調　查　報　告

壹、案　　由：據悉，美國眾議院議長裴洛西訪問我國期間，我國各級政府及民間企業之網站、電子看板相繼遭到駭客入侵，以阻斷服務、竄改網站內容、刊登不實資訊等方式，進行心理及認知作戰。我國資訊產業發達，政府及民間之資訊設備卻頻遭駭客攻擊入侵。究政府及民間企業有否正視網路攻擊之威脅，並建立有效之資安防護能力？如何避免網站及電子看板等公眾媒體遭駭客利用，成為錯假訊息公布欄，致影響民眾認知？政府對於心理及認知作戰是否採取具體之因應措施？均認有調查之必要案。

貳、調查意見：

本案經調閱數位發展部（下稱數位部）、國防部、經濟部、內政部警政署(下稱警政署)、法務部調查局(下稱調查局)等機關卷證資料，於民國(下同)112年2月16日辦理專家學者諮詢會議，嗣於111年2月22日現場履勘數位部等機關人員，並於112年5月17日詢問數位部、經濟部、內政部、調查局及國防部主管人員，已調查完畢，茲臚列調查意見如下：

一、資通安全法及其子法目前僅能規範公務機關及特定非公務機關於事前、事中及事後相關法遵事宜，搭配個人資料保護法於112年5月16日修正通過提高罰則以及金融監督管理委員會對上市櫃公司相關規定，雖可一定程度督促公私部門加強資安治理，惟尚難有效推動可能有重大資安風險並危及民眾安全之私部門建立事前風控或事中通報機制，此有數位部未能掌握美國

裴洛西議長訪臺期間公私部門資安事件全貌，以及無法提供部分個案細節，僅能不斷鼓勵宣導加入台灣電腦網路危機處理暨協調中心(Taiwan Computer Emergency Response Team / Coordination Center，TWCERT/CC)可資佐證；爰此，主管機關數位部宜在堅守法律保留原則之前提下，參考先進國家政策，導入先進資安概念，聽取私部門需求，以強化公私協力措施，研謀建立事前風控取代事後調查及裁罰。

(一)資通安全管理法(下稱資安法)管理範疇及個人資料保護法(下稱個資法)修正概要如下 ,就資安法部分，其管理範疇包括「公務機關」及「特定非公務機關」，不含私部門；個資法部分僅能就個資洩漏事後依法進行行政檢查及裁罰，尚難處理電子看板內容竄改或服務癱瘓等非屬個資範疇之資安風險。

1、資安法管理範疇

（1）第3條第1項第5款規定:「公務機關：指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關。」

（2）第3條第1項第6款規定:「特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。」

（3）第7條第1項規定：「主管機關應衡酌公務機關及特定非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級;其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由主管機關定之」;同條第2項規定:「主管機關得稽核特定非公務機關之資通安全維

護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由主管機關定之」；同條第3項規定：「特定非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向主管機關提出改善報告，並送中央目的事業主管機關」。

（4）第2章及第3章並分別訂定「公務機關資通安全管理」及「特定非公務機關資通安全管理」相關規定。

2、個資法修法概要。

（1）對私部門進行行政檢查之依據

〈1〉第22條第1項規定:「中央目的事業主管機關或直轄市、縣（市）政府.....認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查.....。」

〈2〉「行政院及所屬各機關落實個人資料保護聯繫」作業要點總說明第1點至第11點。

（2）摘述依據立法院院總第20號政府提案第10034077號，行政院函請審議「個人資料保護法第一條之一、第四十八條及第五十六條條文修正草案」立法總說明。

〈1〉近期非公務機關保有個人資料外洩事件，不僅社會大眾高度關注，.....屆期未改正時始能處以行政裁罰，且裁罰額度過低，其處罰方式及管制效果不足，.....有必要賦予主管機關依違法情節行使裁罰權限。

〈2〉修正非公務機關違反第27條第1項或未依第2項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法之裁罰方式，並提

高罰鍰數額,及增訂違規情節重大者之罰則。

〈3〉如違反情節重大者，處15萬元以上1,500萬元以下罰鍰，屆期未改善者，得按次開罰15萬元以上1,500萬元以下罰鍰。

(二)次據金融監督管理委員會證卷期貨局(下稱金管會證期局)亦於111年2月6日「推動上市（櫃）公司及證券商資通安全管理強化措施」新聞稿內容節錄如下：「已督導證交所及櫃買中心組成資安相關跨部門任務型專案小組，並完成「公開發行公司年報應行記載事項準則」、「公開發行公司建立內部控制制度處理準則」、「上市上櫃公司資通安全管控指引」、「建立證券商資通安全檢查機制」等相關法規修正及指引，提醒上市(櫃)公司及證券商自111年起應依相關規定辦理」，其具體內容包括:

1、上市（櫃）公司應於股東會年報中敘明資通安全政策、具體管理方案及投入資通安全管理之資源等資訊。

2、如遇發生重大資通安全事件，應即時發布重大訊息說明發生緣由、可能損失、改善情形及因應措施，並於損失達一定金額以上時，召開重大訊息記者會對外說明，及於股東會年報中揭露所遭受之損失、可能影響、因應措施等資訊。

3、要求證券商若發生重大資安事件，應依規定進行通報及循F-ISAC(Financial Information Sharing and Analysis Center，金融資安資訊分享與分析中心)情資分享管理辦法分享資安情資。

(三)次依iThome網站調查，國內企業過去一年內有8成遭遇資安事件，2成更遭遇50件以上資安事件，情

勢不可謂不嚴峻；按資安法設計架構，完整之資通安全管理制度(Information Security Management System ，ISMS)應包括事前風險識別及保護控制、事中通報應變，以及事後鑑識和復原；又以Sounil Yu[1]提出著名之網路防禦矩陣(Cyber Defense Matrix)如下表，橫軸依序分別為識別、保護、偵測、回應及復原，涵納完整之資安防護所應涵蓋之面向，倘作為本案檢視公私部門防護完整性之基準，則顯示我國目前於私部門之資安事前風險識別及保護控制，尚欠有效之行政指導。

