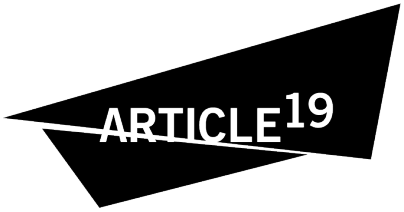
中國特色的資訊安全：

印太地區的數位治理及台灣的另類典範

ARTICLE 19



由ARTICLE 19在2025首次發布

www.article19.org

ARTICLE 19 是一國際非營利組職，致力於在地方及全球反思並實踐言論自由，讓所有人都能發揮其自身話語的力量。

與各個領域的合作夥伴攜手，我們不僅推動前沿技術相關研究，也對法律與政策上的發展進行分析，以求在世界各地推動變革。我們並透過遍及全球的九個區域中心，在言論自由的前線衝鋒陷陣。此外，我們也試著為各地的言論自由運動帶來創新能量，期望藉此帶來新的改變。我們目前透過以下五大主題來實踐我們的理想：促進媒體獨立性、提升資訊近用權、保護新聞工作者、拓展公民社會空間，並促使人權能置於數位空間發展的核心。

目錄

縮略詞對照表

ACS	資通安全署
AI	人工智慧
ASEAN	東南亞國家協會 (東協，譯註 : 引文提及處，保留中國「東協」稱呼)
BSSN	印尼國家網路與情報局
CAC	中國國家互聯網信息辦公室 (中央網信辦)
CCP	中國共產黨
CII	關鍵資訊基礎設施
CNCERT/CC	國家計算機網絡應急技術處理 (我國稱危機處理) 小組 / 協調中心
CPD	中央宣傳部 (中宣部)
CSMA	資通安全管理法
CSO	公民社會組織
DDoS	阻斷服務攻擊
DPP	民主進步黨
HITCON	台灣駭客年會
ICT	資通訊技術
MIIT	中國工業和信息化部 (工信部)
MODA	數位發展部
MoU	合作意向書 (合作備忘錄)
MPS	中國公安部
NTCERT	國家電信電腦緊急應變小組
PDP	個人資料保護法
PECA	電子犯罪預防法
PKCERT	巴基斯坦國家電腦緊急應變小組
PRC	中華人民共和國
PTA	巴基斯坦電信管理局
SIIO	中巴共同人工智慧研究中心
SPCAI	國家網路資訊辦公室
TAHR	台灣人權促進會
VCP	越南共產黨
VPN	虛擬私人網路
WMS	網頁管理系統

研究摘要

在本報告中，ARTICLE 19檢視了中華人民共和國 (中國，PRC) 在印太地區，如何透過與印尼、巴基斯坦及越南三國展開的「數位絲路 (Digital Silk Road)」計畫合作，影響這幾個國家的資訊安全準則 (cybersecurity norms) 發展。研究發現，中國積極地在各項數位發展計畫，帶入其資安治理準則，而這不僅對國際人權、網路自由以及民主制度構成嚴峻挑戰，也凸顯出印太地區現下迫切需要不同於中國式資安的另類治理典範。ARTICLE 19特別在報告中記錄下台灣的經驗，作為在中國的專制模式外，一個更以人權為本的替代方案。

本報告一開始會先建立對中國數位治理的基本理解，並著重說明其中與資安準則相關的部分。有鑑於中國不斷地在試著在數位治理領域中，將自己定位為全球準則的制定者，先拿下印太地區，對中國來說有其戰略上的重要意義。也因此，瞭解中國式的治理準則如何在印太地區擴散，可以幫助我們進一步瞭解其更大的全球野心——在根本邏輯上翻轉全球數位基礎設施樣態，甚至重寫現行數位治理規則。

本報告緊接著對印太地區的三個國家進行個案分析。此三則個案說明了中國的專制模式，如何透過資訊安全法規、政策及機構這三個面向來向外散佈，也點出中國在這三個面向的作法，都限制了言論自由及隱私權。這些法條往往涉及關鍵資訊基礎設施的管理、資料在地化 (data localisation) 以及對身份驗證要求，亦有關於透過所謂「中國式防火牆」來進行的數位監控、隱僻措施及綿密的政府管制措施。

研究指出，雙邊合作協議經常讓純粹的數位發展合作與數位治理準則的採納混為一談，而這正是中國慣常使用的影響機制。透過這些協議，研究對象國家與中國科技公司的公私協力夥伴關係 (PPP) 先深化雙邊合作，而這些以培力 (capacity-building, 譯註：中國譯為「能力建設」，下文中出現培力及能力建構，英文原文均為 capacity-building) 為名、看似無關政治的交流，卻旨在將中國的數位專制治理模式推舉為最佳實踐。

研究也透過研析這些影響機制，呈現中國式資安治理準則在印太地區散佈的現況。各國政府在影響下會以國家安全或是數位經濟發展的名號，訂下嚴峻的資安及資料在地化法規。偏重網路主權的中國式作法，現已成為形塑印尼、巴基斯坦和越南國內的數位治理框架的重要一環。

中國的影響力亦體現在這些國家選擇採納由中央主導的監控與審查機制之中。例如，印尼開始擁護網路主權理念，並在技術交流與合作協議上追隨中國於印太地區的領導。而巴基斯坦則發展中國式防火牆，並整合華為等中國企業的監控技術，兩者均是相當有代表性的實例。越南則是在其資訊安全法中納入了實名註冊與嚴格的內容審查措施。研究也發現，那些通常由中國公司主導的技術培力計畫，不僅加深當地對中國的依賴，亦進一步鞏固中國在區域推動中國特色的資安準則與實踐模式。

這份報告另一個重要的目的是分享台灣的經驗，藉此提出一個在資安治理上值得寄與厚望的另類典範。與中國帶限制色彩的多邊主義 (restrictive multilateralism) 大相徑庭，台灣著重多元利

害關係者參與 (multi-stakeholderism) ，並藉此展現了一種更加透明且讓民間社會得以參與的數位治理取徑。台灣徹底將關鍵資訊基礎設施治理與內容管制分離的做法，可說與中國以維穩為重的策略形成強烈對比。

我們同意台灣模式並非毫無缺點，但加強世界各地與台灣的接觸，將大大地有助於發展以人權為本的數位治理另類典範。我們不僅將這份報告當作一份單純的學術研究，同時也作為對全球政策制定者、技術專家以及人權倡導者敲響的一聲警鐘。

這份報告揭露了中國數位模式的負面特質，以及這個數位模式在印太地區擴散的現況。透過這份報告，我們希望能提出一套有效回應現實困局的路徑圖，讓人們得以辨認、理解並最終能對抗中國制定數位準則的野心，及其對人權造成的深遠影響。

如何削弱中國在網路準則上的主導權

國際社會在各捐助者協助下，必須積極提倡台灣參與全球資安及數位治理對話，藉此強化對抗數位專制主義的國際聯盟。各國政府應確保公民、民間社會與產業利害關係人參與政策制定，要求立法草案須進行公開諮詢，並透過包容性機制放大民主聲音，使台灣利害關係人得以在國際論壇中有實質發聲與參與機會。同時，國際捐助者務必協助區域公民社會網絡的動員，共同蒐集與數位工具與政策相關的證據，與在地民間社群緊密合作，並防範來自威權國家的報復行動，從而以台灣為核心，凝聚能量對抗日益升高的數位專制主義。

台灣政府應持續推行施政透明、資料保護及公共問責措施，並透過立法明確保障隱私、言論自由及資訊近用權，將其作為資安準則制定的核心基石。而在此基礎上，台灣也應進一步運用自身民主資本，積極向國際推廣從人權為本的數位治理，同時透過向外進行培力相關的數位外交，協助印太地區國家建立符合民主價值的資安政策。

台灣公民社會可與區域夥伴協力，記錄並揭露中國「數位絲路」計畫對人權帶來的負面影響，充分發揮其對中國慣用威脅及影響力伎倆的專業知識，協助辨識出各種可疑的技術、政策及手法。另一方面，台灣企業界甚至更廣泛的公民科技社群，也應善加利用參與國際論壇的各種機會，來分享這些應對中國的專業知識，特別是關於網路治理及技術標準制定的場合。

研究背景

在這個數位轉型空前加速的時代，中華人民共和國 (中國) 的技術野心已透過一帶一路倡議及其數位分支數位絲綢之路 (數位絲路，Digital Silk Road) 蔓延全球。中國的數位影響力正迅速重塑印太地區，甚至全球的地緣政治格局及數位準則思維，本報告發布的背景正是這樣一個危急存亡的時刻。

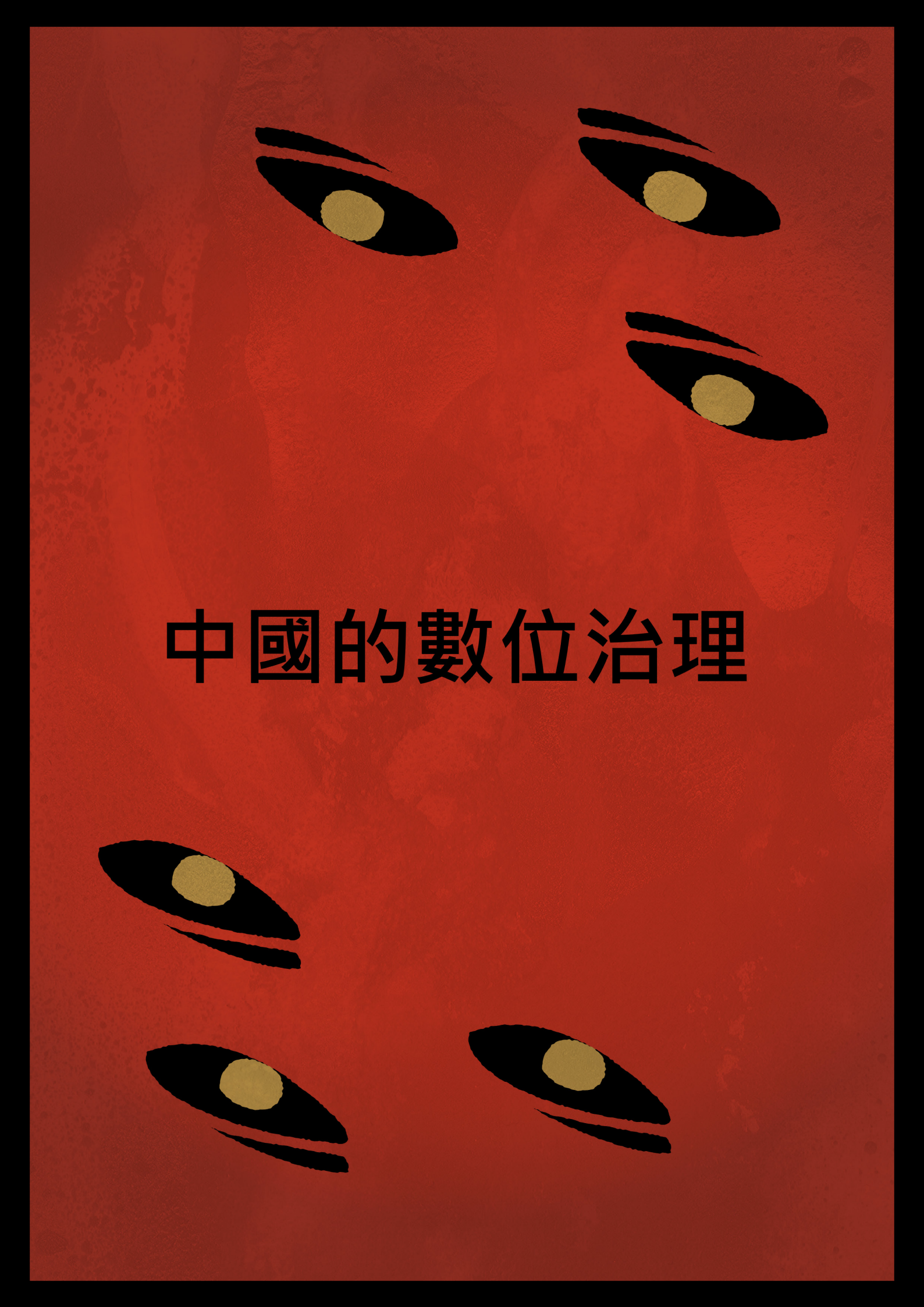
面對日益加劇的科技競爭以及中國有系統地輸出數位基礎建設，可說同時帶來了諸多深遠影響。越來越多開發中國家採納中國的技術生態系統，引致數位準則全球規模的大幅轉型。數位絲路不僅是協助各國發展基礎建設，更是中國用以輸出自身技術與治理模式的戰略工具。無論是這些技術或是治理模式，事實上都對現行國際人權及數位框架帶來挑戰。

中國所推行的數位治理模式，側重共產黨的集權控制、網路主權以及多邊倡議，正是這樣的模式對國際人權保障、網路自由及民主制度構成重大挑戰。如果就這樣將全面性的政府管制、侵入性的數位監控及嚴格的資料在地化措施正常化，恐將從根本上重塑全球數位生態。

