實並監督該計畫之執行、及提供諮詢意見外，亦透過國家科技基金及能源部之補助計畫等方式，鼓勵高等教育機構、國家實驗室及非營利組織投入量子科技新興領域研發及人才培育與教育推廣工作；而針對量子科技發展下最迫切、最具風險之網路安全問題，美國於 2016 年即推動 PQC 標準化計畫，2022 年通過量子運算網路安全準備法，續於 2024 年率先提出具有對抗量子運算之加密演算法標準，並就政府系統移轉至後量子密碼時程提出具體規劃，皆有助於政府機關及產業界及早因應，避免因目前之加密技術未來輕易為量子電腦破解，造成機密資料或營業秘密大量外洩之困境，以期降低衝擊，相關作法皆值得我國參考。

肆、我國相關法制問題分析

一、對於量子科技未來發展欠缺整體戰略規劃

觀察國際間對於量子科技發展之影響已日趨重視，除美國已提出相關政策、法規，從促進量子科技發展及因應其所帶來之風險等角度進行規劃外，歐盟於 2018 年提出「量子技術旗艦計畫」，該計畫將歷時 10 年、預算 10 億歐元[58]，目前已開發出一款開放式超導量子電腦（Open Super Q Plus），並持續精進其效能，目標是在歐洲製造 1,000 量子位元運算之量

[57] Quantum Computing Cybersecurity Preparedness Act Sec.4(e)(2).

[58] European Commission, Shaping the Euro's digital future, Quantum Technologies Flagship, website：https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship, last visited on Sept. 25, 2024.

子電腦[59]，而 2023 年提出之「歐洲量子技術宣言」（European Declaration on Quantum Technologies），則宣示歐盟必須擁有自身之量子技術開發能力，從軟硬體、應用程式及標準等各層面均衡發展，避免非歐盟來源之量子科技戰略性依賴，創建歐盟主導之量子生態系，以鞏固歐盟之技術主權，因此，該宣言要求各成員國致力於量子科技相關之公共投資、新創企業扶植、技術人才培育、國際合作及趨勢觀測，並針對量子科技對於經濟、社會、加密技術等之影響進行研究，以利提出因應措施或方案[60]。

我國科技部（現為國科會）在 2018 年推動「量子電腦專案計畫」提供臺大、清大等學校開發團隊相關補助[61]，2020 年提出「量子科技專案計畫」，透過公開徵求國內研究團隊方式，期望整合量子技術科研人才與資源，針對當前量子科技軟硬體核心技術瓶頸，開發具突破性之關鍵技術[62]，並在 2022 年 3 月宣布成立「量子國家隊」，預計於 2022 年至 2026 年投入新臺幣 80 億元，針對「通用量子電腦硬體技術」、「光量子技術」及「量子軟體技術與應用開發」等三大領域進行研究[63]，數位發展部成立後，亦將後量子密碼之相關領域納入量子國家隊。因我國量體較小，因此於科技戰略上係採取「小國大戰略」模式，期望透過掌握關鍵技術，於未來供應鏈等層面取得關鍵地位，並營造健全產業生態系。

觀察我國目前作法，主要係由主管機關透過專案計畫補助量子技術研究、開發之方式，並無整體因應量子科技發展之國家戰略，包括量子科技對政府機關及產業界各種網路系統可能造成之風險、量子科技相關產業、教育、研發等人才培育之整體規劃、量子科技對於國家安全、經濟、社會之衝擊與因應機制等皆付之闕如，更遑論如同美國透過法制化

---

[59] OpenSuperQPlus, Open Superconducting Quantum Computers, website：https://opensuperqplus.eu/, last visited on Sept. 25, 2024.

[60] European Commission, Shaping the Euro's digital future, European Declaration on Quantum Technologies, Dec. 6, 2023, website：https://digital-strategy.ec.europa.eu/en/library/european-declaration-quantum-technologies, last visited on Sept. 25, 2024.

[61] 羅正漢，量子國家隊成軍，17 項團隊底定，聚焦未來量子世代臺灣產業鏈，2022 年 3 月 22 日，網址：https://www.ithome.com.tw/news/150015，最後瀏覽日期：113 年 9 月 25 日。

[62] 110 年 9 月 2 日科技部科部自字第 1100055541 號函之科技部「量子科技專案計畫」徵求公告。

[63] 羅正漢，同註 61。

方式將相關機制予以明文規定，量子科技技術研發固然重要，但忽略相關風險之評估、控管與因應，恐將導致重大危機，如何透過整體戰略規劃，以引導發展方向至關重要。

二、現行網路系統如何移轉至後量子密碼尚待明確指引、規劃

考量量子電腦技術成熟後，現行加密技術恐將被迅速破解，美國於2016 年著手發展後量子密碼等加密演算法，近期已提出 3 項加密演算法標準供政府機關、產學界等轉換、運用，2022 年並陸續提出國家安全備忘錄、通過量子運算網路安全準備法，內容包括各主管機關應負責之事項、預算、盤點並排定系統移轉優先次序、建立定期評估進度與調修優先順序機制等，針對政府機關之系統移轉至後量子密碼為具體規範。2024 年 7 月白宮依據量子運算網路安全準備法規定，公布「後量子密碼時代報告」（Report on Post-Quantum Cryptography），提出將相關系統移轉至後量子密碼之 4 項原則[64]：