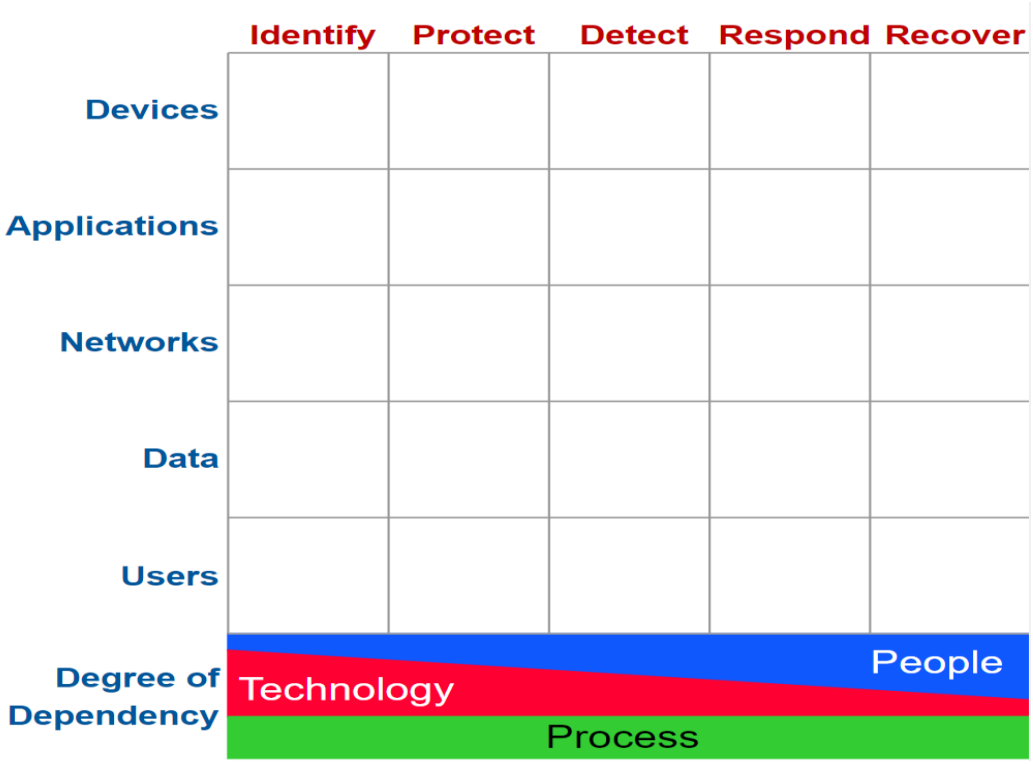

圖1 Sounil Yu 提出著名之網路防禦矩陣(Cyber Defense Matrix)，同時亦為美國國家標準與技術研究所（NIST）提出之網路安全框架Cybersecurity Framework（CSF）重要內容。

[1] Sounil Yu，美國銀行前首席資安專家，Jupiter One首席資安長兼研究主管，所提出著名之網路防禦矩陣(Cyber Defense Matrix)，同時亦為美國國家標準與技術研究所（NIST）提出之網路安全框架Cybersecurity Framework（CSF）重要內容。

(四)次查，主管機關數位部對於裴洛西議長訪臺期間及近期國內資安情勢之掌握及研判如下。

1、數位部說明裴洛西議長訪問期間資安事件樣態主要為以下2種，首先為阻斷服務(DDoS)，即以大量流量造成對外服務緩慢或停止服務，以8月2日為例，政府骨幹網路(GSN)攻擊總量為過去23倍；其次為非法入侵，包括服務內容遭置換，例如：網站頁面、電子看板等

2、官方受駭侵相關細部資料（如機關名、頻率、強度及樣態）經本院兩度函詢，數位部均查復因敏感或涉及相關偵測防禦機制與防禦能量佈署資料，無法提供，惟補充說明該期間(111年8月1日至8月19日)通報之資安事件皆已完成應處及結報作業。

3、私部門受駭侵情形，本院請該部提供所掌握民間遭遇各類型資安威脅之頻率、強度及樣態，該部亦稱無相關資料。

4、此外針對該期間之指標性事件，如屬公部門之臺鐵新左營車站電子看板內容遭竄改一案，數位部僅說明依法通報並進行後續損害控制及復原作業，至於私部門之統一超商電子看板內容遭置換一案，本院請數位部提供駭客攻擊手法，數位部表示無相關資料，該案亦無主動通報TWCERT/CC。

(五)再查，主管機關對於資通安全公私協力方面之辦理情形及現況，數位部則說明：

1、針對非屬資安法管理對象之民間資安事件，目前通報、應處或援助之機制：

(1)臺灣電腦網路危機處理暨協調中心(TWCERT/CC)為我國企業資安事件通報及協處窗口，提供企

業資安事件諮詢及協調協處服務。其通報方式包含：線上通報、電語通報及E-mail 通報。

（2）TWCERT/CC 除接受企業資安事件通報協處外，亦接受產品資安漏洞通報，提供惡意檔案檢測服務及舉辦資安推廣宣導活動等。

（3）警察局及法務部調查局亦有提供報案窗口，提供資安事件受害通報及協處服務。

2、除TWCERT/CC之外，公私協力機制尚包括公部門之N-ISAC及私部門之CISO資安長聯盟。數位部說明如下：

（1）N-ISAC透過情資格式標準化與系統自動化之分享機制，提升情資分享之即時性、正確性及完整性，建立縱向與橫向跨領域之資安威脅與訊息交流，達到情資迅速整合、即時分享及有效應用之目的。

