第五章台灣面對之科技挑戰

曾怡碩[1]

前言

軍民兩用科技對台灣造成的挑戰，主要來自敵意國家或其資助團體以新興科技優勢，壓制及打擊台灣。本報告第二篇提及之匿蹤戰機、超精準武器、極音速載具，均為中國積極發展之未來科技項目，但均非台灣力所能及。目前著眼之因應作為，是以加強戰力保存為未來主要防禦手段，這在下一章將有所著墨。台灣資源有限，必須發展足以形成不對稱戰力之科技，以因應現存最顯著的科技威脅。這類威脅目前主要來自中國解放軍於 2016 年將電戰部隊、太空軍、網軍、心理戰部隊組建之戰略支援部隊。其中，台灣在電戰方面，因長期與中國交手，並能與時俱進，故未讓中國佔到優勢。在太空戰方面，雖然台灣力有未逮，但基於通訊傳輸需求，仍有建構制太空權之必要，這對台灣形成重大挑戰。此外，中國仍在網路作戰以及網路輿論心理戰層面構成之威脅，對台灣資訊安全與關鍵資訊基礎設施保護以及反制網路輿論心理戰，形成重大挑戰。因此本章分別檢視台灣在這三大層面軍民兩用科技所面對的挑戰，並在小結呈現國軍秉持不對稱作戰思維之因應作為。

壹、建立制太空權

前蘇聯在 1957 年發射第一個進入軌道的人造衛星史波尼克（Sputnik 1），開啟了美蘇太空競賽。現代高科技戰爭或非戰爭軍事行動已與太空科技緊密結合。太空科技提供陸、海、空軍即時偵察、通信、氣象、導航、定位等作戰支援任務，不論是對敵軍之軍事及戰略目標實施精準打擊，還是藉由遙測影像進行災害防救，太空科技力量已成遂行軍事任務的要角。因此，除爭奪制空權、制海權、制陸權、制資訊權之外，制太空權已成為軍事行動致勝關鍵。

不論是採取攻勢還是守勢，一國要取得制太空權，必須發展與部署太空硬體設施、信號傳輸鏈結、指揮管制站暨使用單位三大部分的太空科技。太空科技的發展是一國整體科技與產業實力的體現，涵蓋系統工程、機械材料、推進控制、資訊系統、通信電子及遙測導航等科技範疇，發展成果往往具軍民兩用性質，對民生和國防等工業之推動，具有重大影響。然而，不論是在國防軍事用途或與民生相關的經濟應用的太空科技發展，皆須挹注大量人力與資金，由於所需經費與基礎工程過於龐大，有心發展太空科技的國家，也會在獨立自主發展路線之外，採取跨國策略合作方式，希望能取節省經費、截長補短之利，及早實現目標。

[1] 曾怡碩，國防安全研究院網路作戰與資訊安全研究所助理研究員，負責本章內容。

因應中國積極部署發展太空軍力，並於 2016 年將太空軍力納入其戰略支援部隊，台灣持續發展與建置因應措施，逐步形成制太空權戰力。然而，台灣雖積極發展與部署太空科技，仍囿於資源與技術限制，且於尋求國際技術合作時，常面臨國際政治現實面制約。因此短期內，台灣仍需與友好國家維持密切合作，以維繫初步的制太空權。

台灣的制太空權乃專注於防禦中國的太空軍力對於台灣的威脅，台灣目前面對中國太空戰力最大威脅，在於戰時通信與導航系統遭受破壞或干擾。中國北斗全球定位系統將提供「一帶一路」沿線國家服務，落實《推動共建一帶一路的願景與行動》有關「完善空中（衛星）資訊通道」指導，積極建構「天基絲路」，將有利於中國對台軍事監偵。下一部分將呈現台灣太空科技發展現況。

一、 太空硬體設施

太空硬體設施係指置於地球軌道上之火箭、人造衛星或其他可執行任務之裝置。台灣探空火箭計畫分別由國家太空中心統籌系統整合與任務規劃，中科院負責火箭推進系統，國內學術研究單位提出科學研究及酬載儀器研製計畫，於 1997 年至 2014 年間總共發射了 10 枚。台灣探空火箭計畫對於低緯度電離層研究量測、提供大氣觀測飛行路徑即時精密數據、衛星用反應式控制系統的功能測試、推進系統控制能力及回收艙系統能力測試，可用於未來發展衛星的通信、定位、推進、控制及回收艙。

台灣由國家太空中心發展人造衛星，自 1999 年開始，台灣從衛星接收國成為衛星發送國，成為全球第 33 個擁有衛星的國家。國家太空中心發展的福爾摩沙（福衛）人造衛星，已發送福衛一號、二號、三號、五號。其中福衛一號與二號已經除役，而福衛三號在 2018 年 11 月時，已服役超過 12 年，國家太空中心將以發送福衛七號取代三號，詳見圖 5-1。

