



2019

年3月11日，為因應中國「一國兩制臺灣方案」對我國國家安全挑戰，蔡總統召集國家安全會議，聽取各部會報告，並提出因應及反制「一國兩制臺灣方案」指導綱領。會中報告指出，「中國

長期以來，對

臺灣社會持續進行滲透及分

化，...兩岸各層面交流深入臺灣社會各個

階層，在一定程度上，模糊了滲透、統戰和兩岸交流的界限」。這段文字點出，在中共對台各種

策略作為，如滲透、分化、顛覆、破壞、竊密、統戰中，滲透是當中最模糊難辨、最難以因應的攻勢。

## 壹、中國對台滲透

據教育部國語

辭典，滲透是指思想或勢力逐漸侵入或影響。顯見滲透是一種動作或狀態，但其意圖或目標為何並不清楚。自兩岸開放交流以來，除了有限的 [ 半 ] 官方對話外，面對台灣的自由民主開放，北京當局一開始採取的是放話、

試射導彈等文攻武嚇等作為。2000年以後，

中

國在

台灣尋找

代理人與買辦，並

形成外界批評的兩岸政商權貴集團或

買辦集團，這條路線在

2014年太陽花學運爆發後已遭北京棄置。隨後，中共在先前「入島、入戶、入心」的基礎上，提出「三中一青」的統戰策略，擴大與台灣中小企業、中南部、中低收入及青年世代的交流往來。

2017年又提出「一代一線」策略，將統戰工作投入台灣「年輕一代、基層一線」。隨後習近平提出兩岸「融合發展」概念，強調從經濟、社會著手，推進兩岸合作與融合，之後從文化、思想推進，實現兩岸民眾的「心靈契合」。在這些政策指導下，中國開始制定單方面的「惠台」政策，力圖吸引台灣民眾前進中國；另一方面，中方人員、資金、訊息也在兩岸交流掩護下，加速進入

台灣，強化對台交往與滲透。

## 一、傳媒滲透

依法中資不得購買台灣媒體，但2008年中國開始加強對台灣媒體的滲透。最具代表性的是旺旺集團董事長蔡衍明，斥資204億台幣在2008年到2009年間，買下中國時報、工商時報、時報周刊、中天電視及中視等媒體。掌握報紙、無線電視、有線電視後，旺旺集團在2012年7月併購中嘉有線電視系統，取得台灣的傳播通路。隨之而來的是「置入性行銷」。2010年11月，監察委員吳豐山經調查後，確認中國政府以置入新聞的方式，購買台灣報紙包括《中時》與《聯合》的版面。除傳統媒體外，近年中國新媒體如愛奇藝、騰訊、優酷等影音串流平台，也透過代理商規避法規限制進入台灣，加劇北京對臺媒體的操控與影響。對此現象，台大新聞所張錦華教授警告，「當這種有效率的不實宣傳全面塑造中國大陸美好的形象時，台灣人民就會覺得中國政府、中國大陸都是好的...慢慢地我們的警覺性越來越低，甚至很多人對中國政府產生了幻想」。近兩年越來越偏頗的中天新聞，在2019年3月底遭國家通訊傳播委員會（NCC）罰款100萬，也有大學生發起「拒看中天」運動，相當程度反映此一問題的嚴重性。

## 二、網路輿論滲透

台灣是中國不實資訊、假新聞（以下以假訊息代稱）的主要操作對象。近年假訊息問題層出不窮，大量錯假資訊在台灣持續散布，對政府公權力、台灣民主法治及社會穩定，造成極大的負面影響。民眾記憶猶新的例子，包括2018年6月，網路謠傳高雄旗山香蕉滯銷，造謠者附上2007年香蕉堆積如山的舊照，企圖混淆視聽；2018年8月，蔡總統南下勘災，有人在臉書張貼假訊息，稱

陪同救災官兵槍枝均已上膛；2018年9月，颱風襲擊日本關西機場，造成上千名旅客受困，因兩岸辦事處輸運處理問題在網路引發爭議，並導致我駐大阪辦事處蘇啟誠處長自殺的「關西機場假新聞事件」。台灣面對的不只是假訊息，而是一種策略性的資訊操作（information manipulation）。換言之，有策略的輿論戰，可藉由一個事件切入，透過回溯、整理、類比等手法，以聳動具吸引力的敘述吸引民眾關注，把希望引發公眾注意的議題或負面訴求（例如政府施政無能、官員不知民間疾苦等），包裝為新聞或時事熱點。這種資訊操作，除文字傳播，也可透過第三方資金外包給公關公司，甚至網紅，以具時效性、話題性的方式，製作成影片或懶人包，在社群網絡與通訊軟體推播，擴大其影響力。