在這個背景下，台灣會是對抗中國數位治理模式的重要制衡力量。雖然在國際政治上，中國持續孤立台灣，試圖壓制其參與全球事務的機會。但本研究指出，儘管台灣的資安治理模式雖非完美，但相較於中國並放眼全球，台灣所提供的替代方案更尊重人權，可以作為典範有效對抗中國輸出自身數位治理準則的威脅，這在印太地區更是別具意義。台灣以人權為重的資安治理取徑，強調多元利害關係者參與、施政透明及公民參與的可能性。台灣證明了即使面臨嚴峻的網路威脅，民主治理依然存在潛力與韌性。

本報告的主要目標是提供全面且有證據支持的分析，協助政策制定者、民間社會組織及國際利害關係者得以深入理解、預測並有效對抗中國的數位治理模式。透過揭露中國數位準則擴散的運作機制、分析數位基礎建設輸出的戰略布局，並提出替代性的治理取徑，我們期望促成有戰略意義的應對措施，期望這些措施能維護數位人權、弘揚民主價值，並避免專制的科技行為模式不受控地擴散。

我們的研究旨在將這樣的理解，進一步轉化為能付諸行動的洞見，幫助印太地區以至於全球建立具備韌性且尊重基本權利的數位生態體系。隨著中國持續拓展其數位影響力，我們亟須對持續變化的現今局勢，展開嚴謹的審視甚至果斷的行動。政策制定者、民間社會與國際利害關係者都必須認識、理解並有意地抵制威權科技模式對數位空間帶來的轉變。全球數位治理的未來可說正處於關鍵的十字路口，其發展將對全球人權保障及民主價值帶來深遠影響。


中國的數位治理

中國的數位治理

中國的資安及數位治理準則

- 由中共集權控制、重視數位主權及發展上的維穩
- 多邊主義 vs. 多元利害關係者參與
- 諸如2017年《網路安全法》及2021年《數據安全法》等重要法案，都透過資料在地化、審查機制及社會監控，來加強黨對數位空間的控制。

數位絲路上的整合

- 計畫在2015年於一帶一路倡議下啟動，旨在發展數位基礎建設並擴大資通訊技術 (ICT) 合作。
- 強化中國作為數位治理領域領導者的形象，並影響全球的數位準則。
- 透過如「中國 - 東盟戰略夥伴關係2030年願景」及不同的資安培訓計畫，與東南亞國家聯盟 (ASEAN) 進行合作。

推廣技術標準、資安外交及戰略目的

- 截至2019年，中國已與49國簽署85項技術標準協議，令其在數位治理領域有所斬獲。
- 透過中國國家計算機網絡應急技術處理小組 / 協調中心(CNCERT/CC)，與81個國家建立合作關係，並與東協國家簽訂合作意向書 (MoU)。
- 將資安與國家安全及發展掛鉤，讓帶威權主義色彩的數位治理模式帶入合作國家。

中國是透過以下幾項重要的法律、機構及行為準則，來打造其資安治理手法。

中國法律與實行法規

- 2017年的《中華人民共和國網絡安全法》(參閱附錄一) 是構成中國網路主權模式 (cyber sovereignty model) 的基礎，強制要求資料在地化、實名認證及各項網路管制措施。該法對關鍵資訊基礎設施 (Critical Information Infrastructure, CII) 營運商施加嚴格義務，並鼓勵非CII業者也遵循相似規範，有效地將所有的線上服務供應商納入國家控制範圍。後續發布的相關法規，也進一步地強化了這些規定。
- 同於2017年的《中華人民共和國國家情報法》及修訂後的《中華人民共和國反間諜法》規定，所有個人與組織 (包括境外科技公司) 必須協助國家情報工作，讓政府擁有更大範圍的情報收集、招募與監控權力，此舉恐有對隱私權和國家權力過度擴張的疑慮。
- 2021年的《關鍵信息基礎設施安全保護條例》進一步將CII的定義擴大，納入「公共電信及資訊服務」
- 2021年的《中華人民共和國數據安全法》將中國對相關事務的司法管轄權延伸至境外，規定外國實體若從事被認定損害中國利益的資料處理實務，將依法追究其法律責任。
- 2021年的《中華人民共和國個人信息保護法》則賦予國家對個人資料的廣泛公權力，允許政府以定義模糊的不同安全理由，逕行使用身份識別技術。

上述所有法律都為我們帶來了有關隱私權、言論自由及國際資料治理衝突的嚴重隱憂。

中國的資安治理機構

習近平主張「黨政軍民學，東西南北中，黨是領導一切的」，此言充分體現了中國數位治理機構所遵循的層級式架構。**中國共產黨中央委員會**是中國最高決策單位，由政治局常務委員會領導，習近平則執掌大權。中央委員會一般負責設定政治意識形態調性，並領導國家政策和重點工作方向。而**國務院**作為中國國家最高行政機關，實際上從屬於中國共產黨，並忠實執行中央委員會所制定的政策方針，其中就包括資安相關事務。在中國的黨政合一的系統下，很多機構都可能同時具有對外的國家機關名稱與黨內功能定位的雙重身份，即所謂「一個機構兩塊牌子」。認清此一體制區分極為重要，因為在簽署合作協議時，不熟悉這種雙重設定的國家或組織，可能誤以為自己是在與中國政府合作，實際上則是與中國共產黨合作。

中國負責資安、內容審查及大範圍網路治理政策的核心機構是國家互聯網信息辦公室 (中央網信辦，Cyberspace Administration of China, CAC)。自2018年起，該辦公室已經成為直屬中央委員會的「超部級」監管機構。該辦公室執掌防火長城進行的網路審查，並負責新興技術 (如人工智慧) 相關的政策制定。此外，中央網信辦也管理國家計算機網絡與信息安全管理中心，該中心負責中國國家計算機網絡應急技術處理小組 / 協調中心 (National Computer Network Emergency Response Technical Team/Coordination Centre of China, CNCERT/CC)，此部分將在後文詳細介紹。

中央網信辦執掌權力的持續擴大，反映出習近平時代裡數位治理在中國的重要性與日俱增，這也有助於理解中國在海外開展的數位合作。國務院新聞辦公室，同時作為中共中央宣傳部對外宣傳辦公室 (中宣部，Central Propaganda Department, CPD)，是在2011年成立中央網信辦的前身SIIO並在2014年改為現名。(譯註：2011年中共以State Internet Information Office作為英文機構名設立中央網信辦，並在2014年改為 Cyberspace Administration of China，中文機構名維持原稱) 。

中央網信辦與中宣部關係密切，這種聯繫構成了中央網信辦運作的核心。兩機構間的關係常被混

淆，但這也體現了中國數位準則下，網路治理與資訊管控間密不可分的雙重關係。值得一提的是，高層領導者往往兼任網信辦及中宣部的職務，例如以2024年12月來說，莊榮文 (庄荣文) 便同時擔任中央網信辦主任及中宣部副部長。

2014年，中國在黨內將網信辦升格為更具權威的中央網絡安全和信息化領導小組，並由習近平親自擔任組長，此舉進一步提升了中央網信辦的地位與權力。

同年，中央網信辦在烏鎮舉辦了首屆世界互聯網大會 (World Internet Conference)。該會議影響力逐年上升，並成為中國藉以介入全球數位準則的重要平台。2022年，世界互聯網大會國際組織 (World Internet Conference International organisation) 的成立，更是進一步提升了該平台的國際影響力。習近平對其表示讚揚，稱其在「為全球互聯網發展治理貢獻智慧和力量」扮演重要的角色。

2018年3月，中國在進行大規模的黨和國家機構改革期間，將中央網絡安全和信息化領導小組升格為中共中央網絡安全和信息化委員會 (Central Cyberspace Affairs Commission, CAAC)。此項升格進一步將中央網信辦拔擢為中共中央直屬機構。

中國國務院下屬執掌數位治理的幾個關鍵部門包括 :

- **國家發展和改革委員會** : 此部門是國務院中權力最大的部會，負責國家發展規劃及制定「五年計劃」。該委員會推動技術創新並扶植戰略性產業，在制定數位政策框架中有其戰略定位。該機構還管理國家數據局，此單位負責與中央網信辦協調智慧城市及數位治理上的經濟面用途。國家數據局同時還是「數字中國」政策的一部分，該政策旨在使中國在2035年以前取得全球數位發展的領導地位，並同時加強中國的資安能力。
- **工業和信息化部 (工信部，Ministry of Industry and Information Technology, MIIT)** : 此部門負責監管電信、軟體及IT製造產業，同時也為中央網信辦提供基礎設施與技術創新支持。該部門還經常代表中國參加國際組織，如國際電信聯盟 (International Telecommunications Union, ITU)，對全球資安準則擁有一定程度影響力。
- **公安部 (Ministry of Public Security, MPS) :** 作為中國最高警政機關，曾負責執行「金盾工程 (Golden Shield Project)」雖然目前這方面的監管單位已擴大到包括中央網信辦及工信部，公安部仍然參與管理公共網路安全，並執行「網路安全等級防護 (Multi-Layer Protection Scheme, MLPS)」標準的落實。公安部也同時負責管理資安相關事務，諸如VPN使用的監管，並與CNCERT/CC密切合作。公安部並與國家安全部協作，執行涉及境外情報活動與跨國打壓行動等監控業務。

數位治理準則

網路主權

中國數位治理準則的根基，無疑是網路主權之概念。這個概念最初在2010年發布的《中國互聯網狀況》 白皮書中被提出。其主張，網路治理屬於國家主權範疇，並允許各國根據其所認定的國家，來對網路施加管理政策。這是一項中國積極透過多個國際論壇和倡議推廣的概念 :

- 2012年，在布達佩斯網路空間會議 (Budapest Conference on Cyberspace) 上，中國就提出了國際網路合作的五項原則，網路主權是其中的核心重點。
- 2016年，中央網信辦在《網絡安全法》通過前夕發佈了《國家網絡空間安全戰略》目標，其中再度重申了「網路主權」的立場，並聲稱尊重網路主權已是國際共識，訴求全球接受中國所設定的網路治理準則。
- 2018年，中央網信辦及各國不同機構，合作啟動了「一帶一路數字經濟國際合作倡議 (the

Belt and Road Initiative Digital Economy International Cooperation Initiative)」，該倡議鼓勵基於網路主權與多邊式的網路治理展開合作。.

- 2022年，國務院發布的白皮書《攜手構建網絡空間命運共同體》進一步重申網路主權是「國家主權在網絡空間的自然延伸」，將其作為中國主導全球數位準則制定的重要項目。
- 然而，網路主權概念與普世人權原則存在根本上的牴觸。人權應當具有普遍性、不可分割性及相互依存性，且不應受國界限制。是此，中國所倡導的網路主權概念，便引發了對言論自由、資訊近用與隱私權等基本權利的隱憂。儘管中國外交部於2023年發布了《中國關於全球數字治理有關問題的立場》，其中表達了反對網際網路碎片化 (internet fragmentation) 的立場，但「網路主權」準則卻實際上鼓勵各國在數位監管上各行其政，從而加劇全球網路碎片化的風險。

多邊主義與對多元利害關係模式的否定

自2010年《中國互聯網狀況》白皮書發布以來，中國始終高舉多邊主義，這樣的立場可說與中國共產黨對集權控制的高度重視一致。

中國有系統地透過聯合國及其他由國家主導的論壇來鼓吹多邊式合作，並持續強調網路主權概念，主張各國有權自主決定自身網路發展方向及管理方式。中國外交部在2021年發表的《中國關於網絡空間國際規則的立場》文件中即表明此立場，並呼籲各國共同「制定包括數據安全在內的新國際規則」。透過將重點放在網路空間治理中的安全及發展，中國試圖構建一個從根本上挑戰現行國際網路治理準則的框架。這一立場與傳統的「多元利害關係模式」形成鮮明對比。多方利害關係人模式通常涵蓋民間社會、產業界和學術界的廣泛參與。

中國所推動的此類治理模式，不僅偏重國家行動者 (state actors) 更抑制了廣泛公民社會的參與，這也造成在全球人權與網路自由上的嚴重隱憂。儘管如此，網路主權論述正在逐步取得影響力，特別是全球南方國家 (Global South) 。這些國家普遍尋求對抗美國科技霸權的替代方案。

這種模式所帶來的影響深遠：中國所提出的並不僅僅是一種技術面的網路治理模式；而是在積極構建一個強調國家控制、壓制個人權利、缺乏透明度並削弱跨國合作的全新全球數位生態體系。

維穩為重的數位環境

中國將資安與資訊化革新視為國家安全和發展不可分割的一部分。2017年發布的《網絡空間國際合作戰略》明確強調，網路安全對國家主權、安全及發展至關重要。中國積極通過幾個重要論壇推動多邊式國際資安合作，包括東協區域論壇、上海合作組織、中非合作論壇等，並持續協助發展中國家進行相關培力計畫。這種準則取徑會造成的一個人權隱憂，是將數位發展等同於線上資訊空間的維穩式管理 (securitisation)，如習近平曾特別強調的「以安全保發展、以發展促安全」。這樣的做法可能的危害在於，它可能透過與數位絲路發展夥伴國家的合作，讓中國的數位治理模式複製到這些國家，進而影響其法律、政策、機構體制以及基礎設施，從而侵害人們的言論自由及隱私權。這些疑慮會在後續區域個案研究中闡明。

資訊安全與數位絲路

數位絲路概念第一次真正被提出，是在工信部2014年11月發布的《周邊國家互聯互通基礎設施建設規劃》文件中。

2015年3月，國家發展和改革委員會隨後發布了白皮書《推動共建絲綢之路經濟帶和21世紀海上絲綢之路的願景與行動》。該白皮書呼籲加快建設跨境骨幹網路，並擴大資通訊技術 (ICT) 上的