（一）持續盤點、識別使用公鑰加密之資料或系統，於完成移轉至後量子密碼前，透過自動加密技術持續進行加密。

（二）目前駭客已有朝向「先竊取、後解密」之攻擊加密資料趨勢，因此在 CRQC 投入運作前，即須進行移轉至後量子密碼之動作。

（三）應將會受到高度衝擊之資訊系統（High impact information systems）、機關具有高度價值之資產（Agency high value assets）、至 2035 年仍具有高度敏感性之資料或基於非對稱加密的邏輯存取控制系統（如公鑰）等機關認為極可能遭受 CRQC 攻擊之系統優先移轉後量子密碼。

（四）及早盤點、識別無法支援後量子密碼之系統，並將該系統之軟體或硬體進行優化，以利移轉至後量子密碼。

[64] White House, 2024.7, website：https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf, last visited on：Sept. 27, 2024.

上述相關工作既多且繁雜，因此依據該報告評估，2025 年至 2035 年辦理移轉至後量子密碼相關工作至少需 71 億美元之經費[65]。

歐盟針對量子科技可能導致之網路安全問題，除了在 2019 年提出「歐洲量子通訊基礎設施倡議」（Euro Quantum Communication Infrastructure initiative），由歐洲太空總署（European Space Agency, ESA）與各成員國合作開發、部署，期望透過整合光纖、衛星及以量子為基礎之系統，建構跨越整個歐盟之安全量子通訊基礎設施外[66]，針對後量子密碼部分，歐盟於 2024 年 4 月 11 日發布「執委會關於移轉至後量子密碼之協調實施路徑圖建議」（Commission Recommendation on a coordinated implementation roadmap for the transition to post-quantum cryptography，下稱路徑圖建議），依據該路徑圖建議，網路安全於數位世界具有戰略重要性，完善之加密技術為資料與隱私保護、交易安全、數位系統維護防禦之關鍵，為此，歐盟刻正由網路安全局（European Union Agency for Cybersecurity, ENISA）及網路安全專家評估與選擇歐盟之後量子密碼標準，並建議各成員國成立包含國家安全、網路安全及產業界相關專家之小組，蒐集有關後量子密碼關鍵基礎設施與轉型之意見，以制定各成員國之後量子密碼轉換策略，該應定義明確之目標、里程碑和時間表，以符合歐盟共同之路徑圖。為了有效過渡到後量子密碼，路徑圖應提供成員國要採取的行動清單，包括為後量子密碼演算法之不同階段制定明確的時間表、里程碑、所涉及之利害關係人，及其相互間之影響。路徑圖應在該建議書發布 2 年後提出，後續歐盟將依據該路徑圖調整各成員國之後量子密碼過渡計畫，並與各成員國代表定期評估各國之作法，確認進度及各項措施之效果，據以評估是否須制定聯盟層級法律[67]。

---

[65] White House, *supra* note.

[66] European Commission, Shaping the Euro's digital future, The European Quantum Communication Infrastructure (EuroQCI) Initiative, website：https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci, last visited on Sept. 25, 2024.

[67] European Commission, Shaping the Euro's digital future, April 11, 2024, website：https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography, last visited on Sept. 26, 2024.

美歐各國於數年前已關注後量子密碼對於網路安全可能造成之衝擊，並制定相關法規、訂定計畫、確立策略及時程，以資因應。我國目前雖有關於後量子密碼之相關研究，惟未見政府機關針對相關系統盤點、識別及移轉至後量子密碼之時程等規劃，更遑論編列相關預算及制定相關法規。因應後量子密碼尚待建立指引規範及規劃原則方向，主管機關有必要參考外國經驗及立法例進行制度性的整體作法規劃。

伍、結論與建議

一、為促進量子科技發展，建議研提國家整體戰略

我國科技業目前雖位居全球領先地位，惟觀察世界各先進國家無不積極發展量子科技，我國雖已陸續推動「量子電腦專案計畫」、「量子科技專案計畫」，近期並宣布「量子國家隊」成形，惟皆僅限於國科會單一部會層級，從國際作法觀之，促進量子科技發展，應自國家整體戰略層面進行思考，從國安、經濟、社會、教育、財政、金融、甚至犯罪防制領域，全方位盤點、檢視，並進行跨部會之協調合作，爰建議應由行政院統籌研提促進量子科技發展之國家整體戰略，並由各相關部會提出細部計畫，先行確立上位政策後再向下推展。

二、建議研議制定促進量子科技發展專法之可行性

因應量子科技發展，美國設立「量子資訊科學次級委員會」、「國家量子倡議諮詢委員會」、「國家量子協調辦公室」等諮詢、協調、計畫進度管控機制，並要求國家科學基金與能源部至少應設立 2 個相關研究機構，以推動相關人才之培育及技術研發，相關機制建立與機構設立，皆須明定其任務、職掌，並配合相關預算支應，2018 年美國國會通過之國家量子倡議法即為相關機制提供法制基礎，查本院委員於 109 年即提出「量子科技研究及發展條例草案」[68]，亦係考量美國及歐盟於 2018 年即陸續提出相關法規與計畫，惟該草案僅經一讀會交教育及文化委員會審