（2）N-ISAC會員包含領域管理、應變聯防（包含TWCERT/CC）、執法機關、監控服務及技術支援等不同類型會員，以有效進行資安情資分享。

（3）數位部另查復，CISO係為促進我國各產業資安主管之資訊安全技術應用與經驗交流、培育資安專業人才、法規遵從，提升臺灣產業資安韌性，促使企業永續發展。惟無從得知數位部與CISO之間有何具體合作。

(六)再查，基於資安威脅日益嚴峻且不分公私領域，先進國家已開始加以重視，此有「美國2023國家網路安全戰略」[2]，以及美國前國土安全部部長Janet

[2] 2023 national cyber security strategy，2023年3月2日由美國白宮發布，中文說明參考經濟部國貿局。(https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/)

Napolitano於2023臺灣資安大會(CyberSec 2023)演講內容可資佐證。

1、美國2023年「國家網路安全戰略」涉及公私協力部分：

（1）僅靠市場力量不足以保護消費者與國家，將以法律方式讓銷售缺乏網路安全技術的軟體公司負起相關法律責任，以及制定更廣泛網路安全法規框架以保護美國關鍵基礎設施。

（2）主要優先事項包括敦促私部門進行更多合作及威脅情報分享、建立國際夥伴關係以制定網路規範、聯邦技術現代化，並強調需要使用進攻性網路能力，以破壞及消除對美國網路的威脅。

（3）所有服務供應商都必須合理的努力，以避免其基礎設施受濫用或其他犯罪行為的影響。

2、美國前國土安全部部長Janet Napolitano於2023臺灣資安大會表示，當年國土安全部（Department of Homeland Security，DHS）在全美推廣的“See Something Say Something”（一看到、就通報）活動為例，通報可疑的人事物可以降低實體社會面臨的風險，也同樣適用於網路環境，Janet Napolitano認為，即便無法降低網路威脅，也可以減輕這些威脅帶來的風險。

(七)對此，資安署鄭欣明副署長於本院112年5月17日辦理約詢時表示，目前法令(指資安法)確實未納管私部門，茲節錄約詢內容如下；

1、有關企業承包很多政府標案部分，有些積極的企業會主動通報，但是有些公司知道A機關有漏洞，卻不跟有相同漏洞的B機關通報。

2、我們還在想如何比較強制的讓供應鏈廠商揭露，

目前沒有適當的工具。

3、目前要比較大、社會比較矚目的案件，行政院會要求各部會作協處，數位部督導資安院做行政檢查，我們目前規劃跟金管會相互溝通，要求上市櫃公司發布重訊和財報揭露資安等等。

4、我們剛從RSA大會[3]回來，顯示**現在趨勢是認為每個單位、每個人都有責任**，今年底我們會辦資安月，來提升民眾的資安意識，全民資安意識提高讓全民負責，或許是一個可行的辦法。

(八)綜前，數位部堅守法律保留原則雖值肯認，惟目前處理私部門資安事件，僅可仰賴宣導及事後行政檢查或裁罰，不僅事前風控措施之行政指導及管理有待加強，亦不利整體資安情勢研判及政策方向擬定；進行行政檢查之要件也未臻明確，易衍生「選擇性辦案」之爭議，此外相關案件均請資安院協助調查，對該院其他重要資安業務亦有排擠之虞；則如何透過公私協力補強私部門事前風控漏洞，實有賴主管機關數位部與相關部會合作，研謀具體有效之方法。

二、有關裴洛西議長訪臺期間公私部門資安事件樣態，主要可歸納為分散式阻斷服務攻擊(DDoS)及電子看板內容竄改，行政院資通安全會報及相關機關雖陸續頒布如強化網站韌性、「危害國家資通安全產品限制使用原則」清查汰換、「營業場域電子看板資通安全管理指引」，「招牌廣告（電視牆、電腦顯示板）資通安全

[3] RSA Conference 資安大會：RSA大會始於31年前，當時是為RSA客戶舉辦的使用者大會。RSA 是由公司三位聯合創辦人姓氏Ron Rivest、Adi Shamir 和 Leonard Adleman的縮寫而來，目前是全球活動和全年線上網路安全內容的主要提供商。RSA大會是世界談論安全、領袖聚集、進步的場域。使命是促進全球網路安全專業人士就當前和未來的擔憂、想法和解決方案進行對話。

管理指引」等各項措施，惟經查相關橫向協調、追蹤落實及釐訂防護邊界等項目仍有檢討改進空間，行政院資通安全會報、數位部、經濟部及內政部應秉持「資安是持續精進的風險管理」之精神，持續加以積極管理，以儘可能降低類案再生之風險。

(一)由於數位部對於裴洛西議長訪臺期間公私部門資安事件無全盤掌握，本院自行依據iThome網站於111年8月12日發表新聞[4]綜整，裴洛西議長訪問期間資安事件(不含爭議訊息)總覽如下，合計13筆，與政府部門直接相關者占10筆，以阻斷服務及內容置換為主：

1、111年8月2日：

（1）總統府證實網站遭DDoS攻擊。

（2）政府入口網站、外交部網站傳出因遭DDoS攻擊而無法存取，外交部指出網站收到每分鐘多達850萬筆請求。

（3）國防部、外交部及桃園國際機場的網站，疑似遭到DDoS攻擊。

2、111年8月3日：

（1）7-11櫃檯後方數位看板的內容遭置換，刑事局調查指出是遭駭客入侵。

（2）台鐵新左營車站電子看板疑遭駭客入侵，出現簡體中文恐嚇訊息。

（3）國防部8月3日網站遭到DDoS攻擊。

3、111年8月4日：

（1）桃園機場網站疑遭到網路攻擊陸續出現服務中斷的情形。

[4] 周峻佑。2022年8月12日。臺灣8月初因裴洛西訪臺而遭到網路攻擊的事件總覽。iThome網站新聞。https://www.ithome.com.tw/news/152491