國際合作。同時，文件還強調中國在「中國標準2035」政策下的全球技術標準制定野心，致力於在全球技術標準制定領域中取得主導地位。自2015年起，中國就積極將推廣本國技術標準作為雙邊協議的重要組成部分，並將此戰略運用於與印尼和越南等國的合作中，以推動中國標準的國際採用。

中國在2016年12月發布了《國務院關於印發「十三五」國家信息化規劃的通知》，明確提出改革全球網路治理體系的目標，並呼籲加快跟東協合作的腳步 。該目標在2016年11月舉行的東協 - 中國高峰會上進一步深化，峰會最後提出《中國 - 東盟戰略夥伴關係2030年願景》宣示。這也是2020年召開首屆「中國—東盟網絡事務對話」的基礎，開啟雙邊的資安合作。

2019年，中國在第二屆「一帶一路」國際合作高峰論壇上，最終與49個國家 (包括印尼和巴基斯坦) 簽署了共計85項技術標準協議。2023年10月，中國在第三屆高峰論壇上，再次重申其在包括資安治理的全球數位治理規則制定中領頭的野心。這個野心明確地和數位絲路的目標一起持續發展。這樣的野心和目標，也在2021年3月發布的《「十四五」國民經濟和社會發展規劃及2035年遠景目標綱要》中被強調。這份綱要特別強調中國強化其在網路空間中參與的決心，並特別著重資安準則制定。

2022年11月，國務院新聞辦公室在《攜手構建網絡空間命運共同體》白皮書中，進一步闡明了「十四五」計畫中的幾個主題。白皮書中特別著重區域性資安合作倡議，並指出截至當時，中國已透過 CNCERT/CC 將合作夥伴拓展至81個國家，並與包含印尼和泰國在內的33國家簽署了合作意向書。白皮書同時也讚揚與東協從2017年開始的合作關係，這項合作關係起源自「中國—東盟網絡安全應急響應能力建設研討會」，包含柬埔寨、印尼、寮國、緬甸、菲律賓、泰國與越南都是與會國家。在這個基礎上，白皮書也進一步呼籲創設「中國—東盟網絡安全交流培訓中心」，這也是中國意欲藉由數位外交形塑資安準則的實例。

印太地區的個案研究

重要研究發現

個案一：印尼

- **數位依賴性 (Digital dependency)：印尼對中國數位技術的依賴日益加深，這暴露出資安治理中的制度缺口，例如法律框架不夠完整，以及資安相關機構如印尼通訊和資訊部 (Kominfo) 和國家網路與情報局 (BSSN) 等機構的資源欠缺。**
- **MoU和政策轉向：**例如2017年中國CNCERT/CC與印尼的國家網路與情報局所簽署的意向書，就在培力計畫及看似只對印尼有利的雙邊合作的名義下，強化了中國對印尼資安政策的影響力，並讓中國的各項資安慣例在印尼被正常化。
- **監控基礎設施的擴增：**與華為的合作，加上參與中國—東協資安研討會議，都讓中國模式在印尼大行其道，讓實名登記系統以及各項更嚴苛的內容審查政策落地，這都引發了隱私權和言論自由相關的隱憂。

個案二：巴基斯坦

- **將中國視為數位發展的戰略槓桿：**巴基斯坦的數位發展深受「中巴經濟走廊」影響，成為中國數位影響力的試驗場域。與華為和中興通訊等中國企業的合作關係，亦進一步加深了巴基斯坦對中國技術與基礎設施的依賴。
- **威權專制法律架構：**巴基斯坦的《電子犯罪預防法 (Prevention of Electronic Crimes Act, PECA》便大量借鑑中國2017年的《網絡安全法》，引入了網路審查、強制資料在地化存儲及國家級監控等措施，限制異議言論並打壓言論自由。
- **「防火長城」模式的建置：**巴基斯坦在其網站管理系統 (Web Management System) 中就採用了中國技術，其運作模式與中國的防火長城高度相似，進一步在網路存取及內容審查方面走向集中管制型態。

個案三：越南

- **對網路主權的相同重視：**儘管中越兩國歷史上多有衝突，近年來越南已逐步採納了中國式的資安政策，包括資料在地化存儲、網路審查法規及不同的監控措施。
- **該國資安法律及其與中國準則的相似性：**越南資安相關法律在好幾個層面上都跟中國的作法高度相似，比如說強制實行實名登記制度，以及要求服務平台為政府單位提供後門存取權限。

數位絲路已經成為中國通過數位技術和治理準則來擴大全球影響力的重要部分。這項倡議的核心就在於推廣以中國為基準的資安框架，其中並以網路主權、集權式管制以及國家主導的網路治理措施作為主軸。這項倡議也將觸角伸展到整個印太地區，一如ARTICLE 19在2024年發布的《數位絲綢之路：中國與數位壓制在印太地區的崛起》報告所示，在柬埔寨、馬來西亞、尼泊爾與泰國等地都能顯見中國模式的影響力。

儘管本報告只針對印太地區的三個個案進行探討，但中國在資安治理方面的專制模式已經遠超這三個個案的範圍。像是ARTICLE 19早先指出泰國在2014年軍事政變後，顯見線上監測 (online monitoring) 及大規模監控的興起。泰國政府亦曾討論設立全國網際網路閘道 (national internet gateway) ，來針對網路內容集中管理，可說是進一步向中國的專制模式政策靠攏。無獨有偶地，柬埔寨也在多個政策領域深受中國影響，無論是數位基礎設施的方針或網路治理。中國的資金投入和合作項目都讓其資安治理上的專制模式深植該國，並最終促成柬埔寨的《2022-2035數位政府政策方針 (Cambodia Digital Government Policy 2022-2035)》，其中更是明確將中國視為其正面典範一例。柬埔寨也意欲以國家網際網路閘道的形式，建立一套類似中國的防火牆。

本報告分享了三個新的個案研究——包括印尼、巴基斯坦以及越南。每一個個案都顯示中國的資安治理準則，正以獨特卻相關的治理途徑在各國重塑當地的數位生態系統，並影響著印太地區的資安治理及人權相關議題。這些國家也都是實際案例，展現出雙邊協議、與中國科技企業的夥伴關係，以及技術培力計畫，是如何成功地將專制數位治理模式深植當地。無論是印尼對中國技術的依賴、巴基斯坦以防火長城為藍本來建置監控系統，又或是越南如何翻版再製中國式的資安法律，種種個案都揭示著一個讓人擔心的趨勢：威權式的資安準則正逐步制度化 (institutionalisation of authoritarian norms)，國家控制將優先於成就個體自由及公民社會參與。

這些個案研究可被視為過往研究的延伸，顯示出當下發生的中國數位治理準則擴散現況，也象徵著這個現況對言論自由及其他人權議題所帶來的負面衝擊。更重要的是，這些個案研究已經點出，印太地區亟須尋求一個更以人權為本的另類資安治理取徑。

印尼

印尼是中國數位絲路策略的重要合作夥伴，此合作關係切中該國現下快速成長的數位經濟，以及對先進數位基礎設施的需求。在Doublethink Lab所發佈的「中國指數 (China Index)」報告中，印尼是全球第七大受中國影響的國家。中國亦將其眼光放向教育合作，藉此擴大影響力。以華為為例，他們就與印尼當地大學及政府單位合作，提供諸如雲端運算、AI及物聯網等領域的專業培訓。此外，中國還透過不同外交管道來加強與印尼在數位事務上的連結。在2021年，兩國簽署了一份與網路安全及技術合作有關的意向書，這象徵著兩國在數位治理方面會有更緊密的合作。這項協議有助於印尼的國家網路與情報局與中國的中央網信辦展開深度合作，協議內容聚焦在諸如資料安全及數位主權等議題上。

資訊安全治理

印尼的資安治理，可說是其在廣泛的國家安全框架裡相當重要卻尚未妥善發展的一個向度。作為一個快速數位化也持續深化其對數位基礎設施依賴的國家，如何保障其數位空間的安全，是印尼面臨的嚴峻挑戰。

資訊安全的治理架構

在印尼，由兩個主要機構掌管資安治理，包含通訊和資訊部及國家網路與情報局

通訊與資訊部，負責包含網路治理、電信及資安等業務。該部門過往因資料管理失當和缺乏面對資安威脅的預防姿態而飽受批評，且該部門亦推行嚴重侵犯言論自由的內容審查政策。

國家網路與情報局成立於2017年，主要負責資安相關政策、確保關鍵數位基礎設施保護，以及提升國家資安能力。然而，該局處面臨的是資源短缺問題，也欠缺有效應對複雜網路威脅的必要技術專業能力。

印尼在資安上面對的挑戰並不限於治理層面，也包含相關人才的嚴重短缺。該國的資訊與通訊部長Budi Arie Setiadi就特別點出，全球對資安專才的需求增長，預計在2023年為止將出現400萬名的人才缺口。該國專家也向ARTICLE 19表示，儘管印尼的私人企業大多在資料保護措施上表現相對得宜，國家機構卻往往忽視重要的資安實踐，比如定期的資料備份以及更新安全協議等。這種落差也導致數以百萬計的印尼公民面臨身份盜用、詐騙等數位犯罪的危險，也對國家安全構成嚴峻挑戰。透過填補資源上的缺口、強化通訊與資訊部及網路與情報局的協調合作，再加上引入先進的資安技術，印尼有望提升其面對持續演變之網路威脅的抵禦韌性。鑑於印尼所選擇採納的任何模式，都可能對人權保障產生深遠影響，在架構數位治理生態時，優先考量人權議題可說極為重要。

此外，印尼各行其政的資安法規體系也曾導致多起的人權侵害事件。雖然2008年所頒布的《電子資訊及交易法 (Electronic Information and Transactions Law [ITE Law])》所用的管理框架，但批評者指出該法條文模糊，將會對執法過程帶來嚴重隱憂。為求資料保護上更縝密的法制化措施，印尼在2022年通過了《個人資料保護法 (Personal Data Protection Law [PDP Law])。然而，該法的全面實施持續延宕，包含建立專責資料保護的監管機構等，在幾項重要條款的實行上都仍未見下文。整體來說，印尼在資安治理上缺乏有效的領導方向，也缺乏以人權為主的治理取徑。

中國對印尼資安生態產生的影響

印尼在資安治理上遭遇的挑戰，也促使其轉而依賴外部解決方案，這就包含了中國所提供的資源。中國企業持續向印尼提供先進的資安技術，尤其是在關鍵基礎設施及資料安全領域，而中國的專制治理準則也隨之輸入。

2017年的中國—東協資安研討會議：印尼的參與以及隨後帶來的政策轉向

2017年由CNCERT在青島舉辦的中國—東協資安研討會議，可說是中印兩國在資安領域合作關係發展上的重要里程碑。該研討會齊聚了包含印尼在內東協各國的資安專家及官員，共同討論持續演變的網路威脅，並分享在該區域提升資安韌性的相關知識與經驗。

印尼國家網路與情報局的代表，在會議期間積極與中國及東協各國的同行代表交流，希望深入瞭解中國式的資安治理取徑及危機處理機制。此次互動對印尼的資安政策有著深遠影響，促使其更仔細地重新檢視現有資安框架。會議期間的討論特別點出，有效協調的應對措施對資安事件相當重要，也同時指出加強區域合作的重要性。在這個討論中，中國一直是扮演著帶頭的角色。

值得一提的是，這次活動促使東協與中國在資安議題上有了更深度的合作，並直接促成後續東協與CNCERT/CC在2017年所簽署的合作意向書。此外，研討會也進一步凸顯出印尼在有一些升級資安實力的需求，包含打造更健全的危機處理系統，以及強化各個政府機關和民間部門利害關係者的協調機制。印尼政府便在中國主張的區域性治理重點影響下開始作為，不僅開始正視其在區域性資安組織中的角色，也開始以中國建立的標準為榜樣，積極建立更有力、更完善的資安協議。

中印間的合作意向書

中國透過多項合作意向書、國家論壇參與以及包含華為等企業的合作關係，實質形塑著印尼的資安政策。本節將分析有關中國影響力的幾個重要實例，並將聚焦印尼國家網路與情報局與中國中央網信辦的合作意向書，以及和華為之間為強化印尼資安基礎建設所進行的合作關係這兩個項目。

與CNCERT/CC簽署的合作意向書：內容、時間軸以及對治理帶來的影響

在中印兩國的資安合作上，印尼的網路與情報局和中國的CNCERT/CC在2017年簽署的雙邊合作意向書，是一個值得注意的重要里程碑。這份意向書建立起了一套正式的資安合作框架，不僅提升兩國提升處理網路威脅的能力，也推廣數位技術在資安上的使用。與中國設定的資安準則一樣，這份意向書強調對網路主權以及資料安全的重視。

這份意向書也為雙方在提升資安意識、培力計畫以及最佳實踐等方面的合作，提出了幾項原則。但這些原則實際上就是去採納中國的作法。意向書要求雙方針對新興網路威脅定期交換資訊、實施資安專業人才培訓計畫，並為建立網路事件的應對建立一套協作框架。在意向書簽署後，雙方展開的初始重點合作包含有共同工作坊及培訓課程。