[68] 立法院議案關係文書，同註 13。

查[69]，而主管機關並未提出相關草案。為利促進我國量子科技發展，強化相關人才培育及技術研發，並透過租稅優惠、獎勵或其他獎、補助規定，提升產業投入具前瞻性技術及產學合作開發該項技術之意願，[70]爰建議主管機關儘速研議制定促進量子科技發展專法之可行性。

三、建議促進量子科技發展專法主管機關由國科會擔任，數位發展部及經濟部皆應於專法中承擔一定任務

依國科會組織法第 2 條規定略以：「本會掌理下列事項：一、國家科學發展、技術研究與應用政策之綜合規劃、協調、審議及資源分配。二、國家科學發展、技術研究與應用計畫之綜合規劃、協調、審議、資源分配及管理考核。三、基礎及應用科技研究之推動。四、重大科技研發計畫及支援學術研究之推動。五、產業前瞻技術研發與學研新創政策之綜合規劃、協調及推動。.....」；又，數位發展部組織法第 2 條規定略以：「本部掌理下列事項：一、國家數位發展政策之規劃、協調、推動、審議與法規之擬訂及執行。.....三、數位科技應用與創新發展環境之建構及人才培育。.....五、國家資通安全政策、法規、重大計畫與資源分配等相關事項之擬訂、指導及監督。六、政府數位服務.....之策略規劃、協調、推動及資源分配。七、數位基礎建設之整體規劃、推動及管理，相關工程技術規範、系統及設備審驗法規之訂定。八、數位發展之國際交流及合作相關事項。.....」;復依經濟部產業發展署組織法第 2 條規定：「本署掌理下列事項：一、產業發展政策規劃及法規研擬。二、產業管理、輔導、監督、協調及統籌配合。三、產業創新、研發、改善、行銷與推廣之獎勵、補助及輔導。四、產業永續、減碳調適、環境改善、產業安全衛生、資源循環與再生及工廠管理之輔導。五、軍、公、民工業配合與工業動員研議及協調。六、產業合作及投資。七、產業人才培訓。八、其他有關產業發展事項。」，考量量子科技發展所涉事項不僅包含國

[69] 立法院公報，第 109 卷，第 56 期，頁 17。

[70] 臺灣大學物理系（及量子系統推動小組計畫經理）高英哲教授於本局 113 年 10 月 18 日「因應量子科技發展之網路安全相關法制研析」專題研究報告（初稿）座談會意見。

家科學發展、技術研究與應用、產學前瞻技術研究及政策推動層面，量子科技之未來應用更涉及整體數位發展、數位科技應用、產業發展、資通安全，量子網路之建構亦為數位基礎建設及政府數位服務之重要一環，爰建議未來制定專法之主管機關為國科會，惟數位發展部及經濟部（產業發展署）亦應於專法中承擔一定任務，以發揮量子科技發展之整體成效。

四、加強全民資安意識，並研擬因應對策以避免「先竊取、後解密」之風險

以往駭客針對難以解密之資料可能興趣缺缺，或讓相關系統管理人員心存僥倖心理，認為即便資料被竊取，資料亦難以解密，可維持一定之資料安全性，惟隨著量子科技發展，可能使目前難以解密之資料被瞬間破解，因此亦產生「先竊取、後解密」之新興模式，恐將使未來駭客入侵系統竊取資料之情形更為頻繁，系統及資料外洩風險亦將大幅提升，因此除應全面加強全民資安意識，以了解量子科技可能帶來之新興風險外，亦應研擬適當因應措施，以避免「先竊取、後解密」之風險。

五、建議全面檢視資通安全管理法，將量子科技之衝擊納入考量

由於量子破密所產生之衝擊亟須整體資通安全政策規劃，依資通安全管理法（下稱資安法）第 10 條規定：「公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。」，同法第 16 條第 1 項及第 2 項規定：「中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知受核定者。（第一項）關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。（第二項）」因此，我國各級政府機關及經指定之特定非公務機關，皆應依照資安法規定辦理，符合所屬資通安全責任

等級要求，並依所保有或處理之資訊情形，訂定、修正及實施資通安全維護計畫。隨量子科技之發展，勢必對於資通訊安全造成嚴重影響，現行資安法相關法制是否足以因應量子科技所帶來之衝擊，建議主管機關應全面檢視及評估修法必要性或強化法制規範。

六、建議研議制定因應量子科技網路安全整備法案之可行性

考量量子科技將大幅度衝擊網路安全及個人隱私，就政府機關部分，應積極就系統移轉至後量子密碼進行規劃，此外，我國產業多數為中小企業，恐難以自行識別、評估、因應量子科技所帶來之影響，並進而將系統移轉至後量子密碼，爰建議研議制定因應量子科技網路安全整備法案之可行性，明定由主管機關提出評估要項，以受衝擊程度劃分整備等級、因應措施，就各級政府機關排定期程，識別衝擊程度、評估移轉優先順序並依期程完成移轉；針對非政府機關部分，則由各產業之中央目的事業主管機關，依據主管機關所定評估要項，協助業管產業識別可能受到之衝擊，並依據各該整備等級協助擬定因應措施；此外，為提升量能，明定主管機關應整合產官學研之資源，提供主管機關、各中央目的事業主管機關、各級政府機關及產業界相關協助。

參考文獻

一、政府出版品

1. 立法院公報，第 109 卷，第 56 期。
2. 立法院第 10 屆第 2 會期第 3 次會議立法院議案關係文書，院總第 1021 號委員提案第 25093 號，109 年 9 月 30 日印發。
3. 科技部 110 年 9 月 2 日科部自字第 1100055541 號函。