（2）高雄市環保局飲用水網站被置換五星旗。

（3）台電公布8月3日遭到網路攻擊次數達490萬次，已超過6月及7月總和。

4、111年8月5日：國防部、外交部網站凌晨再度癱瘓。

5、111年8月6日：民視節目網路直播內容遭到竄改，起因是影片來源主機遭到入侵。

6、111年8月7日：臺灣大學部分網頁遭到竄改，圖片皆變為「世界上只有一個中國」的恐嚇訊息。

7、111年8月9日：臺灣基督教長老教會網站遭駭，網站被換上中國統一的恐嚇訊息。

(二)依據數位部提供國家資通安全通報應變網站接獲通報之事件分級及威脅類型逐月資料，本院自行繪圖如下圖9及圖10，顯示以公部門而言，111年8月之攻擊強度確實較其他月份為高，且主要為第1及第2級事件；若以威脅類型分類，掃描刺探型態於111年8~10月顯著增加，而入侵攻擊型態則常態性處於高檔。

1、國家資通安全通報應變網站110至111年接獲通報之事件統計逐月資料。

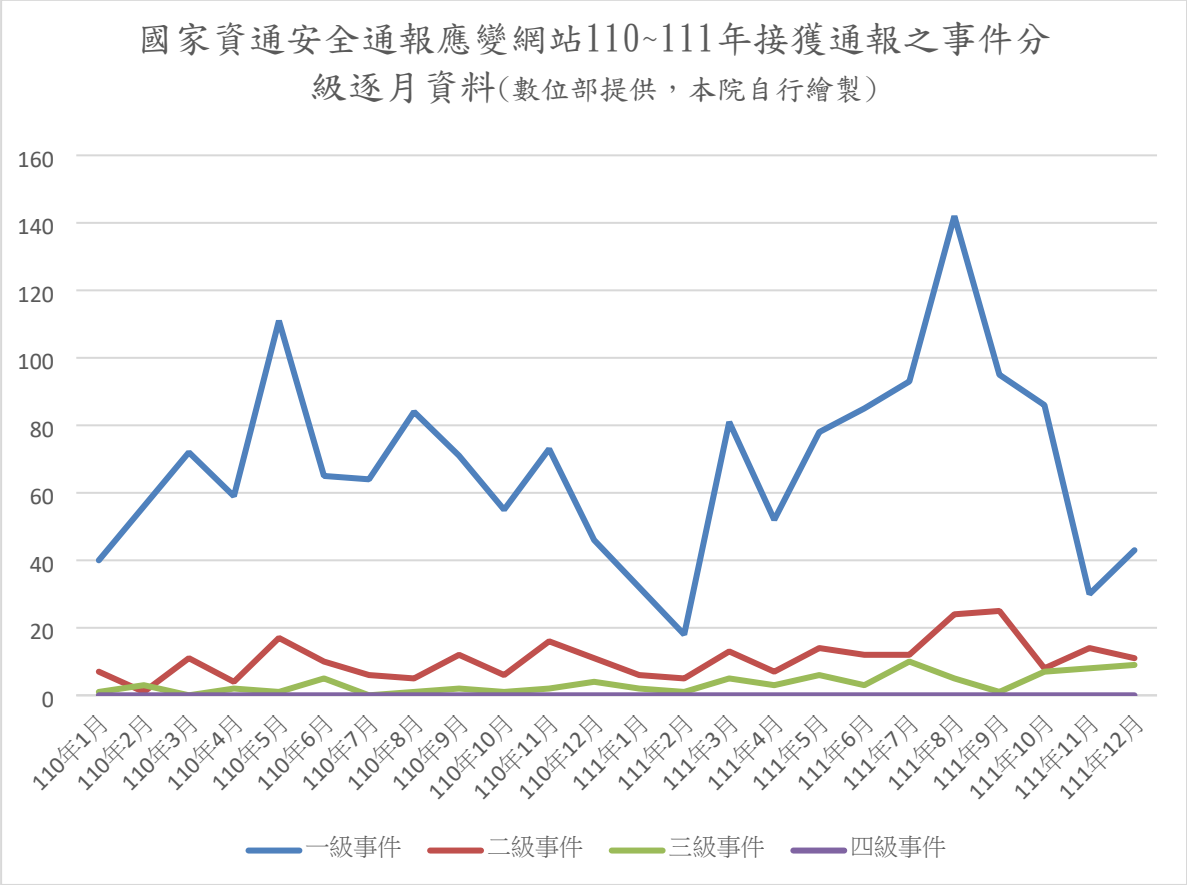

圖2　國家資通安全通報應變網站110至111年接獲通報之事件統計逐月資料。(數位部提供，本院自行繪製)