### 三、資安滲透

駭客攻擊中有許多病毒與「進階持續性威脅」（Advanced Persistent Threat）的手法，都可針對個人或特定組織的電腦，進行複雜且多方位的攻擊，潛伏攻擊的時間可能長達數週、數月甚至數年。植入後門程式的資訊產品，如媒體曾揭露的中國製路由器、鍵盤及智慧家電，也會將使用者的上網、打字資料、語音和影像等，回傳給預設的伺服器。同樣地，華為利用其產品的內建軟體或韌體後門裝置，在未告知客戶下，將客戶的基本個資、通訊錄、通訊過程、電子郵件等訊息，回傳到中國伺服器的行徑，不僅危害台灣國家安全，也嚴重影響美日等盟邦對台灣的戰略互信。2018年，我國政府終於宣布，禁止政府機關使用華為等有國安疑慮的中國廠商產品。2019年1月，美國微軟公司工程師發現華為的筆記型電腦裝有後門程式，並向華為通報，則是再添一個新案例。

### 四、產業滲透

產業方面，中國大陸透過併購公司、挖角關鍵人才、竊取營業機密等方式，取得我半導體、IC設計等產業關鍵技術的案例時有所聞。2016年，國安局長楊國強即曾在立法院答詢時透露，台灣的IC設計、電子科技產業遭中國嚴重滲透。距離新竹科學園區20分鐘車程的竹北台元科技園區，有多家中資企業進駐。其申請來台名義為「銷售中心」，卻違法設置研發中心，在台大舉招聘工程師。檢調單位對此雖有掌握，但卻無法落實執法。許多告上法庭的竊密案例，從2000年的中芯國際案，到近期的宏達電員工竊密攜往北京案、聯發科前員工投奔具中資背景港商，並對其洩漏手機晶片關鍵技術案，及2017年傳出聯發科、台積電、美光、南亞科、華亞科及聯詠等多起遭大陸企業挖角竊密案，2018年面板大廠群創科技遭侵害專利與營業秘密案等，都可看出中國對台灣產業的滲透、挖角、竊密情況之嚴重程度。

## 五、社會滲透

長期以來，中共以交流之名，對臺灣社會持續進行滲透分化。對於地方基層、農漁民、宗教、原住民、文化團體等，透過結對（如成為姊妹村里）、簽署合作備忘錄、招待赴陸旅遊，或提供虛銜（如邀台灣村里

長出任對岸村委執行主任）等方式，

拉攏結納地方人士；以

「體驗式」交流（邀請赴陸旅遊參訪）、

「青年創業基地」及提供就學、工作機會等方式，試圖改變台灣年輕世代、流浪博士與教師對中國的觀感；並以政治性採購、契作、觀光等經濟利益，拉攏臺灣地方政府與地方人士。此外，中國籍人士來台窺探、拍攝軍事或機敏設施，利用台灣現役軍人、台商刺探或竊取我方重要文件，甚至來台發展組織，例如鎮小江共諜案、周泓旭間諜案，相關事例不勝枚舉。這些作為不但危害

台灣民主體制，也對台灣的國家安全構成重大挑戰。據調查局統計，自民國97年起至105年底，偵破的共諜案達55案。國安單位亦曾估計，中共間諜在臺人數至少有5,000人，甚至有報導稱達10萬人者。

## 貳、因應作為的思辨

中國長期對台灣進行統戰滲透及分化，但台灣政府積極反制作為不多；各界對這些極具針對性、策略性的作為，往往缺乏警覺性

；亦有部分人士以人權、

言論自由考量，反對政府相對應的防制作為。

這些都與中共滲透作為本身的隱密性與不確定性有相當的關係。

### 一、反制輿論操弄的困難

由於社群網路傳播快速、自媒體普及，加上假帳號、假網站、留言機器人與「巨魔農場」（troll farm）帶來的大量訊息，使政府在處理假訊息

上，面臨訊息量龐大、處理時間有限，並須考量是否侵犯人權與言論自由等多重困難。針對假訊息的懲處，在確認其錯假違法後，爭議相對較小。真正重要而困難的，是要如何縮短其灰色階段（假訊息出現後到被判定為錯假違法之前），並阻斷該訊息的進一步傳播，以避免造成傷害。