通常探空火箭計畫是做為大型火箭發射衛星進入地球軌道的先行指標，福衛六號原規劃為第一個由台灣自行發射升空的人造衛星。2009 年國科會（科技部前身）界定台灣太空科技發展以科學研究為目標，決定取消原訂 2012 年自行發射衛星計畫，回歸原發展模式，委託國外火箭公司執行發射任務。

表 5-1、台灣人造衛星發展進程

福爾摩沙衛星	一號 原名:中華衛星一號	二號 原名:中華衛星二號	三號 6顆微衛星組成	五號	七號
總經費（NTD）	61.14 億元	46.02 億元	30.23 億元	56.59 億元	32億元（台灣出資）
升空時間	1999 年 1 月 27 日	2004 年 5 月 20 日	2006 年 4 月 15 日	2017 年 8 月 25 日	今年底或明年
除役時間	2004 年 6 月 17 日	2016 年 8 月 20 日	服役中	升空之後5年	升空之後5年
運載火箭	雅典娜一型	陶洛斯	美樂達	獵鷹9號	獵鷹重型運載
繞行地球一周時間	96 分鐘	103 分鐘	100 分鐘	99 分鐘	97分鐘
主要任務	科學實驗 1. 電離層特性研究 2. 海洋水色研究 3. Ka頻段通訊實驗	全球陸地及海域遙測 科學實驗研究及救災	觀測全球大氣層及電離層 建立全球大氣量測網	1. 自行研發台灣衛星關鍵技術 2. 全球陸地及海域遙測	1. 接續福衛3號 2. 密集提供中、低緯度電離層觀測資料

資料來源：中央社，2018 年 8 月 3 日。

二、 信號傳輸鏈結

國家太空中心專家在 2018 年 2 月出版的《科學發展》中指出，台灣位於近赤道的低緯度地區，上空受「赤道電漿噴泉效應」的影響，電離層活動較活躍且形成電離層的「赤道異常區」。這區域的電漿濃度特別高，其擾動現象對於全球定位系統（GPS）使用者，以及其他與衛星通訊相關的民生和國防應用，都可能產生很大的影響。

前述台灣探空火箭計畫與衛星計畫中，多次使用更精進的電漿量測儀器，配合地面設備持續研究台灣上空「電離層不規則體」的產生機制，並實現三方對照成果，具有精進通訊與定位上的功能。此外，2004 年除役的福衛一號，在 Ka 頻段通訊實驗方面，進行 Ka 頻段低速率、高速率及雨衰減通訊實驗，並且進一步做安全通訊實驗，以增強台灣的通訊系統能力。後來取消的福衛六號計畫，主要搭載的儀器將以遙測及導航定位為主，如果當初計畫實現，可算是台灣第一個自主開發的通訊定位衛星。至於地面的衛星操控中心及外部地面設施的資料傳輸，則仰賴地面通訊網路。位於新竹科學園區的衛星操控中心以台灣高品質的學術研究網路連接位於桃園中央大學及台南成功大學的 S 頻段遙傳追蹤指令站，而與海外發射場及海外支援站之間的資料傳輸通訊，則以 VPN (Visual Private Network)線路進行連結。

三、 衛星指揮管制站及資料接收站

國家太空中心負責衛星的操控，主要工作是以衛星操控中心、S 頻遙傳追蹤與指令地面站、X 頻遙測影像資料接收站及海外支援地面站等設施，進行指令傳送、狀態擷取、衛星追蹤、軌道控制、酬載資料及遙測影像接收等之全程任務操作，如圖 5-2 所示：

圖 5-1、國家太空中心衛星計畫衛星操控地面設施關聯圖

資料來源：國家太空中心。

衛星指揮管制站及資料接收站需有重複配置，冀能發揮緊急備援之效。國家太空中心分別於桃園中央大學及台南成功大學歸仁校區設立 S 頻段遙傳追蹤指令站，負責衛星指令發送及遙傳資料接收，而桃園中央大學站則同時兼具有任務操控中心的功能，作為衛星操作控制中心的緊急備援中心。X 頻遙測影像資料接收站建置於新竹科學園區，接收遙測影像資料後，傳送至新竹科學園區的遙測影像處理中心。此外，台南成功大學歸仁校區 S 頻段遙傳追蹤指令站於 2013 年升級為 S/X 雙頻衛星地面站，作為竹科園區 X 遙測影像資料接收站的備援站。

貳、台灣資安風險與關鍵資訊基礎設施保護

隨著物聯網、社群媒體等新興資訊技術服務快速擴展，軍、民資訊系統不論在虛擬網路世界，還是在實體硬體設備，遭受惡意入侵的威脅隨之俱增。台灣面對的資安威脅，是每月高達數千萬次網路攻擊。這些惡意攻擊背後，不乏國家政府資助的駭客團隊，以台灣為其實驗場域，對關鍵基礎設施、廠房企業、個人帳戶進行惡意入侵、竊取資料或擴散，造成國家安全威脅、商業利益損害與隱私人權侵害。