簽署意向書對印尼當地網路治理的影響相當顯著。這份意向書本身就可以說意味著其資安取徑的轉向——不僅加重對中國的依賴，也傾向與非西方勢力合作。這樣的走向實際上是由好幾個不同的因素所造成的。

一方面，部分印尼官員及私人企業領袖漸漸開始認為，西方技術往往與自身地緣政治利益有關，不見得能妥善回應印尼本身的需求。其次，與中國等非西方國家合作取得先進技術及專業培訓，也往往不需要遵循過往西方援助附加的嚴謹人權要求或監管條件。

兩國的合作關係讓印尼對中國的依賴日深，引發關於權力平衡以及逐步採納中華人民共和國網路治理威權模式的疑慮。

國家網路與情報局和中央網信辦間的合作意向書：華為在合作框架上扮演的角色及其對資安作

法帶來的影響

中國對印尼資安生態帶來影響的另外一個顯著案例可見於中央網信辦和印尼網路與情報局簽署的意向書，這項協議促成了網路與情報局和華為的合作關係。這份合作意向書是雙方開始有系統地一齊推動資安培力計畫、技術共享，以及資安基礎設施發展的一個縮影。

在這份合作框架中，華為的角色十分重要，從協議在2019年簽訂後，他們就積極地與印尼共同提升其資安水準，雙方並在2021年續約。華為也協助印尼網路與情報局展開各式各樣的培訓計畫，舉辦工作坊主題包含5G安全、資安事件的應變手段，以及打造資安規範。

印尼網路與情報局和華為之間的合作，主要聚焦在協助印尼制定國家資安策略、推動更大範圍的公私領域合作，並鼓勵印尼在資安治理上採取更積極的態度。在2023年再次續約後，雙方既有的夥伴關係可說又進一步地加深了。然而，華為在印尼資安事務的深度參與也引起諸多疑慮，特別是該公司對於國家安全及資料安全的參與程度。批評者就指出，過度倚賴和中共關係密切的企業存在風險，特別是資安工作和相關需求有其敏感性，但中國資通訊業者卻依法受到中共的掌控與監管。此意味著國家網路與情報局和華為間的緊密合作，有可能導致印尼的數位基礎設施暴露在後門存取的風險下，這會帶來在言論自由和隱私權上的嚴重隱憂。印尼對中國式的專制資安模式的依賴，都可能催生更嚴苛的內容管制規範。印尼通訊與資訊部在近期頒布的新規範就是一個實際的例子。

中方參與所造成的政策轉向

隨著印尼不斷深化與中國的合作，該國在資訊安全、數位治理以至於資料主權等議題上的作法，都可以看到明顯轉變。
印尼對網路主權的重視就是其中一例，這體現在該國於2022年通過的個人資料保護法(Personal Data Protection Law [PDP Law])上。是次立法對個人資料的處理及相關境外存取採取了更嚴格的管制手段。儘管該法符合加強資料保護的全球趨勢，卻也是印尼在中國科技巨頭等外來企業影響下做出的反應。印尼與CNCERT/CC以及中央網信辦簽訂的幾份意向書，都進一步顯露出該國朝向資料在地化發展的態度。

然而，當地的個人資料保護法，也並不表示毫無保留地全盤接受中國的資安模式。該法同時也是印尼對數位生態中外部干預的應對措施，比如說對資料主權及資訊安全上的顧慮，而這些威脅並不僅僅來自於中國。也就是說，與其說是直接受到中國影響，不如說該法反映著印尼目前在網路治理上仿效中國「網路主權」模式的目標。

另一個政策轉向的跡象，是一些策略性數位結盟。持續與中國科技巨頭合作，廣泛地影響著印尼當地的數位策略。該國對數位主權以及基礎設施現代化的側重，實與中國由國家掌控網路治理以及「以安全保發展」的思維高度吻合。而與中國企業攜手開展5G網路、AI與雲端運算等發展項目，也正符合印尼在2035年以前成為數位經濟體的大方向目標。

以上提到的合作關係正影響著印尼的資安治理模式與策略方向。政策轉向的跡象也進一步證明，這類雙邊關係正對印尼國內政策產生日益增長的影響。

官方訪問與外交合作

在與日俱增的資安及數位基礎設施合作上，一些官方訪問及外交協議，是中印雙方目前主要的溝通管道。這一類高層互動促成了幾項重要意向書的簽訂，同時也是深化雙邊合作的重要舞台。

舉例來說，中國外交部長王毅在2021年出訪期間，就拋出擴大兩國在技術與資安領域合作的構想。會談最後促成中國中央網信辦與印尼的國家網路與情報局簽署有關合作意向書。值得一提的是，這是中國首次就資安議題與外國簽署的合作協議。這份意向書的內容為雙方就提升網路

安全及資料治理的合作打下基礎，並主張兩國應在尊重網路主權的原則下，加強網路空間中的合作。這份協議也體現出，在資安甚至廣義的數位治理層面上，中國對印尼與日俱增的影響力。

華為則是另外一個值得關注的例子，該公司在中印雙方的數位外交中也扮演著關鍵角色。藉由參與當地數位基礎設施的擴建，以及和當地業者開展合資事業，都讓華為成為外交關係中相當有用的一個旗子。華為致力於搭建當地的5G網路與資料中心，並持續與印尼政府及當地科技公司展開合作，這都顯示出其在雙邊關係中的重要戰略地位。華為目前也是印尼政府數位轉型的計畫的核心要角，除了協助發展AI實力，也替當地擴建雲端運算所需的基礎設施。這些合作計畫都持續加深印尼對中國技術的依賴，這也與中國在地緣政治的目標不謀而合，有效深化自身技術及準則影響力。

培訓與培力計畫

在技術面之外，中國藉由培訓與培力計畫等軟實力層面帶來的影響也不容小覷。藉此，中國正在將自身治理框架深埋進印尼數位基礎設施的根基之中。在此，華為也扮演了重要的關鍵角色。

比較知名的例子像是「資通訊學院 (ICT Academy)」和「未來種子計畫 (Seeds for the Future)」，透過這些培力專案，華為積極與印尼當地的學生與專業人才接觸，向他們提供AI、雲端運算、大數據以及5G相關的培訓課程。此外，華為也正與印尼總統府幕僚辦公室 (Presidential Staff Office) 合作一項五年期的職業培訓計畫，期間將為超過十萬名的印尼官員提供教育訓練。這也凸顯出，對於印尼未來數位人才的養成，中國擁有一定程度的話語權。

值得注意的是，華為並不單單只是協助當地公部門的教育訓練，相關的技能培訓計畫更是深入其他領域。他們和印尼最大的電信商Telkomsel緊密合作，為旗下員工提供200天的培訓課程，主題從5G技術、雲端運算、AI到顧客體驗管理都有。提供這些學習機會的同時，華為不僅僅是在為印尼打造所需的技術人力，也進一步影響當地數位基礎建設發展的方向。這些培力專案是中國透過數位絲路打造區域影響力的縮影，不僅深化中國科技公司在當地數位發展中的角色，也讓中國技術與數位準則深植當地。

巴基斯坦

將中國視為快速現代化的策略工具

在Doublethink Lab的「中國指數」中，巴基斯坦的受中國影響程度是全球第一。資通訊業界中，諸如華為、中興、中國移動以及阿里巴巴等中國科技公司，都在巴基斯坦的數位基礎設施建置中大舉投資，而這些投資也都可以被視為是2015年開始的中巴經濟走廊以至於數位絲路合作計畫的一部分。事實上，中巴兩國間早在數位絲路之前就已經有過數位合作。舉例來說，2013年巴基斯坦是第一個採用「中國北斗衛星導航系統」的國家。更近期的例子，也有像是2024年五月，中國在兩國合作下，成功發射巴基斯坦的多功能通訊衛星Paksat-MM1，該衛星可以提供衛星寬頻網路連接等數位服務。

除了採納中國技術及數位基礎設施結構，巴基斯坦也逐步納入中國制定的數位標準。巴基斯坦數位生態系近年的這些發展，都在在顯示出中巴雙方雙邊關係的深化，也顯示出中巴兩國科技企業的交好。儘管這些無論技術或資金的投入，都讓巴基斯坦的現代化與網路完善程度大有提升，卻也同時帶來有關數位治理、技術準則、政府管制，以至於專制模式擴張的疑慮。在與中國政府和資通訊企業密切合作甚至學習的過程中，巴基斯坦的網路環境正逐步走向一個更受箝制、內容更受審查的狀態。這也體現在現任總理Shahbaz Sharif對中國現代化模式的大加讚揚，並將其視為巴基斯坦發展資訊科技的未來典範。

巴基斯坦採納中國治理框架的幾個層面

向中國專制模式靠攏的國家機構

巴基斯坦國家網路緊急應對小組 (National Cyber Emergency Response Team of Pakistan, PKCERT) 在該國《2021年國家資安政策》指導下成立，是打造該國國家資安架構的主責機構。在這個架構下，PKCERT專責處理網路安全事件以及加強該國網路韌性。跟中央網信辦手握不受約束的廣泛權力高度相似，該機構在2023年頒布的規範中就提到為了主動應對CII可能面臨的數位威脅，PKCERT需要賦予自身廣泛的資訊搜集許可及監控權。 然而，該規範中卻未能明確定義什麼是CII，導致監管範圍模糊且有擴張的可能性。這份規範也提到，巴基斯坦將成立國家電信網路緊急應對小組 (National Telecom CERT, NTCERT)，並由巴基斯坦電信管理局 (Pakistan Telecommunication Authority, PTA) 來負責NTCERT安全維運中心 (Security Operation Centres) 的營運。NTCERT的重要性在於，他將負責監督巴基斯坦全國範圍內的電信通訊業務及資料。而之所以特別提到PKCERT，則在於該組織的動作頻仍：儘管該組織才剛草創，並積極參與在各大國際論壇中，展開諸多國內和國際上的合作，其中就包含相當多和中國之間的合作。

舉例來說，PKCERT總監Haider Abbas就在2024年北京網絡安全大會上，受邀擔任主講嘉賓。席間，他特別提到PKCERT亟欲和CNCERT展開合作，一同應對資安威脅甚至共推全球網路韌性。這類言論都顯示出，巴基斯坦有意就資安準則方面向中國的做法看齊，甚至進一步將中國思維套用在既有的資安立法框架上。

約束資訊安全的法律框架

要瞭解巴基斯坦在治理數位空間的立法方向，必須瞭解到過往的各種反民主事件 (比如幾次對民選政府的軍事干預行動) 事實上對現在的立法框架有顯著影響。事實上，巴基斯坦的數位監管方向在過去十年裡就經歷過重大變革。2014年政府為打擊恐怖主義所頒布的國家行動計劃，是一個很好的例子，該計畫強調必須採取行動「對抗恐怖主義對網路及社群媒體的濫用」。其次，2016年訂定、主責規範科技相關犯罪的《電子犯罪預防法》 (Prevention of Electronic Crimes Act, PECA) 也值得注意，該法讓我們檢視該國對數位犯罪的定義及應對措施。

該法在2018年通過修正法案，進一步確立該國聯邦調查局 (Federal Investigation Agency) 監控、調查及起訴各類網路法罪的法源。這些網路犯罪的定義包含：存取甚至竄改未經授權的資料、網路詐騙、網路恐怖主義、仇恨言論、網路霸凌以及兒童色情等。

對照之下會發現，巴基斯坦的《電子犯罪預防法》和中國的《網絡安全法》有著極高的相似度。舉例來說，2016年的原始法案就規定，服務供應商有義務至少保留經手資料一年，這部分與中國法規相似度極高。此外，法案中也以「不實資訊」以及聲譽毀謗之類的名義，將各類批判性言論列為刑事犯罪，這便和反對誹謗罪刑事化的國家人權準則有所抵觸。2016年的法案中還提到，任何對「巴基斯坦安全或國防」有關的批評言論都應嚴令禁止，這也跟中國《網絡安全法》中禁止傷害國家安全的網路活動一樣，都是以國安為名打壓異己言論。

而2018年的修正法案，則進一步賦予該國電信管理局更大的權力，讓他們可以隨意撤下網上批判性言論，或是要求社群媒體公司將其定義為「非法內容」並下架處理。這一系列為審查行為建立法律基礎的的立法與規範，都跟中國《網絡安全法》極為相似。該局處目前採用2016年法案中的一系列定義來封鎖所謂的「非法內容」，這些定義通常針對社群平台（諸如原稱推特的X平台）、批判性媒體機構（如FactFocus）以及反對黨的網站（如巴基斯坦正義運動黨 [Pakistan Tehreek-i-Insa] 、人民工人黨 [Awami Workers Party] 等）而來。這些無論是下架或是封鎖的行為，都構成了對言論自由的肆意侵犯。截至2024年八月，該局處就透過深度封包檢測技術 (deep packet inspection) ，來阻擋使用者存取超過2,300個網站以及180個手機app。

巴基斯坦電信管理局現在也正在提案修法，希望在2024年的《數位巴基斯坦法案》中，規定網路營運商採取實名身份驗證措施。該局處提出的構想是，行動服務營運商有義務驗證使用者身份，並盡可能在其中使用生物識別技術。該局處甚至考慮在未來利用一個中樞資料庫儲存身份資料，來達成更精準的身份驗證程序，並在數位生態系統中提升各利害關係者的可問責性。這些措施可說相當程度地借鑒中國的數位治理準則，也讓該國未來的隱私權及言論自由蒙上一層陰影。