二、期刊

1. 吳佳琳，淺論量子科技法制規範，科技法律透析，第 33 卷第 12 期，2021 年 12 月，頁 23-28。
2. 李永悌，為量子網際網路預作準備，國防譯粹，第 49 卷第 8 期，2022 年 8 月，頁 5-15。
3. 阮韻蒨，探析美國因應量子技術所生資安風險之政策發展，科技法律透析，第 35 卷第 3 期，2023 年 3 月，頁 42-49。
4. 柴惠珍，量子運算技術的競賽與威脅，展望與探索，第 20 卷第 10 期，2022 年 10 月，頁 65-75。
5. 劉江龍，量子計算對當代密碼系統之威脅及對策，前瞻科技與管理，9 卷 1/2 期，2019 年 11 月，頁 4-21。
6. 陳繹安、廖家興，量子科技專利趨勢分析—量子通訊與後量子密碼，智慧財產權月刊，第 283 期，2022 年 7 月，頁 34-59。
7. 韓佳盈，美國推動量子運算技術，並維護網路安全發展，科技法律透析，第 34 卷第 9 期，2022 年 9 月，頁 9-10。

三、其他中文網站資料

1. NEXT FORUM，精進量子密鑰分發技術，加速實現量子通訊未來，2022 年 12 月 31 日，網址：https://edge.aif.tw/hhri-221212-yuhrenn-wu/。
2. 林祉均，量子駭客防禦術：後量子密碼學的現在進行式，2023 年 6 月 9 日，網址：https://www.charmingscitech.nat.gov.tw/post/research10-pqc。

3. 科技產業資訊室，主要 16 國家量子科技政策 預算超過 246 億美元，2021 年 5 月 14 日，網址：https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=17799。
4. 量子系統推動小組，網址：https://www.quantumtaiwan.org/tw/modules/cadch/about。
5. 黃品澤、尤俊皓，韓國國家量子科學技術戰略報導，2024 年 3 月 18 日，網址：https://qt.ntu.edu.tw/qoa/202403-korea-quantum-strategy/。
6. 黃松勳，美國 NIST 發布後量子密碼標準 積極應對量子運算威脅，2024 年 8 月 15 日，網址：https://iknow.stpi.narl.org.tw/post/Read.aspx?PostID=21003。
7. 經濟部台日產業合作推動辦公室，日本量子技術創新戰略路線圖(1)，2023 年 2 月 22 日，網址：https://www.tjpo.org.tw/NewsDetail.aspx?id=1096。
8. 資安人，Gartner 在資料安全成熟度曲線新增五大新技術，2023 年 9 月 4 日，網址：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10670。
9. 陳冠榮，推動歐洲轉型「量子谷」，歐盟成員國簽署量子公約，2024 年 3 月 25 日，網址：https://technews.tw/2024/03/25/eu-leaders-sign-declaration-on-quantum-technologies/。
10. 羅正漢，量子國家隊成軍，17 項團隊底定，聚焦未來量子世代臺灣產業鏈，2022 年 3 月 22 日，網址：https://www.ithome.com.tw/news/150015。
11. 羅正漢，NIST 正式發布 3 款 PQC 標準，鼓勵各界盡快轉換以因應量子破密威脅，2024 年 8 月 14 日，網址：https://www.ithome.com.tw/news/164456。
12. 蘇純儀，量子時代預計 2030 年到來恐引發網路安全危機，2024 年 1 月 30 日，網址：https://www.digitimes.com.tw/tech/dt/n/shwnws.asp?CnlID=1&id=683630&query=%E9%87%8F%E5%AD%90。
13. 壽邇琪，下一世代運算工具-淺談量子電腦（Quantum Computer）

（上），2022 年 9 月 16 日，網址：https://www.find.org.tw/index/tech_obser/browse/85207d3a92f8ce9dbce6349b56839f47/。

14. 壽邇琪，下一世代運算工具-量子電腦（Quantum Computer）淺談（下）—潛力應用市場領域，2022 年 11 月 30 日，網址：https://www.find.org.tw/index/tech_obser/browse/c12263f48d1375a035e8e2b339106b9c/。

六、外文網站資料

1. Anat Lior, A QUANTUM OF PRIVACY, March 19, 2024, Nevada Law Journal, Vol. 25, 2024, P.15, SSRN：https://ssrn.com/abstract=4764111.
2. European Commission, European Declaration on Quantum Technologies, Dec. 6, 2023, website：https://digital-strategy.ec.europa.eu/en/library/european-declaration-quantum-technologies.
3. European Commission, Quantum Technologies Flagship, website：https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship.
4. European Commission, Quantum Manifesto for Quantum Technologies, website：https://ec.europa.eu/futurium/en/content/quantum-manifesto-quantum-technologies.html
5. European Commission, Shaping the Euro’s digital future, April 11, 2024, website：https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.
6. European Commission, The European Quantum Communication Infrastructure (EuroQCI) Initiative, website：https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.
7. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, website：https://www.whitehouse.gov/briefing

-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

8. National Quantum Initiative Act, website：https://www.congress.gov/bill/115th-congress/house-bill/6227/text。
9. OpenSuperQPlus, Open Superconducting Quantum Computers, website：https://opensuperqplus.eu.
10. Quantum Computing Cybersecurity Preparedness Act, Public Law 117－260 117th Congress, website：https://www.congress.gov/117/plaws/publ260/PLAW-117publ260.pdf.
11. UNESCO, International Year of Quantum Science and Technology, website：https://quantum2025.org/en.
12. White House, July 2024, website： https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf.