為因應資安威脅，我國政府於 2016 年 8 月即擬定「資安即國安」策略方針。蔡英文總統並在 2017 年的總統府資安週活動中，宣示了三項國安級的資安目標：第一、打造國家資安機制，確保數位國家安全；第二、建立國家資安體系，加速數位經濟發展；第三、推動國防資安自主研發，提升產業成長。有別於中國所強調的網路主權，並汲取中國及其他國家政府侵犯人民數位隱私權的爭議教訓，台灣採取資通安全治理途徑，以政府機關組織、私部門產業、非政府行為者、以及國際組織或建制為多方利害攸關者，共同因應資安威脅，以兼顧數位主權、人權與安全。

國軍保衛國家安全、守護數位國土有責，理應為多方利害攸關者資通安全治理中的重要角色。國防部遂於 2017 年成立資通電軍指揮部，依照 2018 年 5 月立法院通過的「資安管理法」與 2018 年 9 月國家安全會議發布的《國家資通安全戰略報告》，加入資通安全治理的行列。「資安管理法」與《國家資通安全戰略報告》均將國防部列為國家層級資安聯防團隊中的國安國防機制，實質上等於接受國安會指令，平時與各相關機關搭配建構伙伴關係，俾利於必要時協同執行任務，包括協同國土安全辦公室及國營事業，以抵禦消弭關鍵基礎設施面臨之資安威脅。

隨著關鍵基礎設施的資訊聯網已成趨勢，遭駭客入侵風險也遽增。著眼於此，「資安管理法」與《國家資通安全戰略報告》均將關鍵資訊基礎設施保護列為要項，接下來除了處理一般資安風險，將以專節闡述台灣關鍵資訊基礎設施保護措施。

一、 資安威脅現況

根據行政院資通安全會報技術服務中心於 2018 年 3 月指出，全球面臨的資

安威脅，主要類型不外乎：進階持續威脅（APT）攻擊竊取機密資料、分散式阻斷服務（DDoS）癱瘓網路運作、物聯網設備資安弱點威脅升高、網路與經濟罪犯影響電子商務與金融運作及資訊供應商持續遭駭影響供應鏈安全，關鍵資訊基礎設施資安風險倍增。

事實上，台灣不論是政府、企業所面臨的資安威脅，上述這些一樣都少不了。首先，根據行政院資安處於 2018 年 10 月表示，APT 與組織型駭客試圖竊取公務與商業機密威脅持續增高，且潛伏期拉長到五百多天，而分散式阻斷攻擊頻率與規模仍維持高量，並未減緩。其次，由於暗網惡意程式地下經濟猖獗，台灣金融業不只一次遭遇勒索惡意程式或駭客入侵自動提款機。

智慧城市物聯網的舖設建置，讓物聯網元件設備未改密碼而維持一樣的原始碼的便宜行事陋習，不僅讓智慧城市資安蒙上陰影，也成為關鍵資訊基礎設施網路串聯後的噩夢。最後，美國與歐洲多國關注中國資訊產品資安問題，也讓資訊廠商供應鏈的軟硬體資安問題成為眾所矚目焦點，台灣資訊廠商因此面臨供應鏈可能須考慮遷出中國的機會與挑戰。

台灣政府或企業也面臨類似的資安難題。個人攜帶行動裝置至辦公場合處理公務以及微型裝置察覺日益困難導致管理不易、技術更迭與惡意攻擊模式不斷翻新以致應變不易、社交工程防不勝防導致認知警覺不足、資安人才短缺以致資安自主能力不足及協力廠商或者分支機構管理不易造成資安漏洞。

台灣月達數千萬次的網路攻擊，光是國防部各單位每月就承受近兩千萬次網攻。根據 2018 年 7 月國防部公布資料（如表 5-1），在 2013 年，國防部各單位遭受網攻 868 萬次，2014 年大幅增為 7 億 2686 萬次，2016 年降為 3 億 932 萬次，2017 年國防部各單位遭受網攻次數卻進一步降為 2 億 466 萬次，但共軍對於國防部貫徹募兵制最重要的國軍人才招募中心遂行網攻也創下 3 千 196 萬次，是有史以來最高紀錄。

雖然資安攻擊事件往往難以追究確認發動來源，仍然可經資安鑑識與行為模式辨識，確認許多攻擊來源是來自中國。行政院資安處簡宏偉處長警告，中國網軍攻擊的頻率在降低，但成功率卻上升，特別是具有高度影響性的攻擊（第三級資安事件），從 2015 年僅成功 4 件，到 2017 年成功 12 件，成長 3 倍之多。[2]