濫用《電子犯罪預防法》來處理誹謗、數位恐怖主義以及封鎖「非法內容」，實際上已經箝制了民間社會及媒體的正常運作，也成為打壓異己言論的工具。該國記者目前就面臨極大挑戰，只要在諸如X、Facebook及YouTube等平台上發表批判性言論，就會受到聯邦調查局的騷擾。而2024年大選期間的爭議，也使該國從當年二月開始封鎖X平台至今。巴基斯坦的相關作為並不僅限於國內，巴國在國際論壇上也積極發聲、支持專制政策。比如說聯合國在草擬《網路犯罪條約 (Cybercrime Treaty) 》的過程中，巴基斯坦就與中國和俄羅斯一同，以打擊網路恐怖主義及不實資訊威脅為名，主張以網路主權和審查機制為主，更集權、更偏向多邊互動為主的治理準則。

該國擁護網路主權概念的實例，還包含一項電信管理局在2024年八月宣布的政策計畫，其中規劃限制未經許可的VPN使用，而這也與過往中國工信部提出的措施相當雷同。這項政策規劃建立一套VPN的白名單，僅允許國內使用經授權的VPN網路。這其實已經不是該局處第一次提出類似的計畫，巴基斯坦當地的數位權利組織Bolo Bhi就曾針對2020年時類似的政策提案提出警告，認為強制VPN服務登記在案並封鎖不合規定的服務提供者，將加劇網路碎片化並讓政府的監控行為更為猖狂。

而就在2025年的1月23日，巴基斯坦國會新近通過了《電子犯罪預防法》的增修條文，又再次進一步地擴大對網路內容控制的範圍，使得言論自由受到進一步的打壓。條文的一部分強調對抗「虛假資訊」的重要性，藉此作為擴權的名目。

另一方面，2023年的《個人資料保護法案》雖尚有待參議院最終批准，卻也值得關注。該法規定採取與中國類似的資料在地化措施，讓政府得以有權監控並管理個人或公司資料。早在2018年增修版的《電子犯罪預防法》條文，當局就已經要求社群媒體公司將使用者資料儲存在巴基斯坦

境內。儘管該國政府曾在立法過程中與民間社會及科技巨頭溝通，這樣的立法方向依然因為隱私權上的疑慮而受到強烈反彈。即便如此，巴基斯坦現行的政策走向依然向中國在數位治理上的專制模式看齊，一樣是打著資安及打擊數位犯罪的旗號，把重點放在國家對資料的掌控權。

中國影響所帶來的新興監控技術

巴基斯坦總理Shehbaz Sharif在中國會晤國務院總理李強後，雙方的聯合聲明可說是進一步確認了巴基斯坦對中國技術的依賴與信任。這份聲明不僅鞏固中國在巴基斯坦數位轉型中的核心地位，雙方領導者並著重在AI、5G、大數據、雲端運算，甚至航太科技等領域的合作。值得注意的是，巴基斯坦也逐漸在AI倫理及治理框架等議題上，向中國看齊。會後的聯合聲明就提到：「巴方歡迎習近平主席宣佈的《全球人工智能治理倡議》以及中方為增強發展中國家在人工智能全球治理中的權利所作努力，」

除此之外，從巴基斯坦目前的《國家人工智慧政策》草案，也可以更清楚地發現該國在AI及其他新興科技的治理上都明顯與中國的政策風向趨同一致。該項政策草案特別在內文中提及「中巴人工智能中心 (Sino-Pakistan Center for Artificial Intelligence, SPCAI)」，該中心目前座落在中國、巴基斯坦及奧地利三國學術機構合作成立的「巴奧科技應用科學研究所 (Pak–Austria Fachhochschule Institute of Applied Sciences and Technology)」中，位處巴基斯坦的哈普里爾 (Haripur) 地區。一如政策目標第6點所規劃的，SPCAI中心目前積極與廣東工業大學、深圳先進技術研究院等單位維持緊密的學術及商業關係。

此外，這份草案也在政策目標第11點中提到，希望能夠透過SPCAI中心展開雙邊或多邊合作，訴求建立監管框架，以便採納全球最佳實踐來推動AI的發展和普及。巴基斯坦也同時將AI策略與國家發展目標整合，借鑑中國在AI領域領頭的野心。在AI實踐上，看得出來巴基斯坦正在採納中國式的AI標準，這種作法主張建立一套以國家為中心的治理模式、鼓吹審查制度以及用於監控的演算法，有別於由IEEE、ISO、ITU以及OECD等組織所發展、被全球普遍採納的標準。這一系列的技術與政策走向，都可能讓巴基斯坦政府將來有能力對公民採取更綿密且高度自動化的監控措施。

巴基斯坦的「防火長城」翻版

數位主權需要防火長城來維護的這套論述，大概是中國整套數位基礎設施及資安治理思維的核心。而這套論述現在也正在印太地區蔓延，一如ARTICLE 19早前報告所提出的，柬埔寨、尼泊爾與泰國等地，都在政策上或是技術上直接採納或是間接受到影響。巴基斯坦也無法倖免於此。

巴基斯坦的電信管理局早先已宣布，將從2024年的1月開始升級該國網頁管理系統 (Web Management System, WMS)。這次升級中加入了先進的深層封包檢測技術，這種技術可以讓政府從網際網路閘道層級就管制網路流量。這也令人憂心是否政府在基礎設施層級上，就能進行內容審查及監控行為。據傳2018年時巴基斯坦原本是向加拿大公司Sandvine購買上一代的WMS設備，但最近的轉變就顯示出該國不僅擁抱中國的基礎設施治理作法，也開始廣泛採用中國技術。

這次升級目前獲公開的採購紀錄相當有限，巴基斯坦的電信管理局曾在2024年7月公布一項次世代防火牆 (Next-Generation Firewall) 的招標計畫，但他們後來澄清該計畫的硬體只會用在單位內部網路。儘管資料有限，但新一代的WMS明顯和中國的防火長城有不少相似之處。巴基斯坦政府曾多次保證不會實施全面的防火長城，但該國據報已在兩個最主要的網路交換點部署防火牆。正因為電信管理局的作法缺乏透明性，也讓各界仍憂心中國式防火牆在該國的發展。

越南

兩國同樣主張一黨專制的意識形態

越南政治學者阮克江指出，中國與越南之所以會在各領域上相互借鑒，主要是因為兩國有著共同的政治意識形態背景。他表示，越南整體戰略方向符合目前中國擴大影響力的企圖心，這也包含在數位治理層面的規劃。透過兩國共有的「市場列寧主義 (market-Leninism)」框架，執政黨擁抱市場經濟卻維持在民生各個層面的政治壟斷，透過經濟改革開放的繁榮來替政權打造合法性，卻也讓政治上的開放遙遙無期。而兩國這類作法的相似性，在科技發展及治理這塊特別凸出。

越南目前將中國視為「全面戰略夥伴 (comprehensive strategic partner)」，這是越南外交政策體系中最受禮遇的外交層級。習近平在2023年12月造訪越南時，兩國聯合聲明提到，雙方將就政治安全、政府安全及政權安全領域深化合作。值得注意的是，聯合聲明提到兩國同意在資安議題上強化合作，並「加強雙方情報交流及反干涉、反分裂、就防範反對敵對勢力「和平演變」、「顏色革命」、分裂等問題加強經驗分享與合作。」

而中越兩國安全部門定期舉行的會議，也都反覆強調在資安面合作的重要性。舉例來說，2023年的12月，就在習近平訪問越南的幾天前，兩國公共安全部長便達成一項協議，將一同籌辦更多的資安培訓計畫，並提供設備來協助彼此對抗高科技犯罪。2024年1月，雙方也在類似的會議中，簽署了一份合作意向書，內容主要是同意兩國部門交流經驗、共同防範、打擊並應對不同的網路濫用行為，特別是誹謗或中傷黨與國、破壞安全及公共秩序，以及損害中越友好關係的活動。接下來，我們還會進一步發現到，雙方對數位主權概念的共同信仰，是兩國數位專制主義的理論基礎。

被當作數位主權議題的資訊安全

越南在2012年的4月18日成立了專責資訊科技的軍事部門，呼應著中國不到兩年前在規範性白皮書中提出的類似概念，該軍事部門的職責包括「在數位空間中保衛國家資訊主權。」

另外一個將越南網路治理常態化的重要里程碑，是2013年7月15日發布的第72/2013/NĐ-CP號法令。截至2024年12月，這依然是該國在網際網路管理上最重要的法源文件。該法規定：「跨境向越南使用者提供公共資訊 (或允許來自越南境內的網路存取) 的外國組織、事業或是個人，都應遵循相關的越南法規或規範。」該法的提出，可說是政府首次試圖強制外國公司遵守當地法律，也象徵著該國向網際網路主權主張的靠攏，和中國彼時的思想與作法一致。

緊接著在2014年1月14日，時任越南總理阮晉勇 (Nguyễn Tấn Dũng) 發布了一項決議文件，其中就明確提到「數位空間主權 (chủ quyền không gian mạng, or chủ quyền số quốc gia)」一詞。次年，時任越南公共安全部長，並於其後在2016至2018年擔任越南國家主席的陳大光 (Trần Đại Quang)，在其著作《網路空間——其未來與行動 (Cyberspace – Future and Actions)》中，也積極倡導網路主權的概念。書中，他將習近平在2018年網絡安全和信息化工作會議上的演說，視為形塑越南資安政策的重要靈感來源，並提到：「沒有資訊安全就沒有國家安全。網際網路與資訊安全兩者都已成為中國亟須面對的新挑戰，且兩者都與國家安全及社會穩定性息息相關。」

2016年，陳大光正式經越南國會選為國家主席，該職位是越南政治體制中權力最大的四個職位之一 。任期內，他持續推動越南公共安全部起草《資訊安全法》。在2017年8月的一次談話中，他也強調越南有必要要求外國公司將資料存放在該國境內，並加強對社交網路的控制。陳大光可說是讓該國資安政策走向中國專制典範的重要推手。

自此，越南共產黨 (Vietnamese Communist Party, VCP) 的官員和智庫廣泛就網路主權議題進行討論，也讓這個概念成為越南網路治理的立基理論。在2021年12月舉行的《在網路空間中保衛

國家主權》會議，就是一個重要例證，三名政治局 (Politburo, 在各國共產國家中擁有黨內實權者構成的組織) 官員皆列席其中。

近期，時任公共安全部長，也是2018年資安法主要起草人的蘇林 (Tô Lâm) 出版了《數位空間主權：時代挑戰及國家的責任 (Cyberspace sovereignty – The Demands of the Era and National Obligations)》一書，書中論及當今面對的網路威脅，並藉此正當化對網路更嚴格的管制措施。其後，2022年4月以及2024年2月召開的幾場座談會，都針對該書以及網路主權模式進行討論，進一步為這個概念建立正當性。2024年8月，蘇林當選越共中央總書記，進一步讓他成為該國掌權者。這一系列的事證都點出越南是如何將網路主權概念納入其大方向的黨內論述、法律及規範中，而這都和中國採取的作法極其相似。

中國在越南2018年資安法中留下的影響

越南在網路治理層面借鑑中國的早期例證之一，可以追溯到2011年在越共官媒《人民報》(Nhân Dân) 發表的一篇文章。文中分析中國在內容審查、實名登記規定、懲戒使用者言論以及防火牆使用上的效益。

次年，越南人民軍官網上，刊出一則由越共中央宣傳部副部長阮世紀 (Nguyễn Thế Kỷ) 參與編寫的文章，是另外一個例子。該文重點介紹中國的治理經驗，並指出中國的作法是「建立『防火牆』來防堵被認為有重大風險的外國社交平台，同時要求網路服務供應商將伺服器設在中國境內。」阮世紀過往也曾在2010年於越共中央宣傳部官媒《Tuyên Giáo》雜誌上。刊載一篇文章，內文討論借鑑中國網路法規的可能性。

這一系列的文章都顯示，早在2018年越南《資安法》公布前，越共官員早已對該法內文多有討論，並從中國的準則制定方向上汲取養分。與中國作法相似，越南在2018年推行的《資安法》最終成為越南網路治理模式的施行基礎。該法不僅有可能是該國法制史上最具爭議性的法規之一，在幾個重要層面上，其內容也展現出其與中國相關法規的高度相似性。

首先，兩國的資安法在資訊安全的定義上，都和一般民主國家常見的理解有很大的差異。在一般的民主體制下，人們普遍認定資安的目標有幾個，包含維繫技術層面安全的網路空間 (a technically secure cyberspace)、避免網路攻擊、網路入侵及未經授權的資訊存取等，且普遍認為不應包含內容控制。

與民主國家不同的地方在於，中越兩國法規對資訊安全都使用更廣義的解釋方式，將適用範圍擴及到一些非技術層面，比如說內容審查、個人資料的保護與在地化儲存，以及限制對執政黨的批判性言論。兩國法律相同的部分在於，兩者都將網路空間中的資訊與資料處理，視為國家安全的範疇，將資安等同於保護黨及政府官員，甚至是專制政權的合法性。