附錄：「因應量子科技發展之網路安全相關法制研析」專題研究報告（初稿）座談會紀錄及參採情形

時間：113 年 10 月 18 日（星期五）上午 10 時

地點：立法院法制局 304 會議室

主席：翁組長栢萱　　紀錄：陳育靖

參加人員：

一、學者專家

國防大學理工學院　劉教授江龍

二、國家科學及技術委員會

副處長　陳小玲

博士　劉芳君

臺灣大學物理系　高教授英哲（量子系統推動小組計畫經理）

三、數位發展部

科長　何垂芬

四、本局出席人員

郭研究員憲鐘

曾副研究員耀民

楊助理研究員蕙如

發言要點：

國防大學理工學院劉教授江龍：

一、從 2016 年迄今，量子科技大幅進步，以往許多無法解決的計算上難題，有希望透過量子運算來解決，為人類帶來了新的希望。但由於可破解量子脆弱（quantum-vulnerable）密碼的量子演算法的存在，

也對現有運作中的公鑰密碼系統的安全造成嚴重的威脅，這也是為何美國 NIST 在 2016 年會提出制定後量子密碼學（PQC）標準的原因。而後續美國對後量子密碼遷移的種種措施，也是針對現有支持網路安全的公鑰密碼系統而制定。由於相關法案的規範，這些措施均依照規定的時間執行，也被嚴格監督及考核。另外在歐洲及亞洲許多先進國家，也已有相關措施正在進行。反觀國內，並無相對應解決量子脆弱密碼遷移法案，這也是本研究報告撰擬的原因之一。因此，本研究報告主旨相當具有前瞻性，個人對報告內容所提到的國內相關法案立法的建議也相當支持。

二、從 2016 年 IBM 發表 5 位元量子電腦後，許多民間團體紛紛對「密碼學相關量子電腦（CRQC）」備便的日期（也稱為 Q-day）進行估測，本文中則引用其中一個對 2030 年 Q-day 的估測，個人對此則保持比較樂觀的看法。原因是，美國政府將 2025 至 2035 年作為後量子密碼遷移的時程，依據資安風險管理中的 XYZ 定理，若將資料保值期（X）設為 10 年，加上 10 年遷移時間（Y），則 Q-day 的時間點必須落在 2045 年以後。從這個角度來看，對現有密碼系統應該沒有立即的威脅。但若對手採用「先獲得、後解密（harvest now, decrypt later）」策略，則密碼遷移晚一天做，資料就存在早一天被破解的風險。這點對網路平台提供者比較不嚴重，因為他們知道如果比別人早一天進行密碼遷移，就比別人多了許多競爭優勢，例如 IBM 在 PQC 標準發布後，就宣布其所經營的網路平台已經 quantum ready 了；可是對依法辦事的公部門來說，必須要有相關法條或行政命令規範，才能啟動密碼遷移或新的系統建置。以新的採購案為例，若採購設備中牽涉到密碼模組的建置，如果沒有密碼遷移或密碼敏捷（cryptographic agility）相關法條的規範，未來採購後可能又要花一大筆經費進行系統升級，這是一個很嚴重的問題。基於上述考量，及早立法對後量子密碼遷移及密碼敏捷性進行規範，實在有其必要性跟急迫性。

三、本報告內容結構完整，文獻蒐集相當豐富，是個人第一次看到國內

針對量子科技法案的研析報告。為讓這份報告更臻完美，以下從密碼學專業的角度上提供個人幾點建議，作為承辦單位後續修正之參考，其中包括 2 點觀念修正建議及 5 點文字修正建議：

（一）第 4 頁，（三）後量子密碼段落中提到「由於『量子密鑰分發』在具體實現上有其限制性，主因在於目前尚無完全可信任的量子中繼器可擔負遠距離傳遞，於實際部署上將產生困難」，個人認為並非完全是各國進行後量子密碼遷移的原因，其中還牽涉到「量子密鑰分發」與現有網路安全協定界接的問題，建議修正為「由於『量子密鑰分發』在功能面及技術成熟度的限制」，在語意上會比較完善。

（二）第 5 頁，（二）個人隱私段落的最後一句：「但是相對而言，量子科技亦可成為隱私保護之利器，各國刻正發展之 PQC 演算法標準，即為以量子加密對抗量子解密之技術」，這句話是對 PQC 的誤解。PQC 不是基於量子理論所發展的密碼技術，反而是傳統的公鑰密碼技術，因其演算法結構不是量子計算擅長的領域，所以可以抵抗量子計算的攻擊，建請斟酌修正。

（三）第 5 頁，第一段的最後一句：「如何確保政府機關及各項產業得以及時、順利轉換至後量子密碼，將對網路安全造成劇烈影響」，這句話語意上有點問題，建議修正為「如何確保政府機關及各項產業得以及時、順利轉換至後量子密碼，是維護網路安全刻不容緩的問題」，由於這句話是引述別的文獻，建議再對照原文進行合理的修正。