2、國家資通安全通報應變網站110至111年接獲通報之威脅類型統計逐月資料。

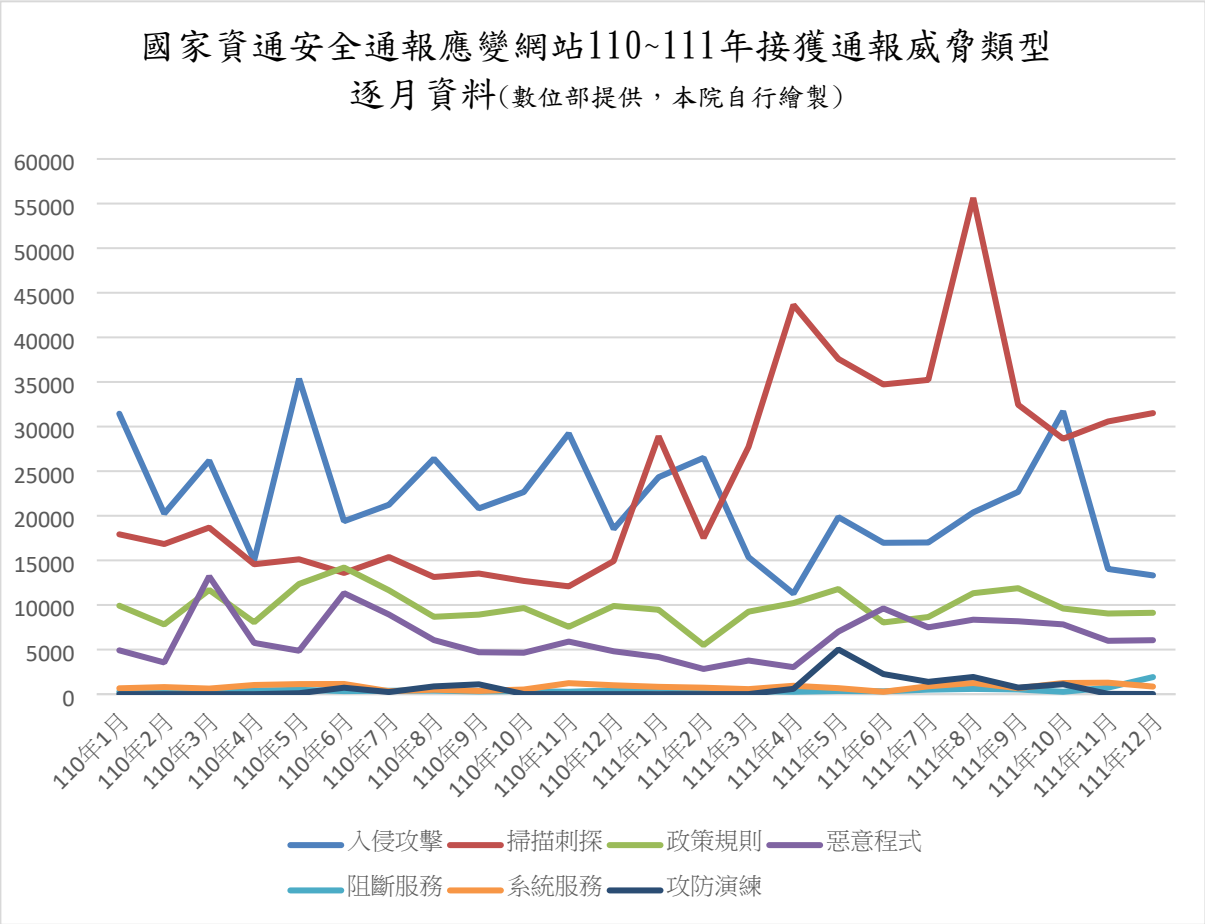

圖3　國家資通安全通報應變網站110至111年接獲通報之威脅類型統計逐月資料。(數位部提供，本院自行繪製)

(三)另據數位部函復，行政院資通安全會報針對111年8月份資安事件要求各機關加強資安防護整備工作及配合事項如下

1、強化網站架構:機關對外系統預先備妥靜態網頁、快速切換機制及低用量網站盤點或下架等，包含所採用流量清洗或DDoS防護服務或設備等替代措施，以減緩遭癱瘓攻擊的影響。

2、各機關提供公眾活動或使用之場地，不得使用中國廠牌資通訊產品之議題:數位部於111年11月28日修正並公告「危害國家資通安全產品限制使用原則」，請各機關據以辦理，並將相關要求納入

契約，如果有特殊原因必須使用，須經機關資安長及上級機關資安長逐級核可。

3、依行政院國家資通安全會報第40次委員會議紀錄，要求行政院所屬二級機關彙整所屬(管)機關警戒專案相關網站韌性強化措施辦理結果，包含靜態網頁、快速切換及下架整併低用量網頁，各機關及二級機關資安長應親自署名，並應於112年2月底前逐項查核確認。數位部亦將本項作業查核納入資安稽核項目。

(四)小結：有關DDoS攻擊及服務癱瘓風險，主管機關及目的事業主管機關應對風險識別、防護邊界及動態網頁因應對策研謀精進作為，包括針對「政府機關重要服務」確實定義及盤點，以及預擬動態服務網頁遭DDoS攻擊之因應措施。

1、基於數位部查復說明「將持續要求政府機關重要服務備妥靜態網頁供需要時切換與預備流量清洗服務」，為釐訂資安防護邊界及風險識別，主管機關及目的事業主管機關應對「政府機關重要服務」確實定義及盤點。

2、另以某大學某對外服務系統於111年8月遭癱瘓後，112年4月總統出訪期間又傳出遭到癱瘓，顯示部分機關網頁雖可以於遭遇DDoS攻擊時上架靜態網頁作為因應，然多數動態網頁為持續營運提供服務(如軌道運輸訂票系統)，無法切換為靜態網頁關閉服務，若於服務尖峰時段遭癱瘓，勢將造成重大衝擊，則是類系統如何因應未來可能發生之跨領域大規模攻擊，數位部及相關主管機關宜先預置相關機制加以因應。

3、此外，DDoS攻擊特點為技術門檻低、難以持續攻

擊，卻也不易防範；數位部曾表示採用WEB3及星際檔案系統(Inter Planetary File System，IPFS)相關技術可以有效因應；惟據悉該等技術所費不貲，短期內普及至所有公務機關及服務有其困難，基於資安工作不會花1000元去保護100元的東西之原則；數位部應就系統之防護等級或可能衝擊，對DDoS攻擊應採取何種合乎比例之防護手段，提供相關指引，以供各機關參考或爭取建置預算。

(五)次查電子看板風險部分，主要由內政部及經濟部分別訂定相關指引，茲將本院112年5月17日辦理約詢時，兩機關說明辦理情形臚列如下，顯示相關規定及指引僅具行政指導性質，或運用既有法規進行延伸管理，不易防杜該等事件再次發生，另就內政部及經濟部立場而言，似仍有以專法管理之需求，此外，本院諮詢學者專家亦表示「在法律面，資安法只是把框架訂出來，只是一個起步，歐盟數位相關法律步調非常快，例如數位媒體服務匯流中介等等，國內相關法律是沒有這些框架的，行政機關宜著手處理」，顯示相關法制整備仍有強化空間，建議數位部偕相關部會宜循適當管道加以溝通：