我國既有法規對假訊

息雖有若干規範，如選舉期間可適用《選

罷法》，平時

有《

刑法》誹

謗罪與《社會秩序

維護法》（散佈謠言，足以影響公共

之安寧者」將受罰），

但這些規範面對自由、匿

名與快速傳播的假訊息威脅，顯已緩不濟急。

為打擊假訊息，行政院院會已通過《災害防救法》、《糧食管理法》、《農產品市場交易法》、

《傳染病防治法》、《食品安全衛生管理法》和《核子事故緊急應變法》、《廣播電視法》等十

餘部法規修訂，納入禁止散播假訊息的規範和罰則，並送立院審議。行政院及相關部會即時新聞

澄清機制及民間的「台灣事實查核中心」，致力加快澄清速度，提升內容查證品質，有助遏制假

訊息傳播。加強學校教育、印製宣傳手冊、舉辦說明會等，亦可強化學生與民眾的媒體識讀（me

dia literacy）能力，有助化解假訊息攻勢。

但對於灰色階段的處置，包括訊息錯假違法的認定及迅速阻斷假訊息的傳播，我國作為仍較為欠

缺。正在立院審議的《數位通訊傳播法》

是讓業者自律建立檢舉、處理機制，只要按機制做，對假訊息傳播，業者就可免責。對於未能落

實的業者似無罰則，而是由受害者要求違法使用者與平台業者負責，態度顯然較為消極（《廣播

電視法》修法版本提高廣電業者自律責任，並對散布假訊息提高罰則）。由法院認定假訊息，也

可能影響處理的時效。

相較之下，德國2017年6月底通過《社交網路強制法》，課予擁有200萬用戶以上社群網路業者快

速審查和刪除貼文的責任（須在收到通報後24小時內，撤除明顯違反德國刑法的仇恨言論；對假  
訊息或

較不明顯、有

爭議的仇恨言論，須在7天內

決定是否移除）、法國2018年11月通過《反資訊操縱法》及《反虛假訊息法》

，要求法官在48小時內針對是否為假訊息做出裁決，均有助截斷網路訊息快速傳播，避免傳統司  
法程序緩慢可能造成的損害。

針對相關法規侵害新聞自由，甚至引發自我審查或寒蟬效應的批評，德法兩國支持上述立法的人  
士主張，政府必須在新聞自由、人權保障與必要的民主防衛機制之間求取平衡。為避免扼殺言論  
自由，德國《社交網路強制法》提供個人和媒體周密的權利救濟管道，包括用戶資料遭濫用時、  
帳號遭不當停權或刪除時、合法內容遭不當移除時、個人或媒體遭不當處罰時，均有周妥及時的  
行政或司法救濟機制。

## 二、保防體系強化千頭萬緒

「保防」顧名思義就是「保衛國家安全、防制敵人滲透」。一般人注意到的保防體系問題，多為  
法令規範與刑度的不足。例如，《國家安全法》第2條規範「不得為外國或大陸地區行政、軍事  
、黨務或其他公務機構...刺探、蒐集、交付或傳遞關於公務上應秘密之文書、圖畫、消息或物品  
，或發展組織」，但其對應刑責最高只有5年。因此歷年最大規模的共諜案主嫌鎮小江只被判刑4  
年。對台灣社會的顛覆破壞或在台滲透發展組織，更缺乏相關規範。2019年3月定讞的陸生共諜  
周泓旭在台發展組織案，僅判刑1年2個月。而

外籍人士在台拍攝軍事設施等情節，通常僅能強制渠等刪除照片。

但更為嚴重的，應是台灣保防意識及預警能量的弱化。台灣解嚴與民主化後，「人二」系統瓦解，改由政風人員負責機關保防。但政風人員重視肅貪而非保防；2011年「政風司」改為「廉政署」後，保防工作的重要性與比重更進一步降低。軍中保防與社會保防，也因對中共敵我意識降低，而日漸鬆弛。近年破獲的保防案件多是已發展一段時間，對國家安全已造成傷害後，才被發現而進行偵辦。失去預警能量的保防系統，對國家安全而言，只能算是亡羊補牢。

事實上，美國、日本等民主國家，都十分重視保防，包括對資安滲透的因應。如何提高國人防意識、如何建立有效預警通報機制、如何因應中共資安威脅、如何從源頭（人員、資金、訊息）加強偵防能量、如何提升保防法規位階（目前僅係行政命令）、如何完備三大保防體系的法律授權等，都是台灣因應中共滲透的迫切工作。

澳洲《國家

安全立法修正案（間諜

活動及外國干預）法案》、《外國影響力透明

化法案》，及美國《外國代理人登記法》的相關規範，或可作為政府參考。

### 三、加強法規與機制配套提升產業安全

近年中國竊取我業者營業秘密案例頻傳，若不在法制上強化技術的保護，台灣可能淪為機密技術破口，影響先進國家政府與業者與我合作及投資意願。目前有關防制中共竊取產業機密的作為，以主張修訂《營業秘密法》者較多（司法體系審理案件速度過慢、侵害營業秘密行為的法人免責

的認定存在模糊空間），制定專法者較少。但對隱而未發的灰色地帶之應處，台灣目前僅有營業秘密法

針對「意圖在

國外、大陸地區、香港或澳

門使用營業秘密者」追究刑責。根據美國《經濟間諜法

》，只要個人或組織意圖竊取營業秘密，以裨益於外國政府或其實質控制的組織，就可適用該法追訴。我國在立法概念上明顯較為限縮，也難以保障技術免於被竊。另外，加強中資審查亦有助防制意圖不法的中資混進台灣資本市場。2018年美國通過外國投資委員會（CFIUS）更新法案，嚴審中資收購美企，以保護美國敏感高科技的作法，值得我國參考。

#### 四、強化民眾覺知（awareness）才能有效反制中共滲透

不論是假訊息、社會滲透或產業滲透，加強民眾對這些威脅的了解與認知，都是反制中共作為的最有效手段。針對假訊

息、共諜滲透、產業竊密的案例與影響，製作

宣導影片、編印宣傳手冊、辦理座談會、說明會或講習會，都有助

加強民眾、公務人員、軍人的媒體識讀（media

literacy）及保防意識，並提

升業者對中共滲透的警覺與因應能力。唯有

喚醒國人警覺，建立保防共識，才能團結國人，共同防制中共滲透，捍衛台灣民主自由體制與國家的長治久安。

作者 李哲全 國防安全研究院副研究員