（四）第 10 頁，（2）針對國安系統段落的第一句：「...負責維運 NSS 者並應持續識別並記錄 NSS 使用量子脆弱加密技術的所有情形，並向其管理機關報告」，其中「量子脆弱」這個名詞來自於 quantum-vulnerable 這個英文，指的是無法抵抗量子計算攻擊的密碼演算法，同時是 quantum-safe 的反意，因是文中第一次使用，應標英文名稱，如可標示出處更佳。

（五）第 11 頁，（三）量子運算網路安全準備法，第一段：「...應防止美

國之對手先竊取敏感的加密資料，並待量子電腦發展成熟之後予以解密」，這句話對應到一句資安上專有的攻擊名詞：harvest now, decrypt later，在本文中翻成「先竊取，後解密」，建議在這句話後面加以註解，以作為後文出現之「先竊取、後解密」參考的來源（共 12 處，分別在第 15 及 18 頁）。

（六）第 15 頁，「（三）應將具有高度影響之資訊系統（High impact information systems）、機關具有高度價值之資產...」這句話建議修正為「（三）應將會受到高度衝擊之資訊系統（High impact information systems）、機關具有高度價值之資產...」，較符合語意。

（七）第 18 頁，第四項：『加強全民資安意識，並研擬因應對策，以避免「先竊取、後解密」之風險』，因與法制無關，建議併入第 19 頁中的第六項，統一說明與建議。

參採情形：

一、第一點及第二點意見，係贊同本報告研提建議。

二、第三點意見（一）至（六），已參採修正；第三點意見（七）部分，考量第 19 頁之第六項係建議主管機關研議制定量子科技網路安全整備法之可行性，該可行性研議應涉及較具廣度、深度之整體性評估、分析，惟現階段為儘速避免「先竊取、後解密」之風險，仍宜先行針對強化資安意識部分研擬對策，二者仍有順序上之差異，爰錄供參考。

量子促進推動小組高教授英哲：

一、量子科技與後量子密碼學應分開觀察，後量子密碼學係指因應量子科技發展後傳統電腦應如何防護之作法，目前應可以開始著手處理。

二、我國量子研究量能尚且不足，倘若以法令限縮方向，以台積電而言，若當時成立時，國家即限制其發展方向，恐怕無法發展成為現今之台積電。本報告以美國為例，惟美國為科技大國，全球合計之研究量能恐怕都無法與之匹敵，尤其量子科技部分，該國更結合公部門

及私部門之研究量能，甚且部分科技進展皆係如 IBM、Google 等私人公司以其資金進行研究，因此無法將美國架構直接套入我國，參考歐盟亦僅有倡議，並未發展專法，之前立法委員提出之專法亦係以倡議為主，倘若於目前做相關規範，對於臺灣之科研而言將是危險的，但針對資安與後量子密碼部分則是一定要進行處理的。

三、目前推動量子科技發展之困難點在於產業意願較低，例如有新技術發展出來後，需要投入產學合作開發，但產業卻不願意投入具有前瞻性之技術，倘若可以租稅優惠、獎勵，或國家認為是重點產業需要投入相關資源等，可能可鼓勵產業投入，因此建議可將經濟部列入相關機關。

參採情形：

一、第一點意見，係贊同本報告研提建議。

二、第二點意見，本報告針對量子科技發展建議研議制定專法之可行性，該專法係以「促進發展」為目的，針對培育相關人才、探究國際趨勢及尋求國際合作機會等，透過法規制定賦予法源依據，亦可納入獎、補助及租稅優惠等規定，以推動量子科技之發展量能，其目的並非限制或設定量子科技發展方向。

三、第三點意見，已參採修正。

國家科學及技術委員會陳副處長小玲：

一、新興科技之特色是日新月異，因此推動之策略初期多是以技術研發與人才培育為主，後續才會朝向產業發展進行推動，產業看到商機就會自動投入發展，間接讓社會大眾了解新興科技可能帶來之影響。因此於技術發展階段較不建議以法規限制其各種發展之可能性。

二、戰略不等同規劃與法規，例如過去 AI 之發展並無相關法規，而是以相關策略推動，畢竟法規制定需時較長，倘若其間技術方向產生新變革，就可能導致須修改法規，過去對於新興科技通常皆採取先行

投入，而非法規先行。臺灣科技戰略及量體與美國有極大差異，美國期望於量子科技中處於領導地位，而我國即便將 1,000 餘億之科技預算全數投入量子科技亦與美國有極大落差，因此我國係採取「小國大戰略」，掌握關鍵技術，期望於未來供應鏈等層面具有關鍵地位，並於發展過程中營造健全生態，結合政府、企業與法人等力量共同推動，避免只有少數產業得到科技發展之好處，量子科技相關策略之研擬亦係經過專家學者、業界、中研院及經濟部等相關部會之參與、討論，而非僅由本會推動。量子國家隊係期望打造上、中、下游之整合研發模式，數位部成立後更將後量子密碼部分納入，使整個團隊戰力更為完整。因此於考慮技術布局時，亦已考量日後對於產業可能造成之影響，以「以終為始」之概念設計技術布局。因此我國已有相關戰略，惟模式較偏向歐盟，期望營造較完整之產業模式，不同於美國以法規等形式呈現。因此，之前除了赴歐盟參訪外，近日亦邀請法國等歐盟學者來臺參與研討會。