1、內政部營建署:

(1) 85年就將廣告物納入建管法來管理，並訂立管理辦法(指招牌廣告及樹立廣告管理辦法)，著重在定義、規模、規範、處所，比較偏向硬體管理，尚無涉及廣告內容管理；這次資安事件後，去年9月參考經濟部的指引發布了一版指引，也發文給地方主管機關要求審查時要提醒申請人注意，這是行政指導部分，但行政指導

不夠，必須在法制上強化。

（2）後續規定於112年4月19日台內營字第1120804945號令修正發布招牌廣告及樹立廣告管理辦法第14條之1，明定如其系統連網環境欠缺資通安全防護措施或防護不全者，直轄市、縣（市）主管建築機關應以書面命設置者立即停止使用並改善，設置者於改善完成並報經直轄市、縣（市）主管建築機關同意後，始得恢復使用。設置者如未依規定立即停止使用，直轄市、縣（市）主管建築機關得斷絕是類招牌廣告使用所必須之電力或其他能源，以維護社會公共利益。

〈1〉該辦法對招牌廣告之定義：指固著於建築物牆面上之電視牆、電腦顯示板、廣告看板、以支架固定之帆布等廣告。

〈2〉該辦法對樹立廣告之定義：指樹立或設置於地面或屋頂之廣告牌（塔）、綵坊、牌樓等廣告。

（3）該署徐燕興副署長亦補充：「我們這些規定主要是規範建築，因為法源還是建築法。這次修法則是建築法以延伸去管理，還是希望有專法可以去管理廣告內容。」等語。

2、經濟部「營業場域電子看板資通安全管理指引」辦理情形：

（1）111年8月18日公告訂定「營業場域電子看板資通安全管理指引」，並函知各超商超市賣場等零售通路、各縣市政府及相關公協會，同年8月30日邀請全國商業總會、中小企業總會、連鎖加盟促進協會等9家公協會及統一、全家、

大潤發、好市多、全聯等11家超商賣場召開座談會宣導說明，請其配合落實指引。

（2）指引雖無強制力，經濟部仍會持續透過溝通、不定期了解業者管理情形，敦促其改善及落實相關資安管理措施

（3）經濟部商業司劉雅娟副司長亦補充:

〈1〉經濟部的指引要求業者不能使用中國大陸製軟體、避免使用中國大陸品牌產品，但指引沒有強制力，屬於行政指導，訂完之後我們不僅宣導，也有追蹤，目前追蹤起來都有依照指引，也有訂資安管理計畫和通報處置程序，部分業者也辦ISO27001等認證。我們也會持續追蹤業者執行情形。

〈2〉統一超商將就終止電子看板之委外契約，預計112年完成轉換，由統一數網公司來做電子看板。

〈3〉經濟部在目前沒有專法要求業者的情況下，因個資法也有對業者有資料安全管理相關要求，現在係用個資法依行政檢查，對業者進行行政檢查。

(六)另查電子看板資安風險，據調查局查復資料顯示，統一超商電子看板承包商近年更承包高雄捷運、台電、中油、高雄市政府新聞局、水利署等數位看板及媒體行銷相關標案，以供應鏈安全及聯防角度而言，該等潛藏資安風險公司之情資，應適度分享或提醒決標機關強化合約內資安條款；然而經詢問相關機關，該等風險目前似乎尚無主責部會或橫向協調機制得以處理;簡言之，發生在統一超商之事件，也可能因相同漏洞，再次發生於其他公私部門，此

請數位部設法協調相關部會處理，如無法確定權責，或可提報國家資通安全會報討論。

三、歸納近年典型資安事件樣態，顯示公私部門欠缺主動發現風險、適當控管及即時通報之誘因，面對資安事件多採迴避態度，並以恢復營運為首要考量，將不利於建構具韌性之資安體系，確有改善空間；主管機關數位部在持續挹注資源、培養人才及輔導產業之外，允宜積極評估或推動資產可視化、鼓勵通報、績優表揚及爭取資安職系以及公私職務歷練等措施，以實質改善資安從業人員之困境。

(一)依據110年9月由國家安全會議公布、總統簽署之「資安即國安2.0戰略報告」，首要目標即為「充實資安卓越人才」，報告同時指出，現今政府與產業各界均面臨資安人才不足的窘境，前者受限於公務人員選才制度致資安人才招募不易，而專責資安職缺與任務日增，專職資安人員的空缺仍多，其中又以關鍵基礎設施之相關 事業單位缺少資安人才為最迫切。從供給面來看，許多在校修讀資訊資安相關科系領域的優秀人才在強大的就業磁吸效應與跨國企業提供優渥的待遇條件影響下，並未選擇進入資安領域的職場工作；至於針對在職者進行跨領域別的資安能力培育則更加不易。在此種種狀況下，國內整體優質資安人才無論質與量提升的努力空間仍大，且整體的聯合防禦能量仍有待進一步提升。再次揭櫫資安人才之重要性。

(二)本案歸納本院過去資通安全相關調查案，以及近期公開情資揭露之資安事件根因如下，顯示無論是公私部門，在資安管理最前端、最基礎的風險及資產

識別方面，仍經常發生低估風險，甚至自始未予評估之狀況，該等缺失將導致後續防護措施不足；簡言之，若連要防護什麼都不清楚，防護措施也就無從設置。

1、108年銓敘部發生全國公務人員個資洩漏，經查該部「銓敘業務網路作業系統」及「公文管理及線上簽核系統」低估為安全防護等級中級。

2、111年2月，公視基金會發生片庫資料遺失事件，經查該會未能認知到片庫係屬重要資產，而將「新聞片庫系統」防護等級設為「普級」有關。

3、本院諮詢學者專家表示:「電子看板問題是去年才發生嗎?5~6年前偏鄉就通報過電子看板問題，這個問題就是大家把他當作電視，而非電腦」。

4、故宮博物院典藏高畫質圖檔流出案，依112年3月22日立法院教育及文化委員會考察國立故宮博物院資安防護機制會議紀錄顯示，該院於事件發生後並未意識到屬於資安事件，亦未認知該等資產之重要性(風險識別)，以致未設置與價值相符的防護或存取控制措施。

