監察院109年上半年度通案性案件調查研究報告

壹、題目:「國家安全局因應中共網路戰威脅之策略與執行成效」通案性案件調查研究。

貳、結論與建議：

一、國家安全會議於民國（下同）107年9月14日提出首部國家資通安全戰略報告，提出「打造安全可信賴的數位國家」之戰略願景。在法令面，行政院於同年通過資通安全管理法及六項子法，將資通安全事務提升至法律位階，並於108年7月增訂國家安全法第2條之2，將國家安全之維護範疇延伸至網際空間。在組織面，國家安全局更早至104年5月成立網域安全處，復於107年4月在「國家安全作業中心」成立專案小組，蒐研爭議訊息危安預警情資，法務部調查局亦於109年4月成立資安工作站等，在在顯示政府極為重視資通安全，而使我國得以完成初具規模之資通安全防禦體系，各相關機關允宜本於「國家資通安全戰略報告」之精神，在法令面、組織面及技術面持續加強推動，並加強戰術情報之情蒐及運用，以因應網路戰時代日趨嚴峻的國家安全挑戰。

（一）國家安全會議（下稱國安會）於107年9月14日提出首部國家資通安全戰略報告，提出「打造安全可信賴的數位國家」之戰略願景，並經總統核定，使國家安全邁入一個新的里程碑。我國對於資通安全之重視始於國安會自89年5月研擬提出「建立我國資通訊基礎建設安全機制」建議書，後續行政院在90年1月第2718次院會核定通過第一期資通安全機制計畫，並成立「國家資通安全會報」，積極推動我國資通安全基礎建設工作，並逐年調整組織架構及

相關任務。

1、行政院在106年通過4年期的「國家資通安全發展方案」，國防部也結合國防戰力成立資通電軍，同時為強化我國八大關鍵基礎設施之資安防護能力，於107年5月推動並通過「資通安全管理法」立法，並搭配投入「資安旗艦計畫」及「前瞻基礎建設計畫」，以落實關鍵基礎設施之各項資安防護工作。

（1）依據世界經濟論壇(World Economic Forum, WEF)「全球風險報告」顯示，在106年全球可能風險排名中，資料欺詐或盜竊名列第5名，大規模網路攻擊則名列第6名，可見資安風險已深深影響人類的生活。

〈1〉根據身分竊盜資源中心(Identity Theft Resource Center, ITRC)的統計數據顯示，截至106年6月30日美國年度資料外洩事件已高達791筆，與105年同期相較增加了29%，創歷史新高。

〈2〉近年資安外洩最嚴重的案例為102年美國知名入口網站系統遭駭客入侵，累計個資外洩筆數達30億筆，這其中包含我國人的個資在內。根據賽門鐵克(Symantec)106年4月的網路資安報告顯示，我國資料外洩程度居全球第5名，更高居亞洲榜首。

〈3〉根據卡巴斯基(Kaspersky)105年第4季釋出的報告指出，有80個國家的殭屍網路參與分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)，其中發起攻擊的多為IoT設備組成的殭屍網路，且攻擊強度有持續提高的趨勢。

（2）關鍵資訊基礎設施無法正常運作

〈1〉越來越多關鍵基礎設施(Critical Infrastructure, CI)的監視控制與資料擷取系統(Supervisory Control And Data Acquisition, SCADA)因有遠端操控系統的需求，紛紛採用開放的連網架構，徜本身的安全性未提升到足以抵禦駭客攻擊的程度，一旦遭到入侵或破壞，可能會對民生經濟甚至國人生命安全造成相當程度的損害。

〈2〉根據105年，卡巴斯基實驗室專家針對工業控制威脅進行調查，發現全球有數千臺主機暴露在網際網路上,其中更有高達91.1%的主機存在遠端控制的漏洞。

2、在國家資通安全戰略報告序言中即揭示，利益競逐與層出不窮的資訊安全問題也在邊界模糊的網路場域中應運而生，甚至產生資訊武器化的現象，是以世界各國多致力於網路治理研究、大力構築網路安全建設、設立專責機關、研定相關法規，並尋求國際協作，資安議題顯已超越科技範疇成為國家重要的戰略選擇。

3、在上開報告有關「資安政策的重要內涵」亦指出，戰略報告以情報驅動提出三大提升及三大整合策略，前者是基礎整備、產業量能和數位防衛能力的提升，後者包含資安人力、研究及產業的跨域整合，以提高資安機制效率、改善我國資安人力不足及產業自主研發能力疲弱等三大議題。而國安局既為國家情報工作法(下稱情工法)之主管機關，依該法第1條負有「規範、監督、統合國家情報工作」之職責。

(二)國安局並針對法令層面整備情形提出說明

1、內政部於108年7月3日完成「國家安全法」第2條之2「國家安全之維護，應及於中華民國領域內網際空間及其實體空間」修正條文，賦予我國安維護範圍擴及網安領域。

2、承上，該局赴本院進行簡報時亦說明，內政部108年7月修過國安法，增列第2條之2，把網路虛擬空間納入，國安局執行網安就有了根本性的母法依據。資通安全法更是首個資安的法規，國安局也曾參與討論及提出立法建議。

3、「資通安全管理法」於107年6月6日訂頒，立法目的係為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益；另該院每年舉辦政府機關資安稽核及網路攻防演練等作業，均邀國安局派員參加。

4、國安局資訊室訂定「資訊系統分級」、「資訊裝備及儲存媒體管理」、「軟體服務及資料備份管理」、「網路及網站設置管理」及「資通安全獎懲審查」等作業規定，不斷強化國安局資安防護相關工作。

5、陸委會亦於108年5月2日赴立法院第9屆第7會期外交及國防委員會報告「中國假訊息心戰之因應對策」時說明，有關強化假訊息管理機制，填補現行規範之不足：行政院前於106年間提出「數位通訊傳播法」草案，正在立法院審議中。就網路社群平臺服務業者保護權利人的協力義務，已制定適當規範管理。復於107年及108年兩度針對假訊息之防制提出修法，內容分別針對散布假訊息之行為人加重刑期與罰鍰，及就網路假訊息為規範管理，第1波修法包含災害防救法等7部法律，第2波修法則包含刑法等3部法律。

(三)我國針對網路戰之組織面整備情形

1、在行政院層級，資安會報成立於90年1月，負責國家資通安全政策、通報應變機制、重大計畫之諮詢審議及跨部會資通安全事務之協調及督導。為貫徹「資安即國安」戰略—提高資安主導層級之重要策略，行政院於105年8月1日成立資安專責單位—行政院資安處，取代原任務編組之資通安全辦公室，擔任資安會報的幕僚單位。

2、行政院資安處簡處長亦於本院6月赴國安局座談時簡要說明，在體制方面，行政院資安處是統整國家資安政策的機關，跟情治機關之間的合作以銓敘部為例，一定會先通報到行政院資安處，如果是重大資安事件，我們會出面邀集各機關比如調查局或刑事局進行調查，如果是可能的資安事件，機關會跟調查局報案，那就進入另一個調查程序，從關鍵基礎設施也是納入資通安全管理法，主要是因為要管到民間必須有法明定。

3、國安局說明，鑒因世界各國已將網路空間提升至國家主權層級，該局於104年5月修訂組織法成立「網域安全處」，主責蒐整全球網安資訊及該局關注網域安全威脅相關情資；另於107年4月1日於「安全作業中心」成立專案小組，蒐研爭議訊息危安預警情資。

(四)至於情報機關在政府整體資安防禦體系之角色，則歸納如下：

1、國安局於赴本院簡報時說明，在面對網路戰威脅部分，政府部分是因為受情工法授權，國安局單純負責情蒐工作，依據資安鐵三角的指導辦理，鐵三角是由國安會資安辦、行政院資安處及通傳會組成，國安局屬支援單位，由於資安防禦政策

講求由情報驅動，故國安局負責供應情報，如果是提到防禦部分是行政院資安處，再行政體系部分有資安會報，國安局業管副局長是會報成員。概略的說，以行政來說是以行政院資安處為主體，以國家層級的防禦是以資安鐵三角為主體，國安局就是在做幕後的情報提供。概略的說，以行政來說是以行政院資安處為主體，以國家層級的防禦是以資安鐵三角為主體，國安局就是在做幕後的情報提供。

2、國安局並函復說明，該局依循以情報驅動之「資安即國安」戰略指導，國安局密切與「資安鐵三角」配合協作，在政府服務網(GSN)之威脅偵測應處機制成效上，各級事件數確有早期發現與即時應處，然中共網軍藉軍改實施整合，我國所面臨網駭威脅未來仍屬嚴峻

3、行政院資安處則表示，根據國家資訊安全發展方案106-109年之目前發展方案，係以加強資安防護管理二線監控機制與資安情報分享為重點。資安會報因應我國資安威脅加劇，新增「關鍵資訊基礎設施安全管理組」，讓資安鐵三角—國安會、行政院資安處及通傳會連結8大關鍵基礎設施領域之7個主管部會，擴大建立國家資安聯防運作機制、建立8大關鍵資訊基礎設施領域及國家層級之資訊分享與分析中心(ISAC)、電腦緊急事故處理小組(CERT)及資訊安全監控中心(Security Operation Center, SOC)，期由情報驅動國家政府、關鍵基礎設施主管機關及提供者三大層級，形成資安聯防與合作網路，組成國家資安聯防體系，進行資安聯防及情資分享，並聯結國際。