[2] 資安事件影響等級分為四級：一.符合下列任一情形者，屬 4 級事件：(1)國家機密資料遭洩漏（機密性衝擊）。(2)國家重要資訊基礎建設系統或資料遭竄改（完整性衝擊）。(3)國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作（可用性衝擊）。二.符合下列任一情形者，屬 3 級事件：(1)密級或敏感公務資料遭洩漏（機密性衝擊）。(2)核心業務系統或資料遭嚴重竄改（完整性衝擊）。(3)核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作（可用性衝擊）。三.符合下列任一情形者，屬 2 級事件：(1)非屬密級或敏感之核心業務資料遭洩漏（機密性衝擊）。(2)核心業務系統或資料遭輕微竄改（完整性衝擊）。(3)核心業務運作遭影響或系統效率降低，於可容忍中斷時間內 回復正常運作（可用性衝擊）。四.符合下列任一情形者，屬 1 級事件：(1)非核心業務資料遭洩漏（機密性衝擊）。(2)非核心業務系統或資料遭竄改（完整性衝擊）。(3)非核心業務運作遭影響或短暫停頓（可用性衝擊）。

中國網軍採取新的技術來隱匿他們的行為，讓網路攻擊更難被察覺，例如透過搜尋引擎或部落格，讓資訊安全部門以為這只是一般網路平台，而忽略其行動。另外，也有許多的攻擊是繞道經由其他國家發動，使其難以被追蹤。專家表示，雖然台灣有良好的網路防禦與調查能力，但是要做到百分之百的防範是很困難。前揭顯示中國網軍在改變其網路攻擊型態，從原本大量進攻調整為精準打擊，一旦攻擊成功，後果將更形嚴重。

表 5-2、國防部所屬民網遭異常偵測、掃描及疑遭攻擊次數統計表

年度 / 單位	102 年	103 年	104 年	105 年	106 年
國防部網站（政務辦公室）	713, 778	1, 001, 142	1, 153, 275	4, 120, 552	9, 552, 884
國防大學	9, 405	877, 450	995, 312	219, 522	198, 469
人才招募中心網站（人次室）	804, 092	4, 309, 186	4, 931, 321	28, 522, 275	31, 968, 975
軍醫局（所屬國軍軍醫院）	4, 557, 186	720, 542, 371	561, 312, 118	276, 271, 708	162, 453, 979
政戰資訊服務網、青年日報社、軍聞社、全民國防暑戰營網站（政治作戰局）	2, 597, 760	133, 587	856, 889	194, 621	492, 549
總計	8, 682, 221	726, 863, 736	569, 248, 915	309, 328, 678	204, 666, 856

資料來源：《國軍資安防護機制書面報告》，國防部通資次長室對立法院第 9 屆第 5 會期外交及國防委員會第 14 次會議關係文書，2018 年 7 月。

二、 台灣關鍵資訊基礎設施保護

台灣將政府、高科技園區、能源、水資源、通訊、交通、銀行與金融、緊急救援與醫院列為八大關鍵基礎設施，而關鍵資訊基礎設施（Critical Information Infrastructure, CII）指的就是用來維運這些關鍵基礎設施所需的資訊網路系統，或調度控制系統（Supervisory Control and Data Acquisition, SCADA）。關鍵資訊基礎設施一旦遭受網路攻擊破壞，將威脅人民性命安全，亦即虛擬世界攻擊將造成實體世界傷亡，其嚴重程度等同於未達戰爭標準的暴力衝突。

為強化關鍵資訊基礎設施的資安防護(Critical Information InfrastructureProtection, CIIP)、風險評估機制及資安事件復原能力，特串接國家層級、關鍵資訊基礎設施領域層級以及關鍵資訊基礎設施提供者層級之三級電腦緊急應變團隊(Computer Emergency ResponseTeam, CERT)、資安資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)及資訊安全維運與預警中心(Security Operation Center, SOC)，建構完整的資安情報區動架構（如圖 5-3）。

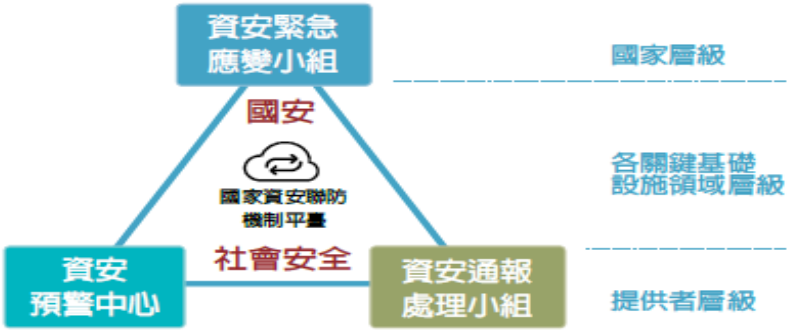

圖 5-2、以情報驅動之國家資安聯防架構

資料來源：國家安全會議，《國家資通安全戰略報告》。

關鍵基礎設施防護的權責分為國家、關鍵領域與設施提供者三層。國家層級由行政院資安處負責召集，主要實施跨領域演練、制定資安防護建議等工作。領域階層由八大領域的中央主管機關負責，例如金融領域是金管會，能源與水資源就歸屬經濟部。第三層則是關鍵設施提供者，金融設施就是銀行、證券機構，能源提供者就像台電、中油等單位（如圖 5-4）。