就在2018年越南《資安法》通過後，時任越共總書記阮富仲 (Nguyễn Phú Trọng) 表示：

全球範圍內，許多國家都有類似的一套法律。在當今第四次工業革命的時代，技術帶來許多福祉，卻也為管理增添不少挑戰。在這個背景下可能產生的是，各種煽動、抗爭、騷亂，甚至顛覆政府的意圖。是此，這套法律對於政權的保衛是必不可失的——人民不應肆意妄言或任意羞辱他人。這份言論大致反映出該法的核心精神，亦即明確將網路空間中的「反國家言論」視為非法行為。越共的中央宣傳體系此後也持續在各種場合呼應這套敘事，特別是2023年以及2024年的數個例子。

除了對資訊安全的定義不同外，兩部法律中使用的另一套類似詞彙，是第二個值得關注的層面。中方法條的適用範圍特別提及「關鍵基礎設施」，而越南則同樣特別提到「攸關國家安全的資訊

系統」。我們可以透過觀察這些相似的法律措辭，來檢視這兩部法律是如何處理相關事務，尤其是在內容控制上雙方相似的思路。

第三個層面在於中越的兩部法律都要求實施嚴峻的網路內容審查。越南的法條中明文規定，禁止發布「鼓吹反對越南社會主義共和國的內容；煽動暴亂、影響安全或擾亂公共秩序的內容；侮辱性或有關誹謗的內容；以及破壞經濟秩序的內容」，這都和中國的資安法條高度相似。而該法也為其它對內容審查更為細緻的規範帶來法源基礎。整體來說，由於兩國法律條文都相當含糊且缺乏第三方獨立監察，執法單位往往可以任意解釋法條，獨斷地壓制批判和異己之聲

第四，兩部法律都強制要求境內及境外科技公司實施資料在地化，作為一種管控手段。這也是一個反映網路主權概念的規範，要求科技公司在境內的實體伺服器、資料中心儲存資料。

第五，兩部法律都規定社交平台使用者以實名註冊，並要求平台在註冊程序中驗證這些使用者的身份資料。這項規範可說直接侵害了隱私權及網路自由中的匿名性原則。如果缺少匿名性，網路使用者就必須向官方公開他們的身份及網路活動，讓他們有效地落入政府監控的範圍內。這不只讓監控者有能力掌握他們的隱私和要害，也進一步讓言論自由蒙受被壓迫的風險。

最後，兩部法律都要求網路使用者及科技公司扮演向黨通風報信的角色。使用者有義務主動向官方舉報網路上的「有害資訊」。而科技公司更有義務主動過濾平台上的內容，並在官方要求時提供使用者資訊。

質言之，這一連串相似的法條效力，都可以佐證越南多方借鑑中國早其兩年實施的《網絡安全法》。

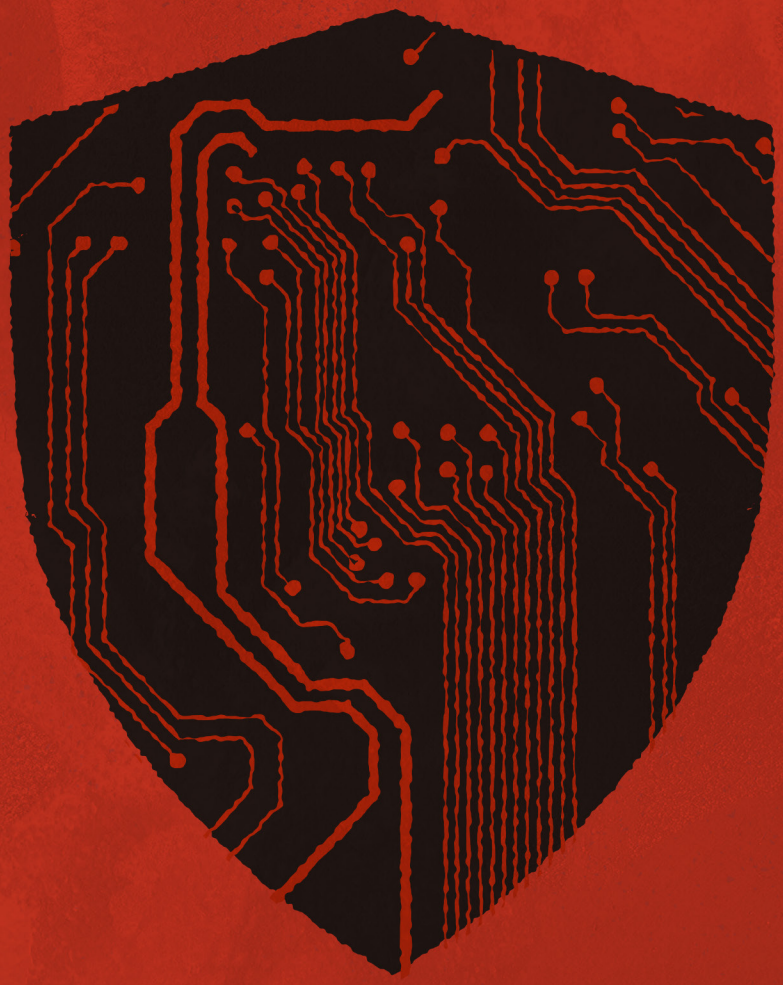
整體來說，越南的資安法特別著重在如何要求海外科技公司遵循當地法規。在境外平台諸如Facebook和Google上流通的外部資訊，因為缺乏有效的管制措施及施壓手段，一直是越南政府管理上的一大挑戰。越南一部份也是為了解決這個問題，所以積極參考中國的專制模式。事實上，在2017年呈向越南國會的立法草案中，越南公共安全部就公開表示他們主要是借鑑中國來起草法條內文。

越南的資安治理措施在2018年後依然在持續發展，後續的法律文件也都在各個層面擴充當年《資安法》的框架。像是第53/2022/N□-CP號法令就針對資料在地化提出一套相對有彈性的管理方案：外國科技公司只要能滿足政府對內容審查及使用者資料存取的要求，就可以豁免將資料儲存於越南境內。又或是第13/2023/N□-CP號法令，內文進一步闡明資安法對個人資料的管控範圍：該法令讓政府能在國安及犯罪防制的前提下，逕行存取其公民在線的個人資料。這條法令另一個值得關注的重點是，它讓越南公共安全部門一樣有權透過各種模糊的理由，禁止個人或組織將個人資料傳輸到海外。

而2024年12月25日生效的第147/2024/N□-CP法令，則正式實施2018《資安法》中提到的實名驗證規範。法令強制社交平台使用者以真實姓名註冊，並要求平台透過當地的手機號碼或是身分證件來驗證使用者身份。這項法令同時也讓政府有權限制不合規範的使用者繼續使用網路服務、封鎖無法配合規定的平台，並要求平台開啟後門便於政府搜查時瀏覽平台內容。

綜上所述，中國的網路主權概念實際上已經成為整套越南監管機制的基礎。我們可以說，來自中國的網路主權概念，奠基了2018年的《資安法》及後續的幾項重要法令；而中國的治理準則作法，則深植在這些法條、法令的立法方向中。在這一系列法規所提供的基礎上，越南已經開始大舉採取行動，擴大對網路言論及個人資料的管制。他們現在的目標是，把過去在現實空間中採用的管理手段，有效地延伸到網路言論上，並且讓當局最終有能力將使用者的個人資料當作執法及迫其就範的工具。

台灣的資安策略



一條兼顧國家安全與自由的路

重要研究發現

別具特色的民主資安模式

- 台灣在帶出完善資安措施的同時，不忘兼顧民主價值，著重在多元利害關係者的參與、施政透明，以及保護言論自由與隱私權，中國推行的專制準則有鮮明對比。

與日俱增的中國網路威脅

- 台灣政府每天面臨多達240萬次的網路攻擊，包含海底電纜設施等CII都是經常被攻擊的對象。幾次的重大事件，包含南希·裴洛西 (Nancy Pelosi) 2022年訪台期間的大量網路攻擊，以及諸如NoName057等駭客組織的網路行動，都說明著台灣每天面對的是持續性、高複雜性的資安威脅。

施政透明與公共參與

- 台灣將公共諮詢程序納入立法過程中，透過像是「公共政策網路參與平台」這類的管道來在立法上兼顧安全需求和公民自由，並達到資安治理上的可問責性。

以人權為本的執政模式

- 面對各方威脅，台灣不願採取以維穩為重的數位發展策略，並且強調施政上的透明性、各界合作以及民主原則。可以說，台灣致力成為中國專制數位治理模式的一個對比。儘管挑戰不斷，台灣確實向我們證明了，有效的資安防護並不需要以犧牲基本自由為代價。

台灣正面臨著不斷升溫的威脅局勢，其所面對的網路攻擊規模前所未見。中國不斷加強他們的「灰色地帶戰術 (grey zone tactics)」來干預台灣，其中的各種網路活動，都結合中共統一戰線工作部的宣傳訊息，向台灣灌輸兩岸統一的敘事。台灣國安局的文件中就提到，2024年間，台灣政府每日平均遭受大約240萬次的網路攻擊，是2023年的兩倍。這已經凸顯出該國面臨挑戰的嚴峻程度。

這些網路威脅最早集中在政府機關上，如今卻也開始轉向產業界，包含針對網路基礎設施實體層的攻擊，像是海底電纜就曾遭受攻擊。威脅範圍的擴大，也讓經濟發展和各類商業活動的嚴重中斷更有可能發生。此外，對網路基礎設施的攻擊，也會嚴重影響通訊傳播及各類網路使用，進而損害言論自由及資訊近用權。

事實上，台灣作為地緣政治導火線的角色與其作爲資安攻擊熱點密不可分。像是2022年8月美國眾議院議長南希·培洛西為演講訪台，就引發中國政府的強烈反彈，大動作展開軍事演習並發動為期九天的一系列網路攻擊。這些攻擊主要是分散式阻斷服務 (Distributed Denial of Service, DDoS) 攻擊、竄改網路頁面，以及一系列真實度極高的虛假資訊宣傳活動。除此之外，在2024年9月10日，親俄駭客組織NoName057稱其針對台灣政府部會網站及關鍵基礎設施，發動了一系列的DDoS攻擊，並將行動命名為「OpsTaiwan」。在當月14日的記者會上，台灣的數位發展部表示，他們確實有觀測到45起攻擊事件。這一系列攻擊鎖定的是當地的稅務機關、區域民航站、主計總處、金融機構及電信業者。所有這些境外攻擊都顯示台灣亟須一套完善卻能兼顧透明與人權的資安治理措施。

儘管網路威脅頻繁，台灣依然開創了一條別具特色的資訊安全之路。台灣的作法把開放性擺在最前面，讓所有來自產官民三界的聲音都能被聽見，也讓公民權利在資安政策中始終能被重視。儘管面對極其複雜的維安挑戰，台灣向我們證明，不是只有犧牲人權才能有效對抗數位攻擊。這份研究顯示出台灣能被當作一個值得參考的實際案例，讓我們知道民主政權如何能夠在不犧牲基本價值的前提下去面對網路威脅。

台灣的資訊安全策略

以上這些威脅事件都可以讓我們發現，台灣在規劃資安治理上的最大難關，在於如何有效應對中國日益複雜的數位威脅。和以上個案或中國不同的是，台灣還必須審慎兼顧資安風險及核心民主價值，包含捍衛與推廣言論自由以及人們的隱私權。這樣複合式的目標其實就凸顯出台灣數位治理的特色在於，試圖建立一個安全卻又兼顧人權價值的數位環境。這樣的想法目前已在2016年的《國家資通訊安全發展方案》中獲得落實。台灣的這套方案有四大核心目標：強化基礎設施保護、打擊數位犯罪、促進公私部門協力並建立國際夥伴關係。國家通訊傳播委員會 (National Communications Commission, NCC)、國家安全會議下轄的資安辦公室以及行政院資通安全處（現數發部資通安全署）三者為方案的主要執行單位。儘管這一系列的發展框架展現出該國完善治理措施的決心，實際執行上的調度及資源分配依然相當有挑戰性。

2016年前總統蔡英文上任後，台灣啟動「資安即國安1.0」計畫。這該計畫目標在於打造一套基礎的政策性框架，包括制定《資通安全管理法 (Cyber Security Management Act, CSMA)》、評估

行政院資通安全處的效益以及創立國防部資通電軍指揮部。隨後在2021年，夾帶著這樣的基礎，台灣啟動了第二階段的「資安即國安2.0」計畫，希望能進一步補強組織架構、法制缺口、人才缺口並更好地與產業界整合。

所謂的「資安即國安1.0」框架，主要的功能是規劃在2016年到2020年間，打造一套由國家安全會議、NCC及行政院資通安全處組成的鐵三角架構。而「資安即國安2.0」計畫則是要進一步將軍方、情治與執法單位，納入國家資安戰略中，希望在2021年到2025年中將國家資安框架發展成一套多重支柱 (multi-pillar) 框架。

以目前來說，這套架構中包含國家安全會議、國防部、數發部、國安局、調查局以及刑事警察局等單位。台灣的現行策略主要著重在如何強化組織架構並加強各單位間的合作，2022年8月成立的數發部是一個很好的例子。但這樣的做法要能成功，台灣也必須要嘗試解決長久以來分權治理模式中的權責及問責問題。正因如此，台灣從2016年便開始將資安治理事務制度化，並以「資安即國安」的概念來統整各部會。