4、本院諮詢學者專家中研院資訊科學研究所李○○客座講座亦表示，「一旦我們觀察到資安事件，資安鐵三角的三個單位就要一起運作。至於現在被攻擊的頻率、次數和力道等等，都是在增加的情況，包括中油事件即為一例」。

(五)有關我國所面對的網路戰威脅情形：

1、在國際上，根據國防譯粹（第45卷2期)「定義新型態俄式資訊作戰」內容略以：

（1）資訊作戰逐漸成為當代俄羅斯作戰整合的核心角色，其廣泛涵蓋面在俄羅斯全般行動中扮演重要角色，完全逆轉了美國準則所提出的戰爭範式(paradigm of war-fare)，並對於美軍聯合部隊構成各種重大挑戰。

（2）俄羅斯的模式將資訊作戰行動與所有戰爭階段結合，而這個作法是美軍聯戰準則與政策面從法律和作戰角度所無法仿效的，因為如此將破壞建立聯合部隊所望確保的自由民主制度和價值。俄羅斯的資訊作戰行動不強調或忽略合法性與公信力面向，無可避免地會獲得美軍聯戰準則與政策面難以比擬的速度和靈活性。

2、摘述遠景基金會相關會議或座談涉及我國面對資訊戰威脅之相關重點：

（1）中國資訊戰能力之評估：

〈1〉311基地已於2016年軍改後併入解放軍戰略支援部隊：中國解放軍2016年軍改後，同時調整作戰形態及組織文化，大幅提升太空、網路、電子及心理等作戰能力。原總政治部變為政治工作部，而原負責行政事務之部門，統一轉至聯合參謀部，由中央軍委統一管理；另原隸屬解放軍總政治部執行對臺統

戰工作的311基地，現已轉至解放軍戰略支援部隊（SSF）執行戰略情資輔助工作。

〈2〉解放軍戰略支援部隊功能編制顯示中國資訊戰略思維已轉變：解放軍戰略支援部隊主要功能在於戰略資訊輔助及戰略資訊操作兩大面向；前者係透過集中化管理科技情蒐系統之權力，使該部隊直接向戰區指揮部提供戰略情資，以擴充太空、核武及聯合作戰能力；後者則在於整合太空、網路、電子作戰能力，以達成開戰前就癱瘓敵人作戰系統體系。

3、我國面對之網路戰威脅情形與現況，根據108年國家資通安全情勢報告內容摘述如下：

（1）分析107年度政府機關遭惡意電郵攻擊之趨勢發現，11月份攻擊郵件數量遽增，惡意電子郵件攻擊數量為全年度最高，主要以資通安全責任等級A級機關為主要攻擊目標，且駭客從8月下旬開始寄送惡意郵件，10月底至11月初針對蒐集到的攻擊目標帳號，客製化相關業務信件與誘餌文件，並發動大規模社交工程郵件攻擊，經研判為當時適逢九合一大選期間，有心人士認為此為結合時事議題以獲較高攻擊成功機會之最佳時機。

（2）107年政府機關間亦發生若干案例，例如：公車站電子看板，存在RootBridge而遭植入挖礦程式、伺服器遭利用ApacheStructs2及作業系統漏洞進行攻擊，植入門羅幣挖礦程式等。由此可知，除駭客過去常用以勒索軟體賺取金錢之手法外，挖礦程式亦為其另闢生財之道，各政府機關需加強防範。

（3）107年出現攻擊政府機關內部機房環控系統之少見案例；駭客入侵該系統，取得調整濕度、空調及電磁脈衝設備設定調整之權限，藉此影響資訊機房運作。

（4）107年發生數起政府機關委外資訊供應商遭駭事件，導致機關所持有之敏感資料外洩，該類事件係駭客利用供應商開發之委外系統漏洞或開放委外廠商遠端連線之測試機，因存取權限設置不當而遭進行攻擊。

（5）政府機關資安事件通報情形：107年政府機關通報之資安事件數量計754件，各級資安事件依嚴重等級低至高共分4級[1]，各級資安事件發生件數及比例依為1級635件(84.13%)、2級78件(10.58%)、3級41件(5.29%)、4級0件(0%)。

4、依據國安局於108年5月2日赴立法院第9屆第7會期外交及國防委員會報告「中國假訊息心戰之因應對策」對我國受到網路戰威脅情形報告

（1）國安局彙整國安單位蒐獲情資，以及合作友方交流研析所得，顯示中共刻正複製俄羅斯併吞克里米亞島的模式，利用我國民主社會、資訊傳播環境與方式之自由開放，以及各種法律層面之不足與漏洞，意圖以散播爭議訊息對我遂行「認知作戰」，旨在分割我方戰力，消耗政府與國安團隊能量，並影響我主要資源之投入方向及重點；據瑞典哥德堡大學（University of Gothenburg）研究指出，臺灣遭受外國假資訊攻擊程度世界第一，且臺灣被評分數與其他國家差距甚大，顯見「如何防制中共對臺遂行認

[1] 依事件造成之機密性、完整性及可用性衝擊之嚴重度區分，由輕至重分為「1級」、「2級」、「3級」及「4級」。

知作戰」已成臺灣刻不容緩須面對之國安議題。

（2）中共散播爭議訊息的模式：綜整中共及境外敵對勢力近年對臺遂行「認知作戰」，係採網路駭侵、散播爭議訊息，結合中共「大外宣」政策及對臺統戰滲透等手法，歸納中共散播爭議訊息之模式及手段，計有「新聞事件—中共加工—回銷臺灣」、「爭議事件—中共變造—改變認知」、「陸媒捏造—掌握通路—擴散臺灣」、「陸方指導—同路配合—引領風向」等4種模式。

5、次據調查局提供意見，該局分析我國面對爭議訊息之優勢、劣勢、機會及威脅分別如下：

（1）優勢：政府已重視爭議訊息之影響及應處，政府部門澄清訊息及溯源法辦時效相較以往皆加快許多，且目前亦有向民眾宣導，可利用專業之第三方查核組織(如「台灣事實查核中心」)，針對假訊息進行查證闢謠，由民間團體與執法單位協力合作打假。

（2）劣勢：

〈1〉包括多數假訊息難以溯源，以過往偵辦假訊息案件經驗，性質多為高隱密、匿名而難以取證至源頭，實際操控之黑手隱身幕後，面對假訊息，僅能透過各行政機關發佈新聞稿澄清不實資訊，對嚇阻假訊息的散播效力仍有限。

〈2〉民眾尚無主動查證習慣，因社群媒體興起，現今社群媒體平臺之使用者亦大幅增加，然使用者所接收訊息多為片面資訊，特別是預存立場之民眾難以客觀看待訊息本身真假，未能做主動查證，以確認該訊息是否係遭人為加工之不實訊息。

（3）機會則在於運用新科技(如大數據、AI分析)防制假訊息：以個案而言，組織性假訊息即使溯源卻也難以偵辦，故應運用整體情報彙整方法，以洞悉爭議訊息擴散手法及路徑，經循之查明擴散帳號、群組及訊息傳遞對象後，進一步運用新科技，建立假訊息擴散之模式及情資，供日後研析運用。

（4）威脅則包括：

〈1〉假訊息散播速度快於澄清辨識，因我國目前針對假訊息蒐情方式較倚賴人工偵蒐方式，尚未完全運用科技輔助，亦較難立即找出假訊息。

〈2〉另外則是封閉性質群組具隱密性，假訊息若於私密群組發佈，便無法於網路等公開管道蒐尋到相關訊息，司法單位將較難分析資訊的散佈來源及管道。

6、依據本院諮詢中研院資科學研究所客座講座李○○教授說明，戰略報告內界定駭侵有四種態樣，包括國家支持型、犯罪組織型、理念宣傳型、恐怖主義型等四種，在關鍵基礎設施又可分有8大類，對於關鍵基礎設施有興趣的駭侵者大部分都是前兩種，而理念宣傳型駭侵者主要是對爭議訊息有興趣，恐怖主義型在臺灣比較少。在爭議訊息其實也就是中共的三戰其中兩個，即心理戰和輿論戰。

(六)在戰術情報之強化方面，調查局說明

1、依網路戰三大型態列舉戰術情報運用實際案例如下：

（1）資料竊取事件：包括，臺北市政府秘書處遭入侵案、臺北市衛生局遭駭客入侵案、銓敘部個

資遭駭案、臺大醫院VIP病歷資料遭駭案、全國政府之公文電子交換系統遭駭客入侵案(包括經濟部、外交部、環保署及NCC等機關)等。

（2）關鍵基礎設施及工業控制系統等案件：包括第一金與證券公司遭比特幣勒贖案、總統府、調查局及中央銀行等機關遭DDoS攻擊案，此外尚包括，司法院遭網軍攻擊案，以及衛福部EEC系統與醫療院所遭植入勒索病毒等案