三、關於法制建議部分，後量子密碼雖係因應量子科技產生，惟其研發方向及可能影響之產業後續發展皆有所不同，本報告亦有將促進量子科技發展及後量子密碼二者做區分，惟量子科技尚在發展階段，較不建議以法制限制之。且新興科技日新月異且種類繁多，從半導體、5G 到 AI 等，難以就每項科技之發展皆制定專法。

四、關於資訊安全部分，112 年 12 月行政院公告「國家核心關鍵技術項目及其主管機關」，已納入後量子密碼保護技術，並由數位部主政。

參採情形：

一、第一點意見，同量子促進推動小組高教授英哲意見參採情形二。

二、第二點及第三點意見，本報告以參考美國法制為主，係因其整體法規較為完備，至於法規如何設計，自應配合我國國情及現況調整，並非全數移植，且正因我國量子科技量能不足，以專法方式將應投入之資源、人才培育、獎補助及租稅優惠等規定予以明定，亦將有

助於整體產業及量能之提升，爰錄供參考。另，第二點意見有關於我國科技戰略及量子國家隊之進展，已參採修正。

三、第四點意見，依據國科會 113 年 3 月 26 日科會前字第 1130020363 號函對於本院張雅琳委員之口頭質詢答覆，「國家核心關鍵技術項目及其主管機關」係行政院依據國家安全法（下稱國安法）第 3 條第 4 項授權訂定之國家核心關鍵技術項目認定辦法公告，惟查國安法第 3 條認定「國家核心關鍵技術」之目的，係為防止該技術之營業秘密外流，因此，雖該項技術清單已納入後量子密碼，但與本報告所建議之內容尚有落差，爰錄供參考。

數位發展部何科長垂芬：

一、倘若國科會傾向訂專法，則本部將協助檢視資通安全管理法（下稱資安法）相關部分；而就資安法部分，目前已有資安維護計畫及例行演練，因每天皆有上千甚至上萬則網路攻擊，倘若日後量子技術成熟，或相關機制已建立完成後，亦可將其納入日常攻防演練。

二、本報告似乎對於國內情況著墨較少，例如何種情況會涉及後量子密碼、哪些產業會有大量儲存機密文件、是否有財力可購置量子電腦加以破解、擁有者是否為百大企業或政府機關（構）等，倘若引入國外法制，宜敘明國外法制運用情境、該情境是否會發生於國內，仍應考量法規範目的及國內產業或技術成熟情形。

參採情形：

一、第一點意見，因量子科技之發展，國際間已警示將出現「先竊取，後解密」之趨勢，在此情形下，駭客攻擊之強度與頻率只可能較以往更盛，資安風險亦將大幅提高，現行資安法規範是否充足？現有之資安維護計畫及例行演練是否足以因應？建議主管機關應及早檢視並研擬對策，而非待量子技術成熟始進行研議，爰錄供參考。

二、第二點意見，涉及實際產業界之相關資訊蒐集與調查，主管機關應

本於權責進行了解，或洽請產業主管機關協助，至於量子科技發展將造成現有密碼體系迅速遭破解已為共識，本報告已舉出美國、歐盟高度關注該風險並積極研擬因應對策之事例，本次座談會專家學者亦認儘速投入轉移至後量子密碼之研議極具重要性，爰錄供參考。

郭研究員憲鐘：

一、本報告係以量子科技發展所造成「網路安全」為研析主題。報告中提及美國因觀察到量子運算技術可能帶來之網路安全問題，於 2016 年起進行後量子密碼標準，並通過「量子運算網路安全準備法」。另提及我國目前針對量子科技，似僅關注技術面之研究發展，對於量子科技發展對於網路安全之衝擊，缺乏相關因應措施與機制，恐將產生「先竊取、後解密」之新興資安問題云云...。爰此，本報告之伍、結論與建議一至三，似宜參酌美國「量子運算網路安全準備法」立法例，建議應聚焦於量子科技發展後，如何因應其對網路安全威脅。

二、本報告建議「專法」主管機關由國科會擔任，數位發展部並應於專法中承擔一定任務。據本報告說明，美國為提升該國量子科技研發能量，防範量子運算技術可能帶來之網路安全問題，於 2016 年起分別制定「國家量子倡議法」及「量子運算網路安全準備法」。前者制定目的在於透過支持量子科技之研發與應用、培訓等方式，確保美國在量子科技應用方面的持續領導地位。後者制定目的則強調如何因應量子科技發展，提供網路安全對於美國國家安全的重要性。查我國於 111 年 8 月 27 日成立「數位發展部」，並責由所轄「數位發展部資通安全署」職司國家資通安全之防護。爰此，建議「專法」之主管機關宜就「專法」之制定目的及所定法定事務性質定之，允為妥適。

參採情形：

一、第一點意見，本報告主題雖係針對因應量子科技發展之網路安全，惟量子科技發展之國家整體戰略規劃，亦須考量量子脆弱所帶來的

影響，又因我國量子科技發展無論在相關人才培育或產業發展上皆有量能不足之虞，倘若未先提升量能，對於後續可能產生之網路安全風險與危機是否有充足能力因應尚有疑慮，因此，促進量子科技發展與因應相關網路安全問題應屬一體兩面，爰錄供參考。