在關鍵設施提供者層級，必須注意工控系統（SCADA 屬於工控系統的一種）的資安。超過 80%的關鍵基礎設施是依賴工控系統來執行自動化作業，因此工控系統的安全可說關係到國家的戰略安全。早期設計時都是在封閉環境中使用，並未預想會以網路互聯，所以較少考量安全上的防護。根據 IBM 於 2018 年 10 月發布的《工控系統安全攻擊報告》，對工控系統的網路攻擊，可透過人工或在工控系統感染病毒，經控制主機植入未經授權的控制程式，再對工控系統網段通訊封包動手腳。因為工控系統的控制協議不具備加密機制，讓攻擊者乘機控制工控系統。2018 年 8 月台積電不慎讓病毒在科學園區廠房擴散，生產線被迫停機檢測數日，估計損失達新台幣數十億元之譜。此次事件直接的肇事原因，指向廠區安裝人員沒有按照 SOP 執行病毒檢測，就把新機台接上廠區內部網路，造成病毒擴散。

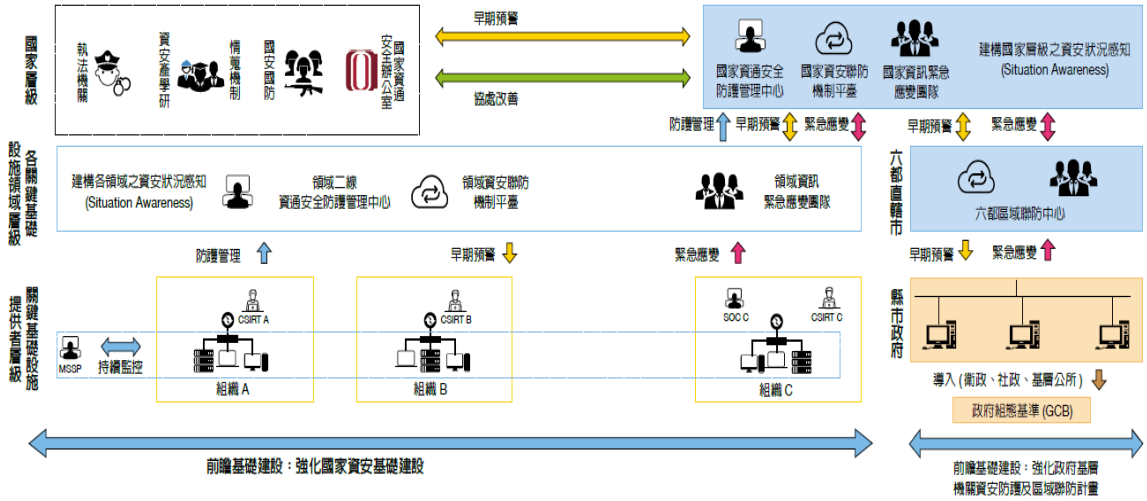

圖 5-3、建立國家級的資安聯防團隊

資料來源：國家安全會議，《國家資通安全戰略報告》。

參、反制網路輿論心理戰

中國一向擅長運用統一聯合戰線，亦即統戰，對台灣進行分化，並進一步對台灣實施三戰，其中即包含輿論戰與心理戰，亦即國軍所界定的政治作戰。中國如今將這些傳統政治作戰，轉化進入網路虛擬世界，形成所謂的影響力攻勢，但有別於傳統宣傳與當代軟實力，中國這類網路影響力攻勢因仍具備統戰的隱匿性、腐敗性及強迫性，因此被美國民主基金會在 2017 年歸類為與俄羅斯以網路干預美國 2016 年選舉一樣行徑的銳實力。

俄羅斯於 2016 年藉由社交工程釣魚郵件侵入美國民主黨系統，竊取機密資料後散佈於網路空間，並於社群軟體發布假消息以及發動謾罵，形成同溫層效應後，進一步分化美國原已對立的分裂社會，造成美國社會分歧，直接影響美國的國家安全。俄羅斯後來對歐洲國家選舉以及 2018 年美國期中選舉，一再重施故技，進行俄羅斯眼中所謂的資訊戰。