（3）該局並與美國、歐洲刑警組織等31國共同偵破「雪崩」殭屍網路案，全球總計有超過80萬筆惡意網域名稱受到阻斷，在全球同步執行偵辦下，我國共蒐索37處所，扣押伺服主機39部，強制離線伺服主機221部，成功阻斷3萬3,925筆惡意網域名稱等。

（4）另外，該局與美國FBI、微軟數位安全中心合作偵辦全球殭屍網路Necurs不法案：全球受Necurs感染電腦總計超過900萬部,在我國則有超過4萬8,000個IP位址感染，且有多達23萬個網路IP遭受入侵,在取下受感染之關鍵IoT設備後，成功令我國免於成為殭屍網路及惡意程式之跳板。

（5）至於爭議訊息部分，該局自主發掘境外假訊息相關情資，即時調查偵辦，並針對潛在假訊息攻擊進行預警分析，甚至先期進行新聞發布供民眾防範，亦給予潛在恐遭受假訊息攻擊之權責單位著手預防之空間。

〈1〉「228連假期間共三波境外假訊息攻擊」：溯源調查出境外假訊息源頭，先期分析出模板化、假造我國公文圖文等資料、進行二度假澄清混淆真實訊息等攻擊行為，即早揭露予

大眾知曉，化解境外假訊息攻擊效果。

〈2〉假造紙漿缺貨以致民眾搶購衛生紙、尿布之亂。

〈3〉醜化我國致贈巴拉圭、日本口罩之亂。

〈4〉「境外勢力收購網址、藉社群軟體及內容農場進行帶風向之認知作戰」。

（6）大批中共水軍假冒國人向譚德賽道歉案。

（7）該局並於座談時補充說明：「調查局是偵辦假訊息，不是爭訊，我們先釐清，基本上要有惡意和涉及國家安全，我們才會依據司法警察的權限去辦理」。

2、調查局另針對強化戰術情報之相關建議如下：

（1）強化戰術情報之指導：國安局、行政院資通安全處等上級機關可藉體系之高度，蒐羅、整合公、私部門涉及資訊戰之相關情資及事件通報，再依所屬機關職掌進行戰術情報之指導，增加第一時間資安事件應變處理之效率，統整個案情報，化被動為主動，對外清查追溯涉案源頭，防範未來再度受駭或假訊息攻擊。

（2）強化戰術情報之蒐集：同前項所述，藉具高度之主管機關進行跨機關、部門、地區之資安情報蒐集及整合;提供資源予蒐報團隊(資通電軍及調查局等)，如教育訓練、業務指導及獎勵措施等，以提升資安能量及技術水平。

（3）強化戰術情報之處理：調查局收到各外勤通報之資安戰術情報，除自行進行情資後續處理外，更計劃能累積個案資訊，藉由新科技分析資訊戰模式，而上層機關及其他相關單位，擁有更廣情報來源，更能以科技工具進行垂直及橫向之統合分析，擴大及深化戰術情報之運用

價值，亦可強化我國行政部門對資安威脅的應變效率。而上層機關計劃運用之科技工具，可提供予情資體系其他單位使用，藉以即時處理資安事件，加速應變及同步驅動。

（4）強化戰術情報之運用：相關主管機關及行政體系各部門，建立垂直及橫向之暢通聯繫窗口及管道，即能在短時間內廣納意見，綜整判斷以建立決策，發布予相關單位，如此即可強化所獲情報之運用效率及價值。

3、調查局另外針對八大關鍵基礎設施（含科學園區）之戰術情報需求補充說明如下：

（1）調查局資安專業人員遍及各縣市調查處站，局本部資通安全處轄下亦增設資安工作站，平時即偵蒐網安駭侵、政府機關及八大關鍵基礎設之漏洞、情資，已具備相當資安情蒐能量。

（2）倘調查局獲悉八大關鍵基礎設施受駭侵情事，除即刻立案偵辦，亦從個案受駭之主機找出駭客連線IP、駭客使用之工具程式、駭客散布之惡意程式、駭客使用之中繼站跳板，據此研判駭客所屬組織、國家、慣用模式及手法。藉由連線IP，結合公開情資，提供受駭機關後續處理建議，並研判有否其他政府機關、關鍵基礎設施亦在受駭範圍，機先阻斷駭客惡行，達成阻絕駭客攻擊之戰術目標。

(七)綜上，國家安全會議於民國（下同）107年9月14日提出首部國家資通安全戰略報告，提出「打造安全可信賴的數位國家」之戰略願景。在法令面，行政院於同年通過資通安全管理法及六項子法，將資通安全事務提升至法律位階，並於108年7月增訂國家安全法第2條之2，將國家安全之維護範疇延伸至網

際空間。在組織面，國家安全局更早至104年5月成立網域安全處，復於107年4月在「國家安全作業中心」成立專案小組，蒐研爭議訊息危安預警情資，法務部調查局亦於109年4月成立資安工作站等，在在顯示政府極為重視資通安全，而使我國得以完成初具規模之資通安全防禦體系，各相關機關允宜本於「國家資通安全戰略報告」之精神，在法令面、組織面及技術面持續加強推動，並加強戰術情報之情蒐及運用，以因應網路戰時代日趨嚴峻的國家安全挑戰。

二、基於情報單位保護情蒐管道之特性，國安局嚴格落實情報隔離措施固有其必要，惟在網路戰時代，情資之即時互相交流共享，對於資通安全體系之重要性自不待言，國安局如何兼顧情報隔離、情資共享及國際合作，允宜進一步與相關機關研謀強化措施。

(一)茲將國際上資安情資分享情形及其重要性綜整如後：

1、依據國家資通安全發展方案(106年至109年)：

（1）美國於2015年通過「網路安全資訊分享法」(Cybersecurity Information Sharing Act, CISA)修正案，更名為「網路安全法」(Cybersecurity Act of 2015)。此法著重於資訊分享，鼓勵企業主動分享情資，以獲得早期預警資料。同時允許ISP業者，可在資訊安全防護目的下，監控企業的網路系統。該法並指定由國土安全部建置網路威脅情資平臺，蒐集並分享威脅情資與預警訊息，以降低關鍵基礎設施的資安風險。

（2）日本於2005年通過「關鍵基礎設施資訊安全策

略行動計畫」，計畫中規劃關鍵基礎設施[2]資訊安全確保的安全基準指導指南、強化資訊共享機制、分析各領域關鍵基礎設施相依性、跨關鍵基礎設施領域的演習，以及資訊安全基礎的建構與國際合作等五大項目。此外，為了持續維持日本國內以及與東京奧運舉辦相關的關鍵基礎設施服務的安全性，日本內閣網路中心於2017年4月19日公布「關鍵基礎設施資訊安全對策第4次行動計畫」中在資訊分享制度方面，分享的資訊範圍應包含IT、OT與IoT的資訊，並排除資訊分享的障礙。

（3）2016年，德國制定了三項與資安有關的政策，其中「德國資訊安全策略」(Cyber Security Strategy for Germany)：強調對關鍵基礎設施的保護，**同時要求公私部門建立更廣泛的網路威脅資訊分享機制**，及協助私部門與公眾強化面對網路威脅的能力。

2、108年度國防報告書亦有「非傳統安全威脅（p19）：國際網路攻擊事件頻傳，所造成之經濟、軍事、科技損失，已構成全球重大安全隱憂。此類非傳統安全威脅具跨國特性，**須藉國際合作機制進行預防與管控**，以避免危害」之看法。

3、中央警察大學國境警察學系汪○○教授於本院諮詢會議提出：

（1）國安局並不是國安會提出《資安即國安戰略》的要角，雖然該戰略是以「情報導向」為主軸，且國安局一向不主動介入。理論上國安局應該可以做到先知快報，然而前提是**它必須建構完**

[2] 2005年日本關鍵基礎設施領域為：資通訊電信、金融、航空、鐵路、電力、天然氣、政府與行政服務(包含地方自治團體)、醫療、水資源與運輸等。

成一個涵善行政與國安體系之「資訊分享環境」(ISE)，此等功能要能夠發展則涉及了「準備」、「參與」、「駐留」和「查詢」等之資安專業。且除了一般情報圈固有的五大「情報來源」以外，國安局有沒有目前各國情報圈均共同關注的「網路威脅情報」之思考?