台灣的資安法律架構

台灣資安規範的演進史

台灣在2018年通過《資通安全管理法》，象徵著該國政府開始強化資安治理框架。該法為政府各部會以及關鍵基礎設施營運商所肩負的資安職責，初步提供了法律依據。而後在2023年，數發部繼續推動資通安全管理法的修法，內容聚焦在強化公部門與特定私人部門單位的監管、強化稽核機制，並建立一套針對關鍵基礎設施提供者 (如不同的關鍵基礎設施營運商、國有事業或國營基金會) 的問責制度。這套修法提案的另一項重點，是要求監管單位資通安全署 (資安署) 在納管關鍵基礎設施提供者後，要審慎衡量其業務重要性及敏感度。也因此，定期稽核各服務提供者的資安維護計畫，會是資安署未來的重責之一。稽核內容將包含：各提供者資通訊系統的設計及規模、資安事件發生的頻率及嚴重程度，以及其他各項與資安有關的風險指標。

資安署也被要求草擬年度稽核計畫，並向上級機關呈報備考，最後交由行政院審核。此外，該計畫副本也將送交國家資通安全會報存查。安全會報組織的設立，同樣是為了強化各單位問責性，也因此安全會報小組中納入多名非政府 (比如學界人士或各界專家) 及地方政府代表，除了加強治理上的透明度也避免資安署行事過於專斷。最後，這次的修法提案中，也設下更嚴格的資安人員資格標準，並授權中央主管機關在重大資安事件發生時，可以對特定非政府的國有或國營機構進行調查。

學界專家就指出，明確定義利害關係者的法律責任，是這次修法的一大進展，這將有效強化各界遵循資安法規。法規中明確的權責設定，可以幫助企業了解自身義務、藉此強化問責機制，最終更主動地採納資安措施，進而提升普遍資安意識。舉例來說，修法提案實施後，企業將需要在一年 (甚至數個月) 內，完成有關人員的義務教育訓練課程。此外，修法提案將階段性實施這些規範，也就是說企業能在不影響營運的情況下，按部就班地達成法律遵循，最終讓產業界能普遍提升長期的資安韌性。

儘管2023年的修法提案獲得部分正面評價，但也有一些批評的聲音指出，法案過度側重稽核機制，可能影響機關之間的情資共享體系運行。儘管修法提案第九條裡，確實要求資安署建立一套資安情資共享系統，但整體立法方向仍以法遵稽核為重。這也令人憂心修法後的《資通安全管理法》是否能兼顧不同的資安需求，並有效應對多變的資安威脅。專家認為，修法方向應該參考國際上的最佳實踐，將情資共享視為立法核心，這樣才能真正地強化公私部門的整體韌性。

另一個引發爭議的點是，數發部最終決議不公開被視為有害國家資安的禁用產品清單。數發部認為，名單一旦公開將可能導致中國等敵對勢力掌握台灣的弱點。但批評聲音認為，這樣的做法並

不是小心謹慎，只不過是反映公務員體系「不做不錯」的心態。事實上，根據草案第11條，公部門應可向資安署查詢禁用產品資訊。批評者指出，一旦數發部拒絕公開清單，也就降低了產業界在相關事務上的可問責性。但數發部依然認為，公開清單可能導致產品偽冒情形發生，比如虛植產品製造地等，以此作為回應的立場。儘管如此，各方批評依然認為，提升管理透明度反而是一種加強外部監督的手段，這樣才能讓產業界重視安全措施並努力完成資安規範。

台灣行政院日前已在2024年10月4日通過上述修正草案，並即時送交該國立法院審查。立法院目前仍在就修法內容進行討論。一般來說，修正案若能經過二讀、三讀通過，就能付諸實施。但現況是，該國執政黨在國會中為能過半，法案通過須仰賴朝野合作。也因此，是否能取得跨黨派支持將成為修法成功的關鍵因素。

在ARTICLE 19的訪問中，一位不願具名的資深數位及資安政策專家指出，無論是《資通安全管理法》的推動、實施，或數發部、資安署這兩個相對年輕的政府部會營運，現實層面都面臨著一個同樣的問題：他們都缺乏實權和談判資本，要能真正落實資安準則恐怕難度極高。目前只有總統府辦公室和行政院真的有權力可以動員和協調各部會，要能完成「資安即國安」提出的願景，事實上需要更完整的規劃以及政治高層更大力道的支持。質言之，儘管台灣擁有充沛的技術專業實力，但執政機關仍在建立資安準則的初期階段，現階段仍一定程度仰賴民間社會的力量應對網路威脅。

我們確實可以看到台灣的政府機關付出許多努力，希望打造完善的資安治理基礎。但另一方面，外界也呼籲進一步擴大《資通安全管理法》的適用範圍，希望將目前僅適用於公家機關及特定的私人機構的法條擴及產業界。尤其是在網路威脅的快速演變下，台灣需要一套更完整的規範框架，來幫助適法範圍以外的產業界應對資安弱點。最後，儘管受資安署稽核對象需要在特定狀況下受政府調查，卻未有一套相對應的補救機制，這是另一個受到批評的立法瑕疵，這已經引發關於公平性及程序正義的疑慮。

台灣資安機構的策略與作法

就機構權責方面來說，修正案也進一步擴張數發部在台灣資安治理中的角色定位。2021年底《數位發展部組織法》獲三讀通過，數發部據此成立。該部成立後已經接手原本分屬5個不同政府部會的職責，包括：國家通訊傳播委員會、經濟部、國家發展委員會、交通部以及行政院資通安全處。此前，數位相關業務是由多個不同的政府部門管轄，這導致數位政策執行時往往衍生極高的協調成本。數發部的成立，成功將這些原本四散的職能整合在單一機關，讓台灣的數位政策能更有效率地集中執行，進一步降低原本官僚體系中的效率問題。

目前來說，行政院已將相關監管權限移交給數發部及資安署，可以說這次的組織重整，象徵著政府希望更有效地集中監督資安事務的企圖心。然而，這一切是否能達到預期的效果，依然要看數發部是否能處理掉最大的燙手山芋：在台灣的分權治理模式下，長久以來機關欠缺協調能力及實權的困境。

回過頭來，面對中國的專制模式，台灣的經驗依然相當具有啟發性。儘管面對來自中國的大量資安威脅及認知作戰，台灣依舊把捍衛言論自由擺在資安治理框架發展的第一位。首任數發部長唐鳳扮演關鍵角色，為機關確立了不少策略發展方向。在任期間，唐鳳的幾項重要計畫及政策風格，都可以體現出這種以言論自由為核心的治理方針。

唐鳳強調，政府與社交平台溝通時，應該就理念原則交換的大方向為主，避免直接介入平台的內容審查作業。儘管深知外界對於各平台演算法透明性存在疑慮（特別是Facebook的處理方式），唐鳳依然強調與平台營運商持續對話的重要性。這樣的做法就明顯和中國的專制模式有所不同，後者將箝制言論表達視為維持資訊基礎設施穩定的其中一環。相反地，台灣更重視營造一個開

放且民主的數位環境，認為對話重於強制性的管控。不若中國透過國家層面的審查機制以及對演算法的操弄，來嚴密管制線上言論，台灣的策略是尊重言論自由及資訊透明原則。

唐鳳在各類國際論壇上都不斷強調，處理爭議性內容時，絕對不能犧牲基本的言論自由，在國際間推廣這樣的概念。其中一例是「全球合作暨訓練架構 (Global Cooperation and Training Framework)」論壇，其主要目的是加強理念相近國家間彼此的夥伴關係，並擴大台灣的國際參與，同時應對嚴峻的全球挑戰。唐鳳也明確反對一些要求揭露使用者IP (internet protocol) 位址的立法提案。即便在2022年，當《數位中介服務法》草案引發民間激烈討論的時候，作為時任數發部長，唐鳳依然堅守明確機關權責界線，強調內容管制並不在數發部的權責範圍內。唐鳳認為數發部的定位就是推動數位創新及跨部門發展，並不是內容監管單位。

唐鳳在2023年8月接受《自由時報》專訪時的一段話體現了他對數位治理的想法：

> 我們也是花了非常多的時間，才讓大家瞭解抵禦境外的訊息攻勢，跟保障我們內部的言論自由、集會結社自由，這兩個是互相加強的，而不是我們抵禦外敵，就一定要讓境內的言論自由變少。

儘管有部分批評聲音認為，在處理境外認知作戰上，這樣的做法顯得過於消極。但無論如何，數發部確實在草創期間就為台灣帶來重要的治理先例。

循此，有別於中國以集權管治、數位主權為先，台灣確實有機會創造出一套不一樣的做法，一套以人權為本的資安治理典範。我們已經認識到，中國的專制模式的重要特色在於：犧牲多元利害關係者的參與以維穩為重、透過強制性資料在地化等方式實施國家管制、內容管制，以及基礎設施的監控。相反地，台灣主張的是一條截然不同的路徑：促進資安不僅不應該侵犯言論自由，甚至應該避免實施任何犧牲基本人權的政策——就算在嚴峻資訊戰的威脅下，都不該有所妥協。

然而，台灣的法規框架是否招架得住瞬息萬變的網路威脅，依舊值得我們關注。儘管台灣確實是對抗中國專制模式的正面案例，該國依然有一系列需要檢討的作法跟挑戰。舉例來說，立場強硬反中的民進黨就有過牴觸前述理念的言論。2017年該黨立法委員曾提議，將網路主勸概念納入台灣的《國家安全法》。這項提議最後被納入該法第四條的修訂條文，條文內容提出：「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。」

在黨內具影響力的民進黨立委葉宜津，當年也主張將數位主權概念納入《資安法》中，他強調：「現在國家主權不只是領土、邊界問題，還包含網路，因為網路可以對國安造成潛在的威脅。」他認為唯有將網路列為國家主權範疇，才能根本解決資安問題。儘管目前為止，網路主權尚未成功被納入資通安全管理法法律框架中，但這種想法在台灣持續演變的治理環境中卻從未消失。

資安規範上的透明性：以《資安法》草案修改為例

台灣《資通安全管理法》的其中一個看點在於，它證明了一國的資安規範能透過透明、全民參與的程序來制定，藉此同時兼顧安全考量及公民自由。這部《資安法》一路變革的過程，向我們證明向大眾諮詢的好處，這樣不僅可以避免資安治理在實施上過度擴張，也確保其執行時有足夠的可問責性。

台灣的「公共政策網路參與平台」是這個程序的關鍵要角，這個平台提供一座重要的橋樑，讓社會大眾可以參與在資安政策的制定中。這個平台規定在提出立法草案時，必須要有一定的民間公告期，讓民眾能透過有效的對話機制，積極地參與在政策制定的過程中。其中，資通安全法小組負責主持討論，確保民眾和決策者間能持續對話。

這個做法也和台灣更廣泛的《開放政府國家行動方案》一致，該方案目前已經公共參與機制在不同的治理領域中制度化。台灣的開放政府及開放議會計畫，為我們帶來一系列藉由多元參與對話來促進透明性及包容性的施政典範，這也都強化了立法過程中的可問責性。台灣在民間參與上的這些作法，都充分展現出該國對於重大治理議題保持開放、多元參與及堅守民主原則的決心。

有一個頗具代表性的例子，可以說明公民政策網路參與平台是如何促進民眾參與決策過程。在當年《資通安全管理法》提出初版草案時，對於條文中提及非政府機構（如私人企業）應受行政檢查，曾引發大眾議論。有幾個重要的問題在平台上被提出，包含：

- 行政檢查是否只應在重大資安事件／重大缺失發生時啟動？這樣是否有錯失早期警訊的風險？
- 相反地，如果沒有相關限制，是否會主管機關濫權的疑慮？
- 是否有其它替代作法或保護措施，能讓主管機關兼顧主動監督與可問責性？

大眾就此提出相當多實際疑慮，質疑主管機關在領域專家不介入的狀況下，是否有足夠的資源或專業能力，來完成有效的行政檢查。就有人提案，或許可以讓法警、資安專家或法律專業人士參與在檢查中，而在這些人士無法陪同出席時，也可以探索其他的替代方案。

這樣的參與過程成功讓大眾提出幾項具體建議，包括：

- 明確規範受監管的產業類別。
- 採用更細緻的分類或商業登記標準來判定。
- 公開行政檢查過程及結論的各項細節，包括通過／不通過的結果、負責機關名銜及任何參與檢查的專業機構。
- 建立明確檢查程序規則，以確保檢查透明及濫權 。

而針對這一系列的討論，決策者也向平台提出一些說明和調整。舉例來說，他們修訂了受監管對象的範圍，優先納管關鍵基礎設施提供者及特定適用資安分級責任制度的非政府組織。中央監管單位也將行政檢查的細節，諸如頻率、內容及施作方法，留待後續子法再行規範。

民眾也進一步強調，檢查機制應該避免商業機密受影響，也應避免干擾商業活動。針對檢查內容的一些具體的建議還包括：驗證資安機制照設計運行、確保資安憑證有效期限、確認與資安供應商契約符合標準，以及監督內部資安規範及標準化作業程序的落實。這種參與式的作法反映的是，儘管面對數位威脅，台灣政府確實有理由採取以安全穩定為主的數位發展方向，但該國在強化其資安準則之餘，依然致力提升透明度並融入多元利害關係者的參與。

與資安社群互動帶來的創新

整體來說，台灣已經把資安整合進更廣泛的經濟及產業政策中，並將其視為發展戰略產業的重要支柱。這種將安全與創新結合的作法，是為了在提升競爭力的同時消弭風險，特別像是智慧製造或是5G網路這些高風險領域，開發中留下的一些弱點都可能帶來廣大影響。此外，藉由一個全國性的資安管理平台整合，台灣現行的多層次資安防禦系統，有能力視部會職責協調各單位的工作歸屬，並強調公私部門間的協作。