由於俄羅斯成功地讓美國淪為被干預內政的國家，中國有意效法俄羅斯，運用網路散布假消息、發動網軍帶風向，對台灣 2018 年地方選舉與 2020 年總統大選進行干預。更重要的，中國是希望能夠嫻熟運用現代網路媒體，先以台灣為實驗場域，進行網路空間的輿論戰與心理戰，日後再用以對付美國，冀能在美中新冷戰後，對美實行政治干預。

一、發展現況

大致上，傳統的輿論戰與心理戰都能套用到網路世界。謠言耳語即假消息、造勢即組成五毛黨網路洗版及收編/分化或分而治之即為網路同溫層效應的不斷延伸。除了假消息之外，利用社群媒體散佈仇恨言論，以達到動員暴力行為的目的，也讓網路虛擬言論造成實體世界性命傷害。社群媒體是現今資訊傳遞的重要

媒介，挾著這股新興網路傳播力量，針對如宗教、人種、性別、族群或性取向等特定群體，散佈具有煽動、貶抑或威嚇的仇恨言論，正蔓延全球國家社會，挑起社會對立衝突，衝擊社會和諧，成為政府亟需正視的安全議題。

網路空間要實施輿論戰與心理戰，就是利用網路假消息與仇恨言論，藉著社群媒體演算法的缺陷，散播貼文速度與方向取決於按讚或否定的數量，達成其動員、煽動目的。查核假消息所面臨的爭議，在於「誰能判定消息真偽」。若政府介入主導，可能因執行內容審查，淪於言論檢查爭議，徒生箝制言論自由的疑慮。目前作法，是採多方利害攸關者共同查核通報機制，由社群媒體業者、第三方查核人士以及政府共同面對與處理假消息。

西方民主國家面對仇恨言論引發的安全威脅，仍存有爭議。對於主張加以限制的國家而言，其著眼點在於避免仇恨言論所帶來的影響與傷害，即「第三人效果」傳播理論觀點，因預期傳播訊息對他人會產生高度影響效果，進而促使其採取預防及因應行動。例如德國於 2017 年通過《社交網路強制法》，規定社群媒體必須在接受使用者通報後的 24 小時內，撤除明顯違反德國刑法的仇恨言論，這項立法使德國成為打擊社群媒體仇恨言論最為積極與嚴厲的西方民主國家。

目前對待假消息與仇恨言論，多要求網路平台業者與媒體自律，對於一向捍衛言論自由的美國來說，限制社群媒體仇恨言論的作法，被視為嚴重侵害言論自由的思想控制，並給予社群媒體過分的權力進行內容審查。美國最高法院主張應保障憲法所言的言論自由為首要之務，國家不應過分介入社群媒體言論的價值判斷，否則恐因產生偏見與歧視。因此，美國採取相對寬容的立場，面對仇恨言論的管制。

台灣主要是由國家通訊傳播委員會因應網路假消息與仇恨言論問題。國家通訊傳播委員會與國安會資安辦以及行政院資通安全處，並列為資安鐵三角，對於網路通訊關鍵基礎設施的資訊安全維護，將強化早期預警、持續控管與維運、通報應變及協處改善等四大面向。國家通訊傳播委員會立場是認為，媒體報導應注意事實查證及公平原則，搭配事業建立之自律機制，如製播新聞違反事實查證原則，致損害公共利益或妨害公共秩序，現行廣播電視法或衛星廣播電視法早於 105 年即訂有違反者最高可核處新台幣 200 萬，並得令其停止播送該節目或採取必要之更正措施。事實上，行政院數位政委唐鳳與通訊傳播委員會都認為，事實查核必須以不侵害言論自由為原則，除網民應該要有意識地查證事實，網路平台必須有自律機制，兼得求證於第三方公正之媒體消息查證團體。

二、軍事發展應用

網路自律牽涉內容識別技術，目前除網路爬蟲兼大數據分析之外，也會以人工智慧偵測假消息與仇恨言論。對於社群媒體假消息的偵測技術，最早來自大數據分析。在 Express Scripts 擔任首席資料長（Chief Data Officer, CDO）的 Inderpal Bhandari 於 2013 年在波士頓舉辦的大數據創新高峰會演講中，提出資料真實性

（veracity）的概念，認為大數據分析中應該加入資料辨識真偽的考慮，分析並過濾資料有偏差、偽造、異常的部分，防止這些「髒資料」（dirty data）損害到資料系統的完整跟正確性，進而影響決策。

偵測假消息的技術規格，須能辨識文字與圖或影像，經前後文分析，分辨內容真偽，並透過大數據分析比對，追蹤來源真實性以及圖或影像是否經加工修飾。目前科技已進展到利用人工智慧偵測假消息，透過「自然語言處理」辨識文本內容及「視覺性質識別」辨識圖片與影像，經由「監督式深度學習」，運用「循環神經網絡」，對照前後句、前後段落與其他文本進行比較分析，藉以辨識其真實性。