（2）特別提到，「資通電軍指揮部」被期待成為「第四軍種」，其實需要很多努力還有很長的路要走，以美國「網路司令部」來說，這是聯合作戰的必要一部分，又要處理「網路情報」。姑不論軍事作戰領域，光是網路情報領域部分，「資通電軍指揮部」就有很多工作要強化了。又如國防部之情次室來源與工作重點又和國安局不一樣，那應情報如何融合或切割？例如「爭議訊息」是與「網路情報」和情報的「戰略報告」是不一樣的。如何分而合之的有效處理，均是此平台建構必須考量的。

（3）今天網路戰的重點不在國安體系自己內部之情資蒐研與分發，而在於如何提供給關鍵基礎設施，使其能夠安全與持續發展的活下去，就像美國今天針對中國大陸之華為公司等之防範與打擊。但我們傳統情報之隔離特性，又怎麼去整合。因此，網路分享平台當然很重要，但不知國安局欲建構之平台是否有想的如此廣又遠且能具體的發揮效能。

（4）說到國際合作也有風險，那是雙面刃，涉及到網路與資安核心技術在合作時必須注意的各項問題，例如「工業控制系統」(ICS) 系統涉及實體與網路聚合之持續營運，且機密分類只是其中一部分的問題；純粹只談合作，可能我國

也會面臨來自美國竊取機密的風險。且合作之交流資料也必須符合國際規範的要求，例如前面提到之歐盟的《GDPR》。若以美國為例，以國安局長期跟美國「國家安全總署」(NSA) 等情報圈的友好關係，應該可以要求類似美國「國土安全部」國土安全情報資料網分享的作法，可以有某種議定書之簽定以進入他們有隨機及時序之機動密碼調整的網站，裏面的資料很豐富，但是情報交換還必須考量我們能拿什麼跟他們換？因為情報利益是很現實的，否則單方面的拿而沒有制衡機制，總究會被美國宰制。

4、中央警察大學朱○○教授在遠景基金會季刊第16卷第3期（2015年7月)「全球化時代情報在危機處理過程之運用」一文亦指出：

（1）美國國家情報總監克萊佩(James Clapper)，於2015年2月向國會表示,來自外國的網路攻擊對國家安全的威脅大於恐怖主義。同年2月25日，總統歐巴馬宣布，成立「網路威脅情報整合中心」(Cyber Threat Intelligence Integaration Center, CTIIC)，旨在強化美國防範和應對網路威脅的能力，是全國性的網路威脅情報中樞，隸屬於國家情報總監辦公室。該機構本身不從事網路情報蒐集，而是負責分析和整合國土安全部、聯邦調查局、中央情報局及國家安全局等情報機關所蒐集的網路威脅情報；加強政府各部門之間、政府與企業之間的協調聯繫和資訊共享，保護美國公民網路資訊安全，期能促使相關機關先期防範網路威脅，並採取因應對策，達到危機預防與危機處理成效。

（2）2004年911調查委員會(The 911 Commission)報告指出，911事件的發生是情報機關之間、機關內部，以及情報體系與政策官員之間，缺乏適切和充分的資訊分享(information sharing)所致。

（3）綜上可知，各情報機關之間、情報體系與政府各部門之間，長期以來存在機構間隙、本位主義及情報分享等層面問題，缺乏有效的溝通與協調，致使獲取的情報無法適時地發揮最大效能，導致情報失敗。

(二)有關爭議訊息之情資分享及查處

1、摘錄國安局108年5月2日赴立法院第9屆第7會期外交及國防委員會報告「中國假訊息心戰之因應對策」:

（1）尋求國際友邦合作：西方民主國家近年因華為設備洩密疑慮、孔子學院涉間諜行為等事件，對中共反感日增，爰各國當前官、民、學界及智庫等友我力量正逐漸匯集，我宜思考以民主、人權等普世價值，作為雙邊「戰略溝通」主軸，持續推動「反制網路攻擊、抵制不實訊息之戰略聯盟」，以結合各理念相近國家成為「利我之支撐力量」。

（2）截長補短主動出擊：中共近來制臺打壓野心日益增強，官方頻藉陸媒公然對我威脅示警，並於幕後操控網路水軍精進網路偽（變）造及匿蹤技術，預判陸方未來對臺爭訊攻擊手段勢必更加精細難辨，國安局將結合大數據系統分析技術，即時掌控分析中共網路水軍攻擊態樣，並強化反制能量，俾利發揮「蒐報快、通報快、應處快」之效能，落實爭議訊息防制工作

2、次據該局赴本院簡報時說明：

（1）爭議訊息部分，無論川普或馬克宏競選都曾發生過，目的是干擾大選，而且是不是只影響輿論，更是結合駭客技術，偷取重要金主及參謀資訊等等競選資料，利用這些情資來布放爭議訊息，當下歐盟有成立混和戰因應中心，國安局也才知道歐洲已經第一時間面對蘇聯的威脅。下一個觀察重點是美國下半年大選，是否俄羅斯或中共的駭客編組會再運作。

（2）國安局從107年4月月開始參考俄羅斯併吞克里米亞及美國大選中來自其他國家的影響，有隱匿性高傳播快速等等特性，因此針對這些會影響國家安全和社會安定的資訊開始情蒐，並且通報國安會及行政院資安處，我們為了具有嚇阻力，就透過偵訊防治鐵三角（警政署、調查局和憲指部)，對散播爭議訊息的帳號進行偵辦。早期國安局為了不閉門造車，我們曾廣蒐國外做法，歸納出來就是一是立專法，二是賦予專門機關權責，三是要求媒體自律及第三方查核機制，四是提高民眾意識，我們後續向國安會報告此事也提供給立委和行政院，行政院後續責成羅○○政委啟動檢討和盤點各部會的偵訊防制相關修法，例如成立社群平台、澄清專區、台灣事實查核中心等等，國安局都曾提供建議。

3、國安局表示，以處理與疫情有關之爭議訊息為例，自本(109)年1月17日至3月17日止，協同國安團隊蒐報有關「嚴重特殊傳染性肺炎」疫情之爭議訊息，編列通報單計226則，其中203則送行政院參處，另循「爭訊防治鐵三角機制」 通報

警、調、憲等單位參處計50則。

4、依據本案赴國安局座談時，該局亦表示，在爭議訊息部分，是和九大情報機關重疊著做，才能做交叉比對，訊息真假國安局不進行判斷，除非明顯為假，所以我們是通報行政院，再請部會去查證判斷，例如水庫被倒文旦，這部分我們通報行政院，行政院再通報農委會後續查處。

(三)茲將國安局及其他機關對於如何兼顧情報隔離與情資分享之看法臚列如下：

1、國安局：

（1）CTIIC是在美國國安部轄下，是前幾年成立的，是情資彙整中心，我國目前是沒有單一單位辦理這個角色，但是在資安及國安的戰略下，國安局責無旁貸是提供敵情的角色。不管是否是中共的威脅，我們蒐集情資後，其中政府機構部份我們會送行政院資安處辦理。如果是政府服務網GSN上的惡意活動的防禦,是由技服中心負責監控，技服中心的功能上基本上是沒有CTIIC這麼強，除了由情報機關做情蒐之外，技服中心也會彙整情資反饋國安局，作為後續蒐情部署參考，這是一個循環的過程。

（2）至於八大關鍵基礎設施的防禦，分別由資安會報下的一個分組來負責，我們跟行政院資安處互動密切，每月都召開例會，國安局也會派人參加，資安鐵三角的月會，國安局也每個月都會參加

（3）雖然我們不是資通安全管理法的規範對象，但是我們也有情報機關資通管理規範的相關規定，使情資分享有所依據。

2、行政院資安處：

（1）我國除面對傳統網路攻擊外，針對新興之混合式威脅，須強化相關預警機制，包含獲取境外勢力情資、關聯性分析及即時交流，以期儘早阻絕可能之攻擊

（2）**我們最需要境外勢力的資訊，因為我們對國內的蒐集很容易，但行政院資安處的能力不及於國外，這部分期待與國安局有更多合作**。

（3）現在預警機制都和國安局合作得很好，利用此一模式已可以因應新興威脅，暫時沒有成立如美國CTIIC及歐盟混和戰威脅因應中心之需求。

3、調查局：

（1）該局情報工作，係透過全國各地外勤人員，以轄區經營方式走動式蒐情，取得相關情報且相互隔離，後依情報類型，透過局本部專責單位統籌、分享，並視狀況與友軍單位橫向交流，以此架構下進行情報分享與互動，並落實情報隔離。

（2）我國已有對資訊安全情報分享之機構，如台灣緊急應變處理中心(TWCERT)、教育機構有TANET、金融機構有相關CERT，調查局更與台灣網路危機應變處理中心、關貿及美國微軟公司簽訂合作備忘錄，以達到情資互享互助合作之效用，並積極參與國際研討會議進行情報交流。

（3）目前國際間，美方設有CTIIC(Cyber Threat Intelligence Integration Center)之架構，係建立一個私部門與公部門對於網路安全情資之分享平台，我國可以比照類似概念，成立窗口，加強資安情報之橫向聯繫，以供司法及國安等後續調查。

（4）該局並於座談時補充如下：

〈1〉各轄區的調查員彼此是情報隔離的，集中後才綜合研判，此外也與其他情資來源進行交叉比對。

〈2〉調查局所列案件在線索發現方面的管道，一是全國都有調查處站，平常就會做資訊收集，也會回報，這占了局裡一半的角色。所以這有可能是主動發掘，後續構成法辦要件就會立案調查。另一個是透過被駭侵案件去查處，也就是從案中找案。

4、資通電軍指揮部：

（1）兼顧情資分享及情報隔離方面，該部依國防部及國安局指導情蒐要項，進行情報專案情蒐作業，簽奉主官核定後，非編組人員不得參與或查閱，以執行情報隔離。而情報處理流程區分蒐集、處理、分發及運用等，於處理階段界定機密等級及可分發之單位等，以利進行後續分享與情資單位互動。該部並於座談時補充，「均依照國安局情蒐要項做情蒐，除非主管批准可以分享，否則原則上是情報隔離」。