二、第二點意見，有關建議「專法」主管機關由國科會擔任，數位發展部並應於專法中承擔一定任務部分，該專法係指「促進量子科技發展專法」，為避免誤解，已參採修正。至於涉及網路安全部分之相關法制，自應由職司國家資通安全政策規劃、計畫核議及督導考核，執行國家資通安全防護、演練與稽核業務及通訊傳播基礎設施防護之主管機關主責。

曾副研究員耀民：

一、本報告首次提到 OMB 於第 6 頁。OMB 是美國總統行政辦公室之一，是美國總統維持對聯邦政府財政計畫控制的機關。本報告譯為預算及管理辦公室（Office of Management and Budget, OMB），後來又出現至少 4 次，分別於第 10 頁、第 11 頁及第 12 頁等，建議將中英文說明置於首次出現之處（第 6 頁）。

二、有關本報告結論與建議第 5 項「建議全面檢視資通安全管理法，將量子科技之衝擊納入考量」，應屬可資贊同，惟其內容論述可再詳盡說明。其中，引述資通安全管理法第 10 條（規定內容略以，公務機關應考量其所屬資通安全責任等級之要求，及保有或處理之資訊種類等條件，訂定、修正及實施資通安全維護計畫。）及第 16 條（規定內容略以，關鍵基礎設施提供者，應訂定、修正及實施資通安全維護計畫。）之規定。本報告對於第 16 條僅引述第 1 項，建議宜進一步引用第 2 項規定：「關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。」如此，能夠較明確地指出，公務機關資通安全管理與特定非公務機關資通安全管理，兩者對於皆有資通安全維護計畫，均須因

應量子科技發展，對於資通訊安全造成之嚴重影響。

三、量子計算的發展為網路安全帶來潛在的重大威脅。傳統的加密方法將很難保護資料，量子計算機能夠利用的演算法，使目前使用的加密技術變得脆弱。量子科技的快速發展需被持續監控，以便及早發現潛在風險。我國應建立量子技術研究與網路安全部門之間的合作機制，確保網路安全系統能即時更新應對未來可能的量子計算威脅。總而言之，隨著量子計算技術的成熟，網路安全架構必須採取積極行動，轉型至抗量子技術並完善安全監控機制，以應對量子科技帶來的挑戰。

參採情形：

一、第一點及第二點意見，已參採修正。

二、第三點意見，係贊同本報告研提建議。

楊助理研究員蕙如：

一、本報告研析意見及建議三「建議專法主管機關由國科會擔任，數位發展部並應於專法中承擔一定任務」之建議方向符合我國目前之發展。本報告雖未明言數位部之任務，惟究數位發展部組織法，數位發展部之任務應以數位基礎建設之整體規劃、資通安全之維護及資安事件發生時之通報機制為主。然由量子科技之新興技術特性，其專法之制定除了「管制」（regulation）外，亦需有相關法令「解除管制」（deregulation）（或稱法規鬆綁）及鼓勵研發等獎、補助之配合，以鼓勵國內企業投入量子科技之研發及商品化，爰建議職司「產業創新、研發、改善、行銷與推廣之獎勵、補助及輔導」之經濟部（產業發展署[71]）亦於專法中承擔一定任務。

---

[71] 本署（經濟部產業發展署）服務範疇
一、產業發展政策規劃及法規研擬。
二、產業管理、輔導、監督、協調及統籌配合。
三、產業創新、研發、改善、行銷與推廣之獎勵、補助及輔導。
四、產業永續、減碳調適、環境改善、產業安全衛生、資源循環與再生及工廠管理之輔導。

二、本報告主要篇幅為美國自 2000 年以來因應量子科技發展之相關法制及發展歷程，內容詳盡具參考價值；另以 2018 年提出「量子技術旗艦計畫」帶出歐盟近年之作法。由於美國掌握極大之經費及先進科技優勢量能超越世界上其他所有國家資源之總和，其做法具指標意義。各國雖難以望其項背，仍試圖做出努力，例如韓國科學技術情報通信部（Ministry of Science and ICT, MSIT），於 2023 年 6 月的國家量子科學技術戰略計畫，發布未來 15 年內投資約 22.5 億美元於量子技術，目標成為全球前 5 名的領導者。而韓國也致力於培訓量子技術專家。同時，韓國眾多龍頭企業，如三星、LG、SK Telecom 等亦積極將量子技術應用於其業務領域；日本 2020 年 1 月日本內閣府發布量子技術創新戰略，將量子技術定位為未來 10 至 20 年國家核心重要技術，近期並對特定量子產品實施出口管制。日本政府預算在 2023 年、2024 年分別投入 777 億及 421 億日圓用於量子相關技術之投資，並於 2023 年 3 月推出日本首台量子電腦。鑑於與我國之文化及社會結構較為接近的日、韓展現對未來量子運算的積極度及作法，值得我國借鏡參考。若能在報告註釋適度補充日、韓鄰國對量子科技之國家策略，將有助於讀者對本新興科技議題之瞭解。

三、本報告所提其他意見，敬表贊同。

參採情形：

一、第一點及第二點意見，已參採修正。

二、第三點意見，係贊同本報告研提建議。

散會：上午 11 時 30 分

五、軍、公、民工業配合與工業動員研議及協調。
六、產業合作及投資。
七、產業人才培訓。
八、其他有關產業發展事項。詳參：經濟部產業發展署簡介，網址：https://www.ida.gov.tw/ctlr?PRO=intro.rwd01&lang=0，最後瀏覽日期：113 年 10 月 18 日。