假消息來源經多方利害攸關者交叉確認，就會由演算法列入通報名單，俾利辨識並阻斷假消息的散播。人工智慧不僅是辨識假消息的有力工具，同時也是製造與散播假消息的利器。人工智慧透過先前累積資料，可以鎖定大量特定社群媒體用戶，目前已被用於假消息的自動化散播。另一方面，若經由跨領域專門知識背景的演算法驅動，以及對於語言、文化以及各類知識的大量快速吸收與學習，加上反覆試誤、修正與練習，人工智慧未來也能成為製造挑撥分化性質假消息的來源。此外，人工智慧演算法的設定，必然存有人為決策思維的偏見（bias）。因此，以人工智慧處理假消息，依然要面對「誰能判定消息真偽」的根本議題。於此同時，在辨識假消息來源時，人工智慧「深度學習」可藉由辨識出演算法中偏見的特質與權重，可以分類及標示人工智慧製造之假消息。

處理仇恨言論就更加複雜，除經由監督式深度學習與運用「循環神經網絡」架構中「長短期記憶－支持向量機器」（LSTM-SVM）網絡模型，對照前後句、前後段落與其他文本，還要進一步進行情緒分析，將內容區分為「非侵犯性-侵犯性-仇恨性」，則可鑑別仇恨言論。由於仇恨言論定義模糊，導致現有人工智慧偵測系統對仇恨言論的操作型定義不一致。一旦檢視的內容超出訓練範疇或字句被刻意動手腳，如故意打錯字、添增不相關字眼或改變字距間隔，便可能輕易瞞騙過偵測體系。因此，目前技術若欲達成全自動化偵測仇恨言論，仍有相當差距。以目前 Facebook 與 Instagram 所採用的「Rosetta」技術為例，即使該系統足以同時處理超過 10 億件不同語言的附圖或影像文字內容，仍需人工進行篩選決策，Facebook 便聘僱兩萬人進行線上檢查。

偵測仇恨內容與偵測假新聞技術要求規格不盡相同，雖皆為辨識文字與圖或影像，前者經前後文分析，著重情緒辨識與侵犯性分級；後者則注重分辨內容真偽，透過大數據分析比對，追蹤來源真實性以及圖或影像是否經加工修飾。此外，一經辨識確認，處理仇恨言論與假新聞的方式也大相逕庭。仇恨言論多經網路平台予以刪除，而假新聞則按不同性質，可以有刪除、降階（demotion）、威懾，或運用充足的資訊對誤導性內容進行平衡、淡化、轉移（distraction）。因此，若有心人士或團體刻意編織假新聞以製造仇恨言論，即使沒有挑釁或侵犯性字眼，也能以肉搜曝光的個資或羅織的文字或圖像，蓄意煽動實體世界的暴力行為。由於此類網路仇恨言論可能不含挑釁或侵犯性字眼或圖像，僅呈現出羅織編造的

文字、圖或影像，因而將大幅增加人工智慧偵測仇恨言論的難度。

社群媒體業者須具備細緻豐富的語言與歷史、社會、文化知識背景，方能同時追查假新聞及審視仇恨言論。以羅興亞遭受種族清洗為例，由於緬甸軍方領袖利用 Facebook 散佈煽動暴力的仇恨言論與假消息，Facebook 坐視不理頻遭指責，雖然 Facebook 在 2018 年 7 月宣示要移除刻意煽動仇恨暴力的假新聞，但卻沒有具體動作，直到聯合國於 8 月發布報告，指責緬甸軍方對穆斯林少數民族羅興亞人犯下戰爭罪行，Facebook 才在 8 月 27 日移除 18 個臉書帳戶和 52 個臉書專頁，包括緬甸武裝部隊總司令敏昂萊（Min Aung Hlaing）和軍方 Myawady 電視台的專頁。

值得注意的是，中國加強對「一帶一路」戰略的同時，勢必對這些國家加緊輸出資通訊基礎建設，以利資料大量蒐集與傳回，遂行網路監控與情蒐，俾利為其實施政治干預做好準備。輸出的規格也可能視該國發展程度或對中國依賴程度而不一。對於低度開發國家或者極權國家，中國可能整廠輸出智慧城市，但必要時，得要先支援水、電、電信、交通運輸基礎建設，才能將監視器與感測設施內建並串接物聯網，達到全面監控情蒐的目標。對於諸如馬來西亞、白俄羅斯等開發中國家，中國則可能藉由爭取特定項目基礎建設，像是中國原先極力促成，後來遭馬來西亞政府取消的馬來西亞的「東海岸銜接鐵道」計畫，以及白俄羅斯的科學園區計畫，然後再將內建資通訊設備經由合法串接或者是非法手段駭進當地國資通訊關鍵基礎設施，以達成情資蒐集佈建的目標。中國未來勢必以「一帶一路」沿線國家作為精進網路輿論干預的試驗場域，藉此試行、實驗以人工智慧輔助的網路輿論量身製作(含假消息)、即時反應帶風向、網路水軍洗版等手法，除可壓制「一帶一路」沿線國家內對中國的不友善言論，也能進一步演練「混合式威脅」中的網路輿論干預他國內政手法，藉此精進其「銳實力」。