（2）至於如何強化情資分享及美國CTIIC及歐盟混和戰威脅因應中心等作業模式之參考價值方面，該部運用國軍MSOC統計軍用民網網攻威脅情資，並研析相關威脅來源，透由國防部將研析資料提供N-ISAC參用。針對CTIIC及歐盟混和戰威脅因應中心，任務主要為整合網路威脅情報，其成功原因為情資互信機制下的情報透通。該部並於座談時補充「現在預警機制都和國安局合作得很好，利用此一模式已可以因應新興威脅」。

(四)綜上，基於情報單位保護情蒐管道之特性，國安局

嚴格落實情報隔離措施固有其必要，惟在網路戰時代，情資之即時互相交流共享，對於資通安全體系之重要性自不待言，國安局如何兼顧情報隔離、情資共享及國際合作，允宜進一步與相關機關研謀強化措施。

三、國安局在網路戰中定位本身任務屬於單純情蒐性質，攻勢作為亦為國際慣例所禁止；惟為避免我國在網路戰欠缺主動權之不利條件下，進而壓縮網路空間之防禦縱深，使相關權責機關疲於奔命，國安局及相關機關宜於資通安全防禦體系成型，以及守勢作為例如惡意程式分析及爭議訊息澄清等略具成效後，進一步配合行政院資安處「主動式防禦」構想，研謀精進措施並爭取充分資源，俾重層保障國家安全。

(一)情報機關對於本身任務之定位

1、據國安局赴本院說明，在面對網路戰威脅部分，受情工法授權，國安局單純負責情蒐工作，依據資安鐵三角的指導辦理。

2、不管是國內或其他國家情報機關，情報單位都是情蒐功能，攻的部分主要是軍方，防的話是行政機關，情報機關對於攻防都沒有參與。

(二)承上，該局雖說明其任務不涉攻防，惟針對委員假設「但是如果要拿到秘密情報，就可能需要進入敵方網路」一節，該局亦不否認情蒐工作完全跟攻防無關，美軍在這部分也是分成三塊，就是攻、防和蒐，蒐的手法當然也可以應用在攻和防。

(三)本院辦理諮詢會議學者專家有關網路戰攻勢作為或主動式防禦之看法如下：

1、中央警察大學國境警察學系汪○○教授：

(1)「混和戰」是在戰爭界線以下，有「非歸屬性」和「模稜兩可」的特性，所以才能運用「灰色

地帶」,例如海巡署面對的中共漁船(或是海上民兵)問題,難在沒有歸屬或法源,就不好去處理。

(2)全世界之情報理論與實踐,均是分為「情報」和「反情報」兩大不同但又必須合作的領域,我國長期以來並沒有「反情報」的觀念,國安局透過《情工法》把反情報窄化為情報工具,迄今反情報並沒有發揮應有之功能,仍局限在保密與防諜。

(3)所謂防護能力只是一面,任何網安部門還必須有攻擊能力,第七處我想應該不會只是做防衛工作,像白帽駭客;若該處不具有攻擊能力就不可能達成全面防衛的要求。

2、中央研究院資科所李○○客座講座:怎麼定義網路攻擊?依照北約所制訂的塔林手冊,主權的概念到哪裡?如果網路攻擊到主權或關鍵基礎設施,我們就可以定義是網路戰,也因為塔林手冊提到的主權延伸概念,我們也就把國安法第2條之2就修法到把網路空間也納入,既然關鍵基礎設施有防禦機制,策略報告有提到要建立資安情資分享及分析中心(ISAC)、資安維運及預警中心(SOC)及通報應變。

3、國防大學中共軍事事務研究所陳○○助理教授:混和戰、資訊戰和網路戰三者的共同點都是具有政治目的、速度快、隱蔽性、不易追查等,這在2014年俄羅斯入侵克里米亞都呈現過相關概念,而且有複雜性和攻勢主動權,能夠運用網路平台使得攻擊者得以掌握主動權。

(四)綜整各機關對於網路戰攻勢作為及主動式防禦之看法如下:

1、國安局：

（1）攻勢反情報或是戰略威嚇或及反向深入等等，考量到我們要維持情蒐管道的安全，所以不會輕易動作。

（2）網路戰工具難以取得，被用過一次都會產生數位指紋，一旦被做成IOC放進網防系統，該武器就會失效，因此非常珍貴，和傳統動能武器有相當大的不同。

（3）拓展到大陸範圍時，就必須和軍情局或電展室合作。

2、行政院資安處：

（1）該處認為，為有效降低資安威脅風險，除強化資安防護機制外，亦可透過預警機制，儘早發現可能的攻擊並加以阻絕，該處刻規劃透過大量情報、數據及資訊之分析及交叉比對，將資安防禦機制提升至主動式防禦，期將可能的攻擊阻絕於更前方。另建議強化情資接收者回饋機制，透過情資之持續優化，深化我國資安防護。

（2）該處簡處長並補充：「建議彙整各機關過去蒐集之資料，再導入更有效的交叉比對分析作業，可以把防禦線再往前推進一步」。

（3）此外，簡處長亦針對我國在網路戰為何只有挨打沒有攻勢進一步說明，是因為在國際法上不允許攻勢作為，國際尚有進行攻勢的國家也就是北韓、蘇聯、中國那幾個國家，塔林手冊也規定只有受到攻擊才能反擊，而且網路戰通常沒辦法確定攻擊來源，我們只能依據攻擊樣態來判斷來源，因為連IP是可以偽造的。因此行政機關不會談攻擊，只會談主動防禦。

3、資通電軍指揮部：

（1）該部針對中共自主研發軍/民資通訊軟硬體及系統，該部持續透過公開情資研析，研判其功能規格，包含資訊及網路設備，如中興網路設備。並建議由國內專業的學研機構對特定專屬系統執行研析，並提供給國安團隊，以增進國家安全。

（2）該部並於座談時補充，依照國防部命令情蒐，例如中共軍事目標做弱點分析，來發現弱點，以利戰時運用。至於中共自研系統，該部都是以公開情資去研析，如果有國內專家願意進行研究更佳。

（3）在資電戰力部分，包含人才裝備技術方面都在逐步達成，按國際經驗，要形成完整戰力都需要時間。由於情工法修法，該部才剛被納入國安體系，不管作業面還是技術交流和會報等等都會積極參與。

4、調查局則表示，有關攻勢反情報(offensive Counterintelligence)部分，該局定義其為一種散布假訊息給敵對情蒐人員，使對方誤判，掌握到錯誤的情報，該局並未進行攻勢反情報之作為，亦未有這樣之專責單位。

(五)小結：

1、網路戰有不易歸責特定勢力及缺乏接戰準則之特性，而我國目前面對網路戰威脅僅採取守勢，以致敵對勢力之攻擊成本低廉而無須考量合法性及正當性，而得以不斷測試防禦體系之能力與反應，並使盟國難以採取支援行動，此等優勢於俄國在烏克蘭之行動中屢見不鮮。

2、行政院資安處做為我國資安防禦體系之核心及

「資通安全管理法」之主管機關，業針對攻勢作為有違「塔林手冊」及國際慣例予以釐清，然該處亦同意將防禦線往前推之「主動式防禦」有其必要。

3、本案所涉情報機關中，國安局定位本身任務僅有情蒐而不涉攻防，調查局未有相關專責單位，而資通電軍僅能依公開情報針對中共自研系統進行研析，益證汪○○教授所表示我國情報機關在「情報」及「反情報」方面未有明確分野之情形。

4、相關機關對於目前中共自主開發之系統或硬體（如鴻蒙系統、UOS系統、北斗衛星、第三代身分證、華為5G設備等）研析工作顯然缺乏主責機關，更遑論探討人力及資源是否充分之課題，倘我國對於相關系統未有相當程度掌握，未來發生實際攻防將無著手之處，亦不利爭取戰略縱深或遲滯敵之攻勢，恐置我國資通安全，乃至於國家安全於潛在風險之中。

(六)綜上，國安局在網路戰中定位本身任務屬於單純情蒐性質，攻勢作為並依「塔林手冊」為國際慣例所禁止；惟為避免我國在網路戰欠缺主動權之不利條件下，進而壓縮網路空間之防禦縱深，使相關權責機關疲於奔命，國安局及相關機關宜於資通安全防禦體系成型，以及守勢作為例如惡意程式分析及爭議訊息澄清等略具成效後，進一步參考行政院資安處「主動式防禦」構想，研謀精進措施並爭取充分資源，俾重層保障國家安全。

四、網路戰之情報作業流程均涵蓋「指導」、「蒐集」、「處理」、「運用」等步驟，而情報品質或效率之日益精進，雖可透由循環式品質管理之計畫、執行、檢核及改善等步驟來達成，但其中較能發掘組織盲點之外部檢

核，較難為重視保密及專業之情報機關所接受，惟國安局既為情報工作之主管機關，面對日益複雜之網路戰型態及龐大資訊量，允宜考量在保密及專業前提下，適度引入外部檢核概念，精進人員專業能力，同時與國內相關機關或民間資安業者交流，全力培養專業人才，確保對資安侵駭系統或技術之與時俱進，俾持續提升情報作業之品質及效益。