5、iRent共享汽機車平台洩漏大量個資案，就目前公開資料顯示，該公司並未認知資料庫之資產價值及資安風險，以至於完全沒有設置應有的存取控制措施。

(三)次據本案諮詢專家學者、業界意見及臺灣資安大會公開發表資料顯示，目前公私部門對於發生資安事件後之對外回應多採迴避態度，顯不利於建構具韌性之資安體系。

1、本院諮詢學者專家：「提到○○醫院的問題，您可以看到第一個反應都是沒有出事，但沒有客觀

第三者去驗證，心態都是大事化小，小事化無。」

2、奧義智慧科技股份有限公司創辦人吳明蔚博士：「我們看到上市櫃公司發生資安事件發布的重大訊息永遠都是罐頭訊息，不外乎『有資安事件』、『已經調查』、『影響有限』，說來說去都是這些。」

3、勤業眾信周哲賢協理於2023臺灣資安大會「統計台灣上市櫃公司的資安重大訊息，看企業資安治理為何失效」演講中指出：經分析456天、2092家上市(興)櫃公司及103,983筆重訊，發現目前上市櫃公司年報資安相關應記載事項，無法明確得知資安治理失效的確切原因。

(四)經查，公私部門或資安從業人員若未能主動發現風險加以控管，或於發生資安事件採迴避態度，究其原因乃是缺乏積極主動之誘因，縱使政府近期不斷提高通報時效或明訂跡證保存及根因調查等相關作業，成效勢必有限，此有本院諮詢專家學者意見佐證如下。

1、我們的人才確實不足，但是面對國內缺口，我們是要跟國外競爭，政府要有足夠的誘因。我10幾年前考過證照，在民間可以獲得加薪，但在政府卻沒有幫助；人才雖然不一定把薪資視為唯一的考量，但是公部門不能與業界差太多，我認為公私之間人力交流，對於兩方都有助益。這樣政府的薪水就不用提高很多。

2、如果一開始就揭露，反而應該鼓勵，而不是上報了才處理。

3、「資安從業人員過勞、高耗損」、「資安長是最糟

糕的工作」、「近三分之一的資安長撐不過一年」

(五)針對本院於調查中請數位部重視公私部門資安從業人員缺乏誘因之困境,數位部有兩項正面回應如下，本院樂觀其成並將持續追蹤;惟爭取資安職系一節，自本院108年調查銓敘部個資案時，前行政院資通安全處即已開始爭取,迄今已逾四年尚無重大進展，數位部承接相關業務後，仍應持續積極辦理；至於學者專家建議資安人才可規劃於公私部門輪流歷練，除可建立良性之公私協力以及技術/經驗傳承機制外，亦可適度紓解公部門與業界之薪資福利差距問題，此與數位部爭取約聘僱彈性用人機制之考量殊途同歸，均有利於營造國內資通安全人才友善環境，亦請數位部評估可行性。

1、行政院資安會報每年辦理攻防演練及資安稽核，並於資安會報會議中，由行政院副院長公開表揚表現績優機關；針對落實資安管理及防止資安事件擴大之情形,後續將研議公開表揚等鼓勵機制，以推動機關持續精進資安防護工作。

2、有關增設資通安全職系，資安署刻與考試院、銓敘部及行政院人事行政總處研商納入公職人員考試等相關事宜，已就應考資格、考試方式及應試科目等規劃初步構想，後續將會同相關機關，邀集專家學者及相關利害關係人討論規劃可行性，持續辦理相關作業。

四、基於現行系統開發作業日益仰賴第三方函式庫或開源軟體，將形成軟體供應鏈安全問題，五倍卷網站原始碼出現簡體字註解及Log4Shell漏洞透過開源軟體潛藏於諸多商用產品等案例不勝枚舉，將成為惡意程式滲透管道之一；基於先進國家已逐漸導入SBOM規範並

列為採購規格，不論是基於國家資通安全或資訊產業國際競爭力考量，我國導入SBOM勢在必行，數位部對此宜有具體之重點規劃。

(一)根據行政院資通安全會報111年6月發布之「110年國家資通安全情勢報告」指出，歐盟ENISA於110年發布之供應鏈威脅報告(Threat Landscapefor Supply Chain Attacks)中指出，供應鏈攻擊仍持續增長，且影響範圍也更為廣大，該報告並指出約**66%事件攻擊者係針對供應商程式原始碼**，58%攻擊目標是客戶端資料，如個人資料與智慧財產等，隨著對供應鏈之依存性越來越高，供應鏈資安威脅亦與日俱增。

(二)次據資安大廠趨勢科技對軟體供應鏈攻擊風險之描述[5]，開發人員經常會從GitHub這類公開分享的儲存庫複製其日常所需的原始程式碼。當別人已經寫好一段程式碼來處理欄位間的訊息傳送時，為何還要浪費時間撰寫相同的程式碼？就是因為很容易使用，所以今日**有90%的應用程式都使用到開放原始碼**；然而，許多企業都無法明確掌握開放原始碼之間的相依性。開放原始碼不受監督的特性，很容易造成像熱門開放原始碼軟體Apache Log4j所帶來的嚴重攻擊。網路犯罪集團利用Log4j事件記錄軟體框架的一個重大漏洞將惡意程式碼注入含有漏洞的系統。根據美國FDA的估計，Log4j大約影響了30億台以上使用Java的醫療裝置。