為因應中國於網路空間對台施行輿論戰與心理戰，蔡英文總統於 2018 年國慶致詞禮指出，必須阻止外來勢力對國內進行滲透破壞，確保民主制度及社會經濟正常運作。對於製造散布假消息以及企圖用各種方式介入選舉及干擾政治運作的行為，只要罪證確鑿，一定嚴辦到底。針對系統性、來自特定國家背景的假消息傳播，台灣也將加強跨國合作。未來要建立查核和通報機制，共同來因應這些假消息對各國的社會穩定，所帶來的破壞和衝擊。

中國正藉由台灣 2018 年選舉，作為其利用假消息施行政治干預的試驗場域，並可能於兩年後，將人工智慧「深度學習」的成果，套用在干預 2020 年美國總統大選，並進一步染指印太區域民主體制。因此，台美合作反制中國假消息，實為迫切的安全需求。然而，辨識與追查假新聞所需要的，是細緻豐富的語言與歷史、社會、文化知識背景。因此，台灣憑藉著語言與文化等知識上的優勢，以及對於人工智慧科技的積極研發應用，勢將成為印太區域反制中國假消息的國際陣營中，不可或缺的要角。

小結

台灣太空科技發展為科學研究用途，其中可應用於軍事、並形成制太空權的相關技術，除基本衛星部署與遙測影像之外，也對通訊傳輸環境進行研析，未來將藉福衛七號初步建置通訊定位系統。對於指揮管制部分，則包括衛星操控中心所建置的衛星操控系統，藉分析衛星下傳的 GPS 資料及地面站收集的天線追蹤數據，以掌握衛星的飛行動態，並進行衛星軌道轉換，已經成功地操控福衛一號、二號及三號衛星，初步具備不對稱反衛星能力。

除了太空科技發展，台灣的關鍵資訊基礎設施以及通信設施，同時面臨中國火箭軍以飛彈或電偵部隊以無人機、空軍以反輻射飛彈攻擊之威脅。此外，中國也可能以電戰部隊發動干擾。台灣除加強防空與反干擾戰力，面臨中國發展反衛星戰力之威脅，若要發展可直接打擊衛星的武器，則有資源上的限制。國軍未來可持續發展無人載具、增購機動化雷達系統、機動干擾器（中科院正積極研發「單兵導航衛星干擾系統」、「衛星導航干擾系統」、「合成孔徑雷達衛星反制系統」）、整合預警系統及強化反飛彈能力等作法，削弱中國在衛星的軍事運用，以創造制太空權不對稱能力。可持續發展無人載具、增購機動化雷達系統、機動干擾器、整合預警系統及強化反飛彈能力等作法，削弱中國在衛星的軍事運用，以創造制太空權不對稱能力。[3]

目前各國對於軍隊在資安治理中的角色，其實尚無明確界定。國安會於 2018 年藉由發布《國家資通安全戰略報告》，將國軍界定在資安人才培育與資安產業發展的促進角色，並與其他政府部門一同參與國家資安聯防體系，對於資安風險診斷、關鍵資訊基礎設施保護及國際情報分享等，國軍參與的角色及途徑仍待進一步釐清。

在平時獲得授權，被動受要求支援的情形之下，國軍可以秉持「超前部署，預置兵力」原則，參與平時資安聯防，發揮專業人力與設備能量，對於關鍵資訊基礎設施實施資安風險診斷，俾利實現關鍵資訊基礎設施保護之國土防衛，並可進一步實現與國際理念相近國家遂行國際資安聯防與情資交換，並進一步合作組成資安虛擬聯防體系。

最後，國軍面對具高度政治性的假消息與仇恨言論，必須謹慎處理。另一方面，防禦中國輿論戰與心理戰，乃國軍職責所在。因此，國軍必須拿捏投入此一政治作戰的分寸與界限，才不至於淪於政治不中立的批評。就此，建議國軍政治作戰專業應結合第三方公正事實查核團體或個人，並輔以人工智慧技術發展，遂行假消息與仇恨言論之查察，俾利反制中國對台之輿論戰與心理戰。

[3] 林柏州，＜從美國升級 GPS 看全球導航系統發展＞，《國防安全週報》第 18 期，國防安全研究院：2018 年 10 月 19 日，第 15-16 頁。