(一)依據國安局及其他情報機關提供資料，因應網路戰之分工如下：

1、在架構面，依據「國家資通安全戰略報告」內容中「建立以情報驅動之國家資安聯防架構」中提及，國家資安聯防體系的建立，包含由國安單位及行政院各部會，分工籌組並整合資安緊急應變小組、資安事件通報及處理小組、資安維運及預警中心、以及情資分享與分析中心等單位，建立以「情報驅動」(資訊分享並協同應變)的資安聯防架構，提升早期預警、緊急應變及持續維運的能量及效率。

2、摘錄國安局政策方針涉及網路戰情報品質及流程者如下

(1)「研整關鍵戰略情資、確保國家安全利益」：內容略以「.....依國安會指導，以『先知快報』為導向，掌握大陸、國際情勢發展，即時蒐整關鍵性戰略情報報告，呈報層峰及分送政府部會，作為政府決策參考，發揮情報支援決策功能.....」等語。

(2)「提升科技情報能量，強化我資安防護網」：面臨中共銳實力及5G通信技術發展迅速，且持續發佈爭議訊息，對我國政、經、軍、心產生嚴重威脅，將賡續整合產、學、技、研提升科

技情報作業能量，並精進資安防護技術，強化保密系統整體防禦能量。

3、國安局赴本院簡報時亦說明,「.....除了由情報機關做情蒐之外，技服中心也會彙整情資反饋國安局，作為後續蒐情部署參考，這是一個循環的過程」等語。

4、綜上，無論整體資安防禦體系如何組成或分工，均顯示網路戰情報之提供及使用既分屬不同單位，則情報提供者所提供之情報品質良窳或時效，顯然對於使用單位運用之成敗有相當程度關連，並與循環式品質管理Plan-Do-Check-Act之步驟及原則相符。

(二)有關情報作業之流程，以及如何使整體流程高效順暢而獲致良好情報效益，可參考相關學者之論述得其梗概如下：

1、中央警察大學國境警察學系汪○○教授：

（1）情報循環一般指的是「指導」、「蒐集」、「處理」、「運用」四個主要部分，而各國或有關的情治部門可以自己再去細分，但是均以此四個階段為主軸。則請問誰給國安局「指導」？國安會的專業是否足夠可能指導?

（2）但傳統上，國安局需要「保密」，誰都不知道他們在幹嘛?而此種特徵可能也會影響此平台之建構及民眾對其可發揮功能的信心。

（3）現在好像沒有評估機制來評估國安局的工作績效?國安局自己說了算,沒有人有能力或授權可以質疑，這也可能是造成他們保守的原因之一。最近媒體大肆報導國安局局長對北韓領導者判斷之錯誤說法，可能就是此等問題的核心必須正視。

（4）美國有《督察長法》有一個直接向總統負責的「督察長」機制，可以從情報圈內部來進行人權與業務的監督，但是我們純由國安局領導的機制下卻沒有此等設計。

（5）資訊與網路安全是以「生命週期」去建構與評估其「安全」與「保安」，但目前實在是不知道國安局是怎麼驗證自己有沒有此等功能，或者是他以機密為由也不允許有客觀的「第三方」去評估，但**除非國安局拿得出評估指標，類似KPI的東西，否則我們無法驗證國安局有沒有此等能力**，就會變成「一言堂」，他說了就算，但危害卻仍存在。

2、中央警察大學朱○○教授在遠景基金會季刊第16卷第3期（2015年7月）「全球化時代情報在危機處理過程之運用」一文：

（1）依情報活動是指情報體系之實際運作，涵蓋情報蒐集(intelligence collecton)、情報分析(intelligence analysis)、反情報(counterintelligence)及祕密行動(covert action)四項密切關聯的情報要素(element of intelligence)。全球化時代情報蒐集途徑與方法，包括人員情報(Human Intelligence, HUMINT)、科技情報(Technical Intelligence, TECHINT)及公開來源情報(Open-Source Intelligence, OSINT)，通稱全來源情報(All-Source Intelligence)。此外，受到資訊化趨勢的影響，網路情報(Cyber Intelligence)和戰略情報、預警情報併列為當代情報重要任務目標之一，情報蒐集途徑與方法可整理如下表2：

表2. 情報蒐集途徑與方法				
類型				內容要點
全來源情報	人員情報	公開人員情報		具官方掩護身分，以外交官或其他政府官員身分派駐國外。
		秘密人員情報		非官方掩護身分，以商人、記者、學生及遊客等掩護身分偽裝。
	科技情報	訊號情報	通訊情報	透過欄截二方以上的通訊所獲得之情報。
			電子情報	截收、處理、分析軍用設備工作時的非通訊電磁輻射而得之情報。
			遙測情報	欄截各種武器系統測試階段所傳遞資料而得之情報，如飛彈試射。
		地理空間情報		利用衛星或空中偵察機系統所蒐集的照片或數位影像情報
		測量和識別情報		使用尖端科技感應各種現代化武器所使用之材料
	公開來源情報			經由各種公眾可取得的管道所蒐集之公開資訊
資料來源：遠景基金會季刊第16卷第3期「全球化時代情報在危機處理過程之運用」				

（2）情報循環(intelligence cycle)是研究情報理論與情報過程實務運作的基礎。情報界為凸顯並強調情報實務運作整體過程中，每一個環節之重要性、聯結性與關聯性缺一不可，亦即著重彼此之間的溝通、協調與整合，亦有將其稱為情報過程，是連續的動態發展過程，必須注意情報體系的計畫及流程的效率。

（3）情報過程包括計畫與指導(planning and direction)、情報蒐集(intelligence collection)、處理與淬取(intelligence processing and exploitation)、分析與產製(analysis and production)、分發與運用(dissemination and consumer)及評估與反饋

(evalution and feedback)等六個步驟；各階段並非單向、閉鎖式的循環狀態，而是各階段間彼此互動、循環往復、相互影響。其中，溝通(communication)是情報過程中的潤滑劑與軸心，具有四項功能如下，若缺乏溝通的協調聯繫作用，則對目標、威脅認知、環境動態發展之調適等皆可能產生負面效應，減損情報效能。

（4）2004年911調查委員會(The 911 Commission)報告指出，911事件的發生是情報機關之間、機關內部，以及情報體系與政策官員之間，缺乏適切和充分的資訊分享(information sharing)所致。綜上可知，**各情報機關之間、情報體系與政府各部門之間，長期以來存在機構間隙、本位主義及情報分享等層面問題，缺乏有效的溝通與協調**，致使獲取的情報無法適時地發揮最大效能，導致情報失敗。

（5）**情報與政策實乃雙向互動關係，情報服務於政策，政策需要情報，二者是相互依存關係。**政策制定者應充分掌握並指導情報要項優先順序之情報過程，情報體系則扮演協助者、輔助者及諮詢者的角色，為使用者提供所需要的情報，俾利制定國家政策之參考，以謀求國家利益之最大化與最小損害。

(三)爰此，無論是循環式品質管理中的「check」、汪○○教授所稱「好像沒有評估機制來評估國安局的工作績效」以及朱○○教授所稱「評估與反饋」步驟，均顯示除了機關本身的內控機制以外，客觀之反饋、評估或檢視機制有存在必要。

1、情報機關所提供之情資品質及時效是否需要檢

討調整，應由下游使用機關或客觀第三者，就相關情資能否達成達成「驅動」資安即國安戰略加以反饋、評估或檢視，始能引導情報單位之情蒐方向、管道或效率滿足使用單位需求。

2、以本院調查銓敘部個資洩漏案為例，案發前該部歷年均通過委外廠商之ISMS驗證，直至案發後具客觀立場之行政院資安處率專業團隊深入稽核，始發現諸多資通安全漏洞或未能落實執行之處，並指出該部資通安全相關委外事務有「球員兼裁判」之虞，而未能收互相監督制衡之效。而外部檢核具有協助組織發現本身盲點之功能，亦非僅銓敘部一案可證。

(四)茲綜整本案涉及機關對於網路戰情報循環式品質管理或外部評估機制之看法如下：

1、國安局說明係由國安會資通安全指導小組每季檢討該局績效，不會球員兼裁判。

2、資通電軍指揮部表示，該部依國安局情蒐要項所獲情資於內部機制審認，再與其他情資交叉比對後，依情報傳遞流程回報需求單位執行績效評鑑，並藉由評鑑結果納入後續情蒐精進方向。

3、關於情報單位如何善用循環式品質管理(PDCA)原則進行品質管理部分，調查局則認為：

（1）情報工作會動態檢討機制流程，進行評估、調整與監控，因此情蒐單位將遵循已訂定之程序，包含：該情報目標為何、蒐報重點為何；評估可由哪些資源開始著手，持續進行程序與時程為何；所蒐集情報要如何運用回饋，在過程中有無標竿情報可當成檢驗基準；以成果再評核是否需要改變情報蒐集內容與方式等。

（2）行政機關為了加強內部監督，會設立獨立監察

機制，要增加第三方進行評估，需考慮該第三方是否懂得情報工作相關事項，若無經驗者來實行，可能無法達到監督效果；惟情報貴在時效及運用，有些情報在特定時段的價值很高，但過了一段時間後就變得沒有價值，績效評估標準若不夠具體，就無法客觀衡量比較。