(三)另據中華資安國際檢測團隊林峰正經理於2023台灣資安大會「誰是豬隊友，從紅隊和事件調查實例看

[5] https://blog.trendmicro.com.tw/?p=76072

供應鏈及邊界安全」演講歸納，涉及開發流程供應鏈APT(Advanced Persistent Threat，進階持續性威脅[6]) 攻擊樣態至少包括開發工具加料(如Xcodeghost) 、更新網站掛馬(如ASUS Updates Hijacked)、內部攻擊(如Phishing Attacks)、原始碼加料(如SolarWinds)，以及下載網站掛馬(如CCleaner)等。

(四)法務部調查局於109年8月19日發布「中國駭客組織對我國資訊供應鏈發動攻擊」新聞稿，指出:

1、調查局近來偵辦數起我政府機關遭駭案件，調查過程中發現中國駭客組織Blacktech與Taidoor，已長期滲透國內政府機關及其資訊服務供應商，尤其是承接政府標案之資訊服務供應商，因其負責政府機關重要資訊系統之開發及維運，故成為駭客主要攻擊目標，作為跳板攻擊政府機關，試圖竊取機敏資訊及民眾個人資料。

2、中國駭客組織深知政府機關為求便利，常提供遠端連線桌面、VPN登入等機制，提供委外資訊服務廠商進行遠端操作與維運，由於國內廠商大多缺乏資安意識與吝於投入資安防護設備，亦未配置資安人員，故形成資安破口，以Blacktech駭客組織為例，該集團主要活動於東南亞地區，駭客先鎖定國內存在尚未修補之CVE漏洞的網路路由器設備，因多數民眾未對設備做韌體更新或修改預設設定，故遭駭客利用此CVE弱點取得該路

[6] 主要是透過長期性的網路攻擊活動來達到目標，此種攻擊的特色:1.有目標性2.持續性3.手法先進，首先APT攻擊都是有目標的，譬如說這次攻擊是為了取得某些文件，或是取得特定人士的E-mail密碼，不像過往透過蠕蟲與後門隨機攻擊，並且攻擊並不是只有一兩次，而是每天或是每周一直不斷的攻擊，再配合先進的病毒，或是手法，一直攻擊直到目標達成。(https://www.khhpd.npa.gov.tw/ch/app/faq/view?module=faq&id=2370&serno=ad4e6d3c-b977-487b-9a65-1ec516ba7bc4)

由器控制權作為惡意程式中繼站，並以另一途徑攻擊國內資訊服務供應商或政府機關之對外服務網站、破解員工VPN帳號密碼及寄送帶有惡意程式之釣魚郵件等，成功滲透內部網路後，利用模組化惡意程式進行橫向移動。

(五)據悉，110年傳出五倍卷官網原始碼註解出現簡體字一事，經濟部表示「五倍券官網為關貿網路公司負責開發管理，程式工程師在各大討論區相互學習、交流技術，是常見的作法，因此工程師團隊曾在中文技術討論的CSDN討論區討論交流，但相關引用應該修改，原始碼註解出現簡體字樣確實不妥。.....程式安全及正確性是以程式源碼本身為主，註解文字部分於程式編譯或執行時，不會被納入執行，也不影響資訊安全及程式正確性」等語[7]，雖未造成資安事件，惟顯示現行系統開發已不可能在未引用第三方或開源資源的情況下，自行撰寫數百萬行程式，故軟體供應鏈之風險仍宜獲得主管機關一定程度之重視。

(六)業界及本院諮詢學者專家均表示軟體供應鏈安全必須進一步強化，佐證如下：

1、GDPR[8]、CMMC[9]等各國資安相關法規越趨嚴格，全世界的法遵都在盯供應鏈安全，不能獨善其身。

2、例如錄影機都是中國製造，世界上90%都是中國製造，內部軟體都是2~3家寫的，因為成本問題，

[7] 110年10月10日自由時報「5倍券官網原始碼有簡體字 經濟部坦言不妥」 https://ec.ltn.com.tw/article/breakingnews/3699860

[8] GDPR：General Data Protection Regulation，歐盟個人資料保護規則。

[9] CMMC：Cybersecurity Maturity Model Certification，網路安全成熟度模型認證，主要目的在於評估美國國防部承包商的網路安全能力，而2.0版的修訂，希望確保承包商遵循最佳實務做法，以保護網路上的敏感資訊，同時也使中小型業者更容易遵守這些規範，預計2026財政年度起，將成美國國防採購案的必要需求。

程式碼漏洞很多，這就衍生軟硬體的製造來源是哪裡，現在有個SBOM(SOFTWARE BILL OF MATERIALS)的概念，產品要交代軟硬體的來源是哪裡。

3、美國由白宮發布規定，軟體要賣給聯邦政府要附上軟體成分表，目前成分表有一定的標示規範和定義，目前有三套指引。美國政府也會定義營業秘密的範疇。因此，現在美國主要軟體商，都有具備支援美國成分表的能力。這是一個軟體供應鏈的概念，類似食安的管理方式。

(七)對此，數位部有正面回復如下，本院樂觀其成並將持續追蹤：

1、數位部將推展政府資訊系統可利用之開源軟體，並對其建立SBOM，以期協助政府機關資訊系統使用的開源軟體具完整性和可追溯性。

2、隨著全球化發展，醫療、工程、資訊及電子等各產業藉由供應鏈協同運作，如CMMC之供應鏈管理制度也推行透過SBOM進行資產管理。此外，工程會亦將於採購制度要求供應商應標示其軟體組成(即SBOM概念)以利機關管理並進行軟體品質之維護把關。

3、資安署鄭欣明副署長於本院112年5月17日辦理約詢時亦補充：「軟體通常由原始碼編譯成執行檔，我們要分析必須反向編譯，所以是一個技術問題，全世界都在煩惱這塊，數位部產業署正在研究此議題，亦將於採購制度要求供應商標示軟體組成」。

調查委員：賴鼎銘

葉宜津

林郁容

中　華　民　國　　１１２　　年　　5　　月　　３１　　日