在發展監管制度時，台灣選擇體現民主原則，將公共諮詢納入立法過程，這樣的透明度確實相當亮眼。然而，要能在處理急迫資安威脅的同時兼顧開放性，一直都是一個棘手的挑戰。儘管台灣已經在處理資安挑戰上有具體成就，該國是否能長期維持韌性，依然有賴政府與民間更有效的協調、強化部會執行能力，以及確保國家能明快處理不斷湧現的各種安全風險。

放眼民間，台灣現在也有一些草根計畫在發展，比如說零時政府 (g0v.tw)、台灣駭客年會 (Hacks in Taiwan Conference, HITCON) 以及各類的黑客松，這都進一步豐富台灣目前的資安發展生態。以HITCON為例，從2005年開辦以來，已經成為台灣的資安盛事，不僅提升全民資安意識，也讓資安專才有彼此切磋進步的機會。該活動是由台灣駭客協會主辦，內容涵蓋研討會、工作坊及各類應對全球資安挑戰的培訓課程。他們組織的一些計畫或活動，比如ZeroDay弱點回報平台、CTF駭客競賽，都展現出HITCON提升國家資安實力以及作育資安專才的企圖心。此外，台灣駭客協會也積極開辦諸如物聯網黑客松等大型活動，在促進產官學三界合作上，扮演著重要角色。這類大型活動不僅希望將創新帶入資安產業界，也能吸納更多新興人才。

其它一些像是零時政府這樣的案例，則是根植在開源開發的原則上，希望推廣資訊透明性及公民參與。透過結合線上協作及線下的黑客松等活動，零時政府讓公民能積極參與在資安專案中、學習資安技術，並一同應對資安挑戰。而台灣政府也吸納了這樣的公民參與模式，2019年的總統盃黑客松就是很好的例子。這樣的平台可以促進了公私部門間的協作，讓雙方藉由開放資料及技術創新改善公共服務的品質。幾個向度不同的政府部會，包括數發部、衛生福利部，都是活動協辦者。這樣多元的單位組成，讓跨部門甚至跨學科的合作成為可能。

其它一些民間社會團體，比如「麥擱騙　MyGoPen」、「真的假的　Cofacts」的出現，也都在對抗虛假訊息威脅的作戰中功不可沒。這些組織並非經由正式法規成立。卻積極倡導言論自由，並藉由事實查核、媒體素養教育以及公眾參與等業務來為民賦權。其中，「麥擱騙」主要專注在監測網路內容，辨別並反制虛假資訊，尤其是在像是選舉這樣的敏感時期。該組織會負責核實各種說法，同時發布正確資訊，藉此來揭穿可能影響公眾意見的虛假敘事。「真的假的」的作法類似，他們透過一個AI驅動的平台，讓使用者回報網路上看到的可疑說法。這個平台會向使用者提供經驗證的回覆以及一些教育資源，讓民眾有能力持續辨別可靠與虛假資訊，進而提升全民資訊素養。這兩個組織都讓民眾實際參與在面對資訊威脅的作戰中，藉此在資安議題上促進草根參與。

此外，民間社會也在處理公眾疑慮中扮演重要角色，像是「電子國民身分證 (eID)」的換發計畫就是一個例子。2018年12月的時候，國家發展委員會宣布將在2020年中全面換發電子國民身分證。新式身分證在設計上除了原有身分證的功能外，也新增自然人憑證功能，在上面嵌入晶片來安全地儲存數位身份資訊。

2019年9月，台灣人權促進會及民間司法改革基金會等民間組織，都召開一系列的記者會，對eID可能帶來的隱私權侵犯問題提出警告。他們批評整個換發推動過程缺乏透明度，特別是有關資料管理作法以及資訊涵蓋範圍等，都未能充分公開相關資訊。

2020年5月，台灣人權促進會發起連署，反對強制換發eID，並主張應保留現行傳統身分證作為民眾可用的替代選項。這份連署獲得超過200名專家學者的支持，要求在引入任何新的數位身份系統前，都應該先立法保障完善的隱私權機制，強調政府保護個人資料的重要性。各類公民社會組織也群起呼籲，應設立一獨立的資料保護機構來監督eID的建置過程。他們強調若未有適當監管措施，這套整合醫療、教育及商務資訊的資料庫，可能帶來一系列的重大風險。

儘管eID計畫已擬定換發時程，這些來自公民社會組織，有關隱私權及法律框架的疑慮，最終使得計畫數次延宕，並在2021年宣布暫停。以上這些公民組織的行動都能體現民間社會如何透過包容性、教育導向及政府體制外的作法，來對抗網路及資訊威脅。他們的努力都在應對台灣民主所面臨的複雜挑戰時，兼顧了言論自由的強化。

台灣的資安治理典範展示的是民主政體在治理上是如何兼顧國家安全與公民自由。透過施政透明及平台參與，台灣成功避免採行可能傷及基本自由的政策。儘管近期納入數位主權概念的立法提案顯示出，台灣也出現以維穩為主的意見聲浪，台灣此刻亦然決心在面對威脅是捍衛民主價值。台灣的經驗不僅向我們證明了，保衛國家安全並不一定需要專制模式的數位管控措施，同時也向全球各地面臨相同資安挑戰的民主政體，分享寶貴的經驗談。

如何對抗中國在網路準則上的主導權

對國際社會的建議：

1. 支持台灣

鼓勵台灣參與國家資安及數位治理討論，藉此強化國際反數位威權主義同盟。

2. 支持多元利害關係者參與

鼓勵各國政府將公民、民間社會及企業利害關係者，納入政策制定過程中，並規範法案起草時進行公眾諮詢。此外，也要確保相關的台灣利害關係者，能確實參與在國際論壇中，藉此創造一股能擴大民主聲音的包容性機制。

3. 讓快速反制成為可能

國際社群應動員自身區域網路，來蒐集專制數位工具及相關政策的事證，並在避免吹哨者遭受報復的前提下，與民間社會一同揭露這些問題。此外，也應該以台灣為核心，反制日益高張之數位專制主義的全球聯盟。

對台灣政府的建議：

4. 將數位人權置於資安政策核心

台灣應持續推動政策透明度、資料保護及公開問責機制。也要以法律明確保證隱私權、言論自由以及資訊近用權，藉此作為發展資安治理準則的基礎。

5. 帶領全球推動人權為本的資安治理作法

台灣政府應以其成功的民主發展作為資本，向外推廣重視人權的數位治理作法。同時也應結合數位外交，以培力計畫等方式，協助印太國家發展完善且具有民主價值的資安政策。

對台灣公民社會與私部門的建議：

6. 協助國際社會觀測中國向外擴張的數位影響力

台灣民間社會可以和區域夥伴一同合作，記錄並揭露中國數位絲路的一系列計畫，是如何對人權帶來負面衝擊。尤其是台灣民間社會應發揮其對中國資訊威脅及技巧的知識，來幫助印太地區公民社會觀測中國影響力下的新興技術與政策。

7. 積極參與國際準則發展

台灣的私部門及更廣泛的民間科技社群，應把握參與國際論壇 (特別是與網路治理及技術標準制定有關者) 的機會，發揮自身知識及影響力。

附錄一：對人權造成影響的中國法規

2011《互聯網信息服務管理辦法》*

第四條	要求對商業性網路資訊服務實施許可制度，並對非商業性的網路資訊服務實施備案制度。
第五條	要求如「網路、出版、教育」等網路資訊供應商，須經國家審查、許可方可營運，讓這些服務提供者可能收到國家的專斷限制。
第十四條	特別要求「新聞、出版及電子公告」服務供應商，需記錄發布訊息內容、時間、IP位址或使用網域名稱；而網路服務供應商也同樣須記載使用者登入時間、IP或使用網域名稱。這些供應商被要求至少應留存相關紀錄60天，以供主管機關使用。
第十五條	規範網際網路資訊供應商不可任意「製作、再製、發佈或傳播」包含謠言或破壞社會秩序等九大類訊息，這牴觸了國際法中所允許的言論管制範圍。

*該法早於2017年的《網絡安全法》，但已經可以在其中看到後續不同法律、政策及執法機關所用框架的影子。該法可能也被視為後續不同增修法條、條款的法源依據。

2017《中華人民共和國網絡安全法》

第十二條	規定任何網路使用者不應從事危害國家榮譽及利益、顛覆社會主義制度、宣揚種族仇恨及歧視 (這部分的條文內容經常用來起訴捍衛自身權利的少數民族或宗教團體)、製造及散播虛假訊息等行為。與該法中其它條款類似，這項條文著重的並不是實質的網路安全，而更著重在控制經由網路擴散的資訊類型。這類規範不應該被放在任何資安相關法律的適用範疇內，鑑於其可能對言論自由造成的侵害。
第二十一條	要求網路營運商採取措施，監控並記錄網路流量資料，更要求至少保存網路日誌資料 (network logs) 六個月以上。
第二十四條	規定網路營運商必須要求使用者提供實名身份，特別是出版及即時訊息服務領域，這對線上匿名性造成極大衝擊。這項實名制的要求應同時與2017年工信部《關於清理規範互聯網網絡接入服務市場的通知》一同審視，該項通知將任何未經工信部核可的VPN網路視為非法。這不僅衝擊越過審查機制的翻牆工具，也對保障線上隱私構成重大影響。
第二十八條	規定網路營運商必須向大眾及國家安全實體，提供模糊定義的「技術支援」。這可以被解讀為強迫配合國家的監控行動。
第三十七條	提出資料在地化要求，規定CII營運商有義務將「重要資料」儲存在中國大陸境內。這項規範迫使蘋果等科技公司，將使用者資料儲存在中國境內，並涉及將解密金鑰在地化的問題。

第四十六條	禁止個人或組織建立「傳授犯罪方法、製造或銷售管制物品」。或「發佈與違法行為相關資訊」的「網站或通訊群組」。結合該法第二十四條以及工信部的相關規定，這項條文對於分享翻牆及匿名化工具資訊施加更大的限制，同時也讓網站或即時通訊軟體無法分享中國迫害人權的資訊，以及和抗議事件或起訴少數群體有關的報導。
第四十八條	要求電子資訊發佈服務供應商及應用程式服務供應商，審查定義模糊的所謂「法律或主管機關規範禁止資訊之發佈與傳送」。這迫使服務供應商實施主動的安全管理措施、移除特定資訊、保存紀錄，並向當局回報違規者。這項條文不僅授權政府審查，也要求私部門業者預先審查被官方禁止的內容。第四十九條接續強調，網路營運商應與資安及資訊等相關政府部門配合，履行其法定義務。
第五十條	指示資安及資訊部門實施安全性監督與管理，並在發現「禁止」資訊時，命令網路營運商中止其傳輸、移除內容並保存紀錄。這樣的法定義務，也適用於中國境外資訊，當局將通報相關單位採取技術手段封鎖該內容。結合第四十九條及第五十條，兩者可說是往後以資安名義行審查之實的藍本。
第五十八條	針對「保護國家安全及公共秩序」的網路干預，提供法律依據。這可能導致不同程度的網路中斷或頻寬限制，舉例來說，過去在印度、印尼、緬甸及巴基斯坦等國，就曾有過蓄意降低網速的紀錄。

2017《中華人民共和國國家情報法》

第七條	規定「所有組織及公民均應支持、協助並配合國家情報工作」，這項法定義務對境外科技公司一樣適用。
第十一條	規定從事國家情報工作者應在發現威脅時，「蒐集並處理與外國機構、組織或個人有關情資」。然而此處對威脅定義極為模糊。
第十二條	規定國家情報單位可與個人或組織「建立合作關係」，並「雇用其從事相關情報工作」。
第十三條	規定情報工作單位可以強制「相關機關、組織及公民」提供支持、協助及合作。
第十五條	規定情報工作單位可以採取科技調查措施。

2021《中華人民共和國數據安全法》

第二條	規定如果境外處理資料被認為對國家安全、公眾利益或損及「中國人民及組織合法權益」者，中國有權追究其法律責任。
第二十六條	規定若外國監管單位試圖限制中國在全球數位領域的企圖心，中國可採取相對應的報復行為。因該條未具體定義前述行為，僅指出如果任何國家或地區「在與數據和數據開發利用技術等有關的投資、貿易等方面對中華人民共和國採取歧視性的禁止、限制或者其他類似措施的」，中國即可採取報復措施。

2021《中華人民共和國個人信息保護法》

第三十五條	規定在部分定義模糊或鬆散的情況下(比如通知可能干擾官方業務進行),官方可在不知會當事人的狀況下收集個人資訊。
第三十六條	規定個人身份識別設備(諸如臉部辨識攝影機),能嚴格在「保護公共安全」的前提下使用。然而,何謂公共安全依然交由相關單位定義,這也造成一些機制濫用的漏洞叢生,比如說中國對曾向維吾爾族、藏族族人強行收集生物識別資料,另外中國也在國內儲存個人資訊。
第四十三條	規定任何國家或地區,若在個人資訊層面對中國採取定義模糊的「歧視性禁止、限制或其他類似措施的」,政府有權採取報復性措施。這項條文可以被解讀為,若合作夥伴對中國科技公司的個人資料使用採取限制性措施,中國將以反制措施威脅。

article19.org