（3）情報機關顯然不適合與行政機關一體適用於公開績效指標來評估情報績效。

4、小結：參照國安局及調查局之說明顯示，情報機關基於保密及專業考量仍偏好採取內部稽核，則相關機關亦應參考國外制度設計，研謀有效避免內部稽核先天缺陷之評估方式，使情蒐工作得以適當被引導至符合政府決策及運用所需。

(五)在精進人力資源及培訓部分:

1、根據「國家資通安全戰略報告」中「**資安人才培育及留才策略**」中說明，推動資安人才培育策略，係以「跨域試煉」為主軸，由教育部提供資安扎根正規教育，科技部和經濟部提供實作場域試煉，培育出國家、國防、關鍵資訊基礎設施、打擊犯罪及產業所需的資安人才，以強化我數位國家發展的根基，並透過以下四個方式來達成：

（1）扎根正規教育，培育實作人才。

（2）養成職場菁英人才。

（3）建立機動性及彈性延攬資安人才機制。

（4）建立並落實資安人才培育藍圖。

2、次據法務部調查局於本案座談中分享如下，值得各相關機關參考。

（1）調查人員特考有資訊科類組，先期就有專業需求經過一年訓練，原來是資訊科學組就會在技術面上再精進。非資訊科學組只會有基本教育。

（2）調查局資訊類組的人會請資通安全處去做全局人力配置，臺北市因為機關較多，當地調查處站就會有較多資安專業人員。到目前資安人力培訓很少發生轉換跑道的情形，顯示人員素質相當穩定。

3、此外，行政院資安處亦在規劃現行資訊職系以外，另行增設資安職系，將資通安全於政府部門中進一步專業化，在在顯示政府對於資通安全之重視。

4、另以，針對中共因應不同議題與事件發起之網路戰，該局能即時調整網蒐作業面向，並彈性佈署網蒐人力運用，而中共亦自主開發系統或軟體，如華為(含鴻蒙)、北斗衛星、華為5G、UOS（統一作業系統, unity operation system）等，且網路戰使用工具及網蒐作業技法亦因網路戰特性而隨時演進，再者中共駭客組織更以對我國網路攻擊做為試煉場域等情，均涉及專業人員素質、技能、設備、情報敏感度等。凡此網路戰情蒐過程中對資訊系統之高度專業性、情報的評估與反饋等均有賴人員素質與技能之提升，網安情蒐能量之情報工作涉有其獨特性及機敏性，除形成國安局內部自我強化訓練外，允宜與國內相關機關或民間資安業者交流，以確保對資安駭侵系統或技術之與時俱進，掌握多元情資及技術，藉以精進人員之專業能力。

(六)綜上，網路戰之情報作業流程均涵蓋「指導」、「蒐集」、「處理」、「運用」等步驟，而情報品質或效率之日益精進，雖可透由循環式品質管理之計畫、執行、檢核及改善等步驟來達成，但其中較能發掘組織盲點之外部檢核，較難為重視保密及專業之情報

機關所接受，惟國安局既為情報工作之主管機關，面對日益複雜之網路戰型態及龐大資訊量，允宜考量在保密及專業前提下，適度引入外部檢核概念，精進人員專業能力，同時與國內相關機關或民間資安業者交流，全力培養專業人才，確保對資安侵駭系統或技術之與時俱進，俾持續提升情報作業之品質及效益。

五、**為防止侵害人權情事，相關法令對國安局及法務部調查局等機關進行情蒐或調查之範疇、對象及內容等，均訂有嚴謹規範。惟網路戰之三大型態包括駭侵、關鍵基礎設施服務中斷及爭議訊息，均有利用跨國企業行動及網路設備、民營ISP業者或國際社群平台及群組為工具，而遂行其隱匿攻擊來源及模式之目的，或將形成情蒐及執法之灰色地帶，並使相關機關容易陷於侵害人權之指控；而公、私部門遭網路攻擊後以恢復服務為導向之搶修方式，更增加了蒐證及調查的困難。爰國安局、法務部調查局及相關機關，在國安法第2條之2將國家安全範疇延伸至網路空間之際，允宜通盤檢視相關法令及既有作業模式，以因應日趨繁複之網路戰趨勢**。

(一)為防止侵害人權情事，相關法令對國安局及調查局等機關進行情蒐或調查之範疇、對象及內容等，均訂有嚴謹規範，茲就相關規範臚列如下：

1、國安局

(1) 國安局無論赴本院簡報或赴立院報告時，均曾表示該局係依「情工法」主責外國或境外敵對勢力網安情蒐工作，如涉境內設有戶籍對象者，移請警、調依「警察職權行使法」及「調查官職權行使法」偵辦。換言之，國安局之職責不及於敵對勢力在境內活動之情形，境內部

分是由調查局和警政署來負責。

（2）該局並表示，國內有多個電腦被利用當中繼站，這時就必須和司法警察體系合作，再回饋給行政體系。

2、調查局於本院赴國安局辦理座談時，亦針對基於我國相關資通訊服務多為國際企業，關鍵基礎設施亦非全為國營企業，則如何在此條件下兼顧人民隱私權及情蒐效率或品質表示：

（1）以關鍵基礎設施遭到網站攻擊而言：中油、台○及力○等關鍵基礎設施及上市櫃高科技公司遭勒索病毒攻擊等案件，在偵辦過程中，第一時間受害公司大多報案意願不高且對案情多有所隱瞞，而中油公司屬於國營事業單位，尚能在政風單位之協助下進場調查，對於台○與力○等私人企業，若不肯報案，司法單位則無相關法令依據可進入現場了解，此類加密勒索案件，普遍發生在國內企業，不為人知必不在少數，若國內國安、司法單位無法掌握狀況，對我國家安全、科技與經濟發展是一大隱憂，**政府應訂定相關法令，授權司法單位在一定層級以上之資安事件發生時，可以介入調查**。

（2）至於關鍵基礎設施之八大領域主要部門網路系統並非全部採用GSN(政府網際服務網)，調查局進行調查作業是否遭遇困難之建議如下：

〈1〉強化證據保全：當**有關單位發生資安事件，為儘速恢復運作與杜絕入侵管道，常任由資訊服務供應商重灌有問題之主機或不配合司法單位進場調查，導致相關跡證無法取得或遭抹除**，或調查境外駭客租用我國內VPS廠商或二類電信之服務遭業者向承租人告

知，應研提辦法納入相關權責單位之配合義務，予以究責。

〈2〉建構良好溝通管道：有關單位之資安團隊應與委外資安公司建立聯繫管道，除駭侵事件的立即通報外，應研提辦法整併各資安公司資安情資，以完善資通安全情資分享，俾利於駭侵鑑識作業

（3）至於爭議訊息之查處與情蒐部分

〈1〉民眾為使生活更加便利，常自行於該等雲端服務上留下諸多個人基本資料，惟觀大多平台之功能，須經過本人同意方會於網際網路公開個人資訊，可被任意人蒐尋、觀看，即認定該等資料已屬於公開情資範疇，因此運用網路蒐得之情資，**即使情資內容夾雜許多民眾個人喜好及相關交友狀況，應可認定該等資料係公開情資**。

〈2〉而國際間之網路通訊服務平台業者，能否妥善管理我國民眾之資料，**我國政府如何管理和規範，在保障我國人民隱私前提下，進行國安情資蒐集與犯罪調查，而不受制於業者之配合度，確實是當前重要課題**。

〈3〉調查局當前做法係積極與平台業者建立窗口進行資料調閱之程序，**後續希從法律面建立相關平台之監管機制**。

(二)而事實上，網路戰與過去傳統衝突差別最為顯著之處，咸認在於其平戰、境內外、歸責、溯源、法源、接戰準則及隱私權之定義模糊及困難，例證如下：

1、2018年3月國防譯粹（第45卷2期）「定義新型態俄式資訊作戰」：**網路空間和社群媒體的種種作為甚難明確歸究於正式的俄羅斯權力手段，因此**

讓俄羅斯的宣傳機器可以否認涉入這些行動。少了被認定為正當或具公信力的負擔或先決條件，俄羅斯資訊作戰行動可以透過不斷以各種可促成其利益的訊息充斥資訊空間，以扭曲、捏造和製造各種輿論風向。

2、國安局於108年5月2日赴立法院第9屆第7會期外交及國防委員會報告「中國假訊息心戰之因應對策」：中共刻正複製俄羅斯併吞克里米亞島的模式，**利用我國民主社會、資訊傳播環境與方式之自由開放，以及各種法律層面之不足與漏洞**，意圖以散播爭議訊息對我遂行「認知作戰」。

3、據調查局提供本院看法略以:「.....包括**多數假訊息難以溯源**，以過往偵辦假訊息案件經驗，性質多為高隱密、匿名而難以取證至源頭，實際操控之黑手隱身幕後。」

4、摘述中央警察大學朱○○教授在遠景基金會季刊第16卷第3期（2015年7月)「全球化時代情報在危機處理過程之運用」

（1）美國和英國的《國家安全戰略》報告，皆明確指出當前面臨的傳統和非傳統安全威脅，可能來自國家、非國家行為體(non-state actors)、次國家行為體(sub-state actor)及其他跨國力量(other transnational force)。

（2）網路運用的動員功能，**突破主權疆界的藩籬**，具有迅速串聯及無遠弗屆的滲透力與感染力，集結各式各樣、彼此互不相識的人，針對同一目標採取一致行動。

(三)茲綜整本院辦理諮詢會議時學者專家針對本項結論之看法：

1、中央警察大學國境警察學系汪○○教授指出：

（1）**「混合戰」是在戰爭界線以下，有「非歸屬性」和「模稜兩可」的特性，所以才能運用「灰色地帶」**，例如海巡署面對的中共漁船（或是海上民兵）問題，難在沒有歸屬或法源，就不好去處理。

（2）情報怎麼樣才可以安全又兼顧符合透明化不違反人權？當然可以達成，例如美國「情報總監辦公室」都有透明化的年度報告公布，分為機密和非機密的版本。

（3）通保法規定戶籍設在國內要法院授權，國安局標準當然可能和法院不同，真的在做這個報告時就會碰到問題。

（4）談隱私權保障，目前此等法律的保障其實不夠，而且執行起來有模糊空間，特別若又是涉及國家局之情報單位主導，就很容易變成「政治議題」。

（5）特別是在進行「大數據」分析時，之前的「海撈」也一定會有對象，問題是此對象是之前「針對性」還是「隨機性」，且接續這些資料如何處理?保留多久?是否有補救措施均是必須審慎思考的。

（6）對於處理恐怖份子這部分的問題，我們仍有很大的努力空間。但最基本的，現在連恐怖份子的定義都沒有，完全依靠美國提供的名單，對於處理上會有困難也不利安全之維護。且假設未來如果某些沒有犯罪前科且經由美國或德國等友我之民主國家來到臺灣的人，卻惡意傷害大陸人，則中國引用其依於國際反恐文書而訂立之反恐法對我國作出一些法律上之要求，我們在處理上就可能馬上面臨一些「兩難」的問

題。

2、中央研究院資科所李○○客座講座：雖然國安局負責國外，調查局負責國內，但是現在有內部人民和境外有連結，做各種傳訊或介接，他們又如何進行處理？

3、國防大學中共軍事事務研究所陳○○助理教授：隱私權部分，這個平台可涉及情報蒐集，所以他有必要在建置之前就有充分的法源。我們其實可以看到國安局和立法單位並沒有充分的共識。

(四)另查，「資訊戰爭」一書作者David E. Sanger亦於「中間人」專章詳細說明美國聯邦調查局與科技公司（如Apple、Google）就國家安全與客戶隱私權保障議題之間的衝突與協調如下，我國公私部門間雖未有如此明顯的齟齬，仍值得國安局及調查局參考。

1、站在國安機關立場，科技公司開發之加密系統或無金鑰之保密設計，等同提供恐怖份子或間諜低廉的秘密通訊手段，而調查局將被鎖在系統之外，時任聯邦調查局局長柯米（James Brien Comey, Jr.）並將之比喻為「沒有鑰匙的公寓大門和汽車行李箱」，會對合法的搜索造成妨礙，而此在真實世界是不可容忍的，則為何在數位世界應得到容許？

2、惟蘋果與Google公司則表示，因為美國國家安全局無法妥善管制內部人員，導致全世界的人都要求蘋果公司證明資料安全無虞，這是「華府自找的」。而蘋果執行長庫克亦主張，聯邦調查局天真的以為如果科技公司做了個鎖，並把鑰匙交給聯邦調查局，其他人（例如俄羅斯、中國及北韓

駭客）都不會找出撬開鎖的方式。

（五）綜上，為防止侵害人權情事，相關法令對國安局及法務部調查局等機關進行情蒐或調查之範疇、對象及內容等，均訂有嚴謹規範。惟網路戰之三大型態包括駭侵、關鍵基礎設施服務中斷及爭議訊息，均有利用跨國企業行動及網路設備、民營ISP業者或國際社群平台及群組為工具，而遂行其隱匿攻擊來源及模式之目的，或將形成情蒐及執法之灰色地帶，並使相關機關容易陷於侵害人權之指控；而公、私部門遭網路攻擊後以恢復服務為導向之搶修方式，更增加了蒐證及調查的困難。爰國安局、法務部調查局及相關機關，在國安法第2條之2將國家安全範疇延伸至網路空間之際，允宜通盤檢視相關法令及既有作業模式，以因應日趨繁複之網路戰趨勢。

六、國安局建置「網安情(技)資分析平台建置案」之目的，係為該局遂行先知快報及支援政府決策之任務，以及建構國家完整資通安全防禦體系，該局允宜戮力完備相關功能並爭取充分經費，並適度釋出分析成果予資通安全法主管機關行政院資安處及其所屬參考運用，俾使該平台效益最大化，並落實資安鐵三角之緊密合作關係。

（一）國安局「網安情（技）資分析平台建置案」簡介，其任務與需求：國安局第七處於104年5月1日正式編成，即基於「研發能最大化」、「系統運作最佳化」及「維護管理最小化」之作業原則，陸續完成建構「網安探測之基礎工作環境」，藉以實體隔離方式，針對「網安威脅」等資訊樣本，完成探測及分析；另因應中共網路戰威脅及我整體網域安全防護需求，為使相關蒐集之情訊資料及研發工具完整運

用，分於108及110年度規畫籌建及擴充「網安情(技)資分析平臺」，藉整合各不同作業介面及資訊環境，採集中管控方式，管理「網安弱點探測」及「網安研發工具」，以達「快速反應」、「及時阻絕」之目標。

(二)現況檢討

1、國安局第七處司各項網域安全防禦事項，近年已建置完成「靖安工具開發平臺」與「網域安全攻防模擬訓練平臺」；惟因應資料量及網路傳輸速度之倍增，現有設備及設備效能，實已不足負荷。

2、依據年度任務推展之規劃，國安局第七處處冀針對整合「研發需求」、「人才培育」及「資安防禦」等各個面向，擬以現有「實驗網路系統」為基礎，結合既有之「網安工具開發平臺」及「網域安全攻防模擬訓練平臺」，規劃建置「網安情(技)資分析平臺」以有效提升網安訊息運用價值，提升主機運算效能及維持跨網設備維管之一致性。

(三)預期成效

1、提升資安工具研發能量：有效滿足各類網安技術研發作業平台整合需求，精進實質工作效率，逐步邁向「研發能最大化」、「系統運作最佳化」及「維護管理最小化」之目標。

2、完善訓練平台服務效能：藉由落實系統存取控制與儲存系統升級之擴充，提升「網域安全攻防模擬訓練平台」之安全性與執行效能，藉資料分析及分享為基礎，精進人才培育質與量。

3、建構資訊安全檢測環境：強化資安檢測防護能量，提升系統服務效率及高可用性，整合目標分析運用效益，提昇系統資安防護作為。

4、國安局說明，本案係因應中共網路戰威脅及我整

體網域安全防護需求，藉以提升國家安全整體網域安全為基礎，強化駭侵防禦、即時偵測、威脅分析及機先預警為目標，故須持續建置及擴充「資訊安全」暨「自動化」等全面性之系統整合，絕無「網域監控」情事。

(四)針對前開平台建置之必要性，國安局於赴本院簡報時亦補充，在網安防禦及分析工具方面，盡量不跟國防部在這部分交流太多，因為KnowHow或工具共通性太高，如果作業疏失讓工具曝光，會讓敵方有所防範。

(五)行政院資安處簡處長亦對該處及國安局前開平台於分析資安事件樣態及駭侵手法之可能入侵指標(Indicators of Compromise；IOC)提出補充表示，入侵指標不是普遍性的指標，是一種病毒碼的概念，不會只有一種，以中油為例，行政院資安處去蒐集病毒碼及中繼站，轉交給其他機構，他們可以立即檢查公司內的系統有無遭到汙染。

(六)次查，本院諮詢專家學者僅針對該平台提出下列建議：

1、此平台是否有「模擬」?「分析」威脅到什麼樣的程度？是否有涉及到「分發」？網路戰攻擊方式其中包括動能武器直接攻擊、電磁攻擊、運用惡意程式或代碼攻擊。不管是網路戰或資訊戰，均牽涉到偵察、掃描、取得存取、維護存取和覆蓋磁軌等，則國安局第七處的平台是不是都可以做得到?

2、國安局的這個建置案到底可以做到什麼程度？然而一定要跟當下行政體系資訊與網路安全之ISAC、CERT與SOC等等做結合；在情報上也應該要和資通電軍指揮部之情資蒐研做結合。

3、國安局這個平台我其實也沒看到，我是認為這會很類似一個情資整合平台。我是建議，八大情治機構都是向上送，但是是透過什麼方式呢？我自己都是看到紙本，未來這部分應該要資訊化，把資訊自動彙整上去，比如中繼站查處等等，在平台上進行分類，這樣可以把中繼站的拓樸做出來，而且技術上應該可行。

(七)綜上，國安局建置「網安情(技)資分析平台建置案」之目的，係為該局遂行先知快報及支援政府決策之任務，以及建構國家完整資通安全防禦體系，該局允宜戮力完備相關功能並爭取充分經費，並適度釋出分析成果予資通安全法主管機關行政院資安處及其所屬參考運用，俾使該平台效益最大化，並落實資安鐵三角之緊密合作關係。

調查研究委員：劉德勳

尹祚芊

包宗和

田秋堇