台灣亞太安全研究協會

Taiwan Asia-Pacific Security Research Association (TAPSRA)

研究報告 TAPSRA-2026-04

# 台灣韌性與非軍事安全評估

能源、通信、供應鏈、網路安全與全社會防衛的政策框架



| | |
|---|---|
| **發佈月份** | 2026 年 8 月 |
| **資料基準日** | 2026 年 8 月 11 日 |
| **關鍵詞** | 社會韌性 / 基礎設施 / 能源安全 / 網路安全 / 供應鏈 |





研究屬性：戰略與政策分析｜公開來源研究（OSINT）｜非機密

# 執行摘要與核心判斷

*本報告以公開來源為基礎，對可查證事實與分析判斷作明確區分。下列“核心判斷”屬於研究性研判，不應理解為對未來事件的確定性預測。*

| | |
|---|---|
| **J1** | 現代安全競爭越來越針對“系統是否能持續運作”，因此社會韌性不能被視為軍事實力之外的附屬議題，而是危機穩定的重要組成。 |
| **J2** | 台灣 2026 年的公開演練把關鍵基礎設施、軍民聯合應變與通信條件變化納入城鎮韌性演習，顯示韌性建設正在從政策口號轉向跨部門驗證。 |
| **J3** | 韌性建設應優先減少單點故障與恢復時間，而不是追求所有系統在任何情景下“完全不受影響”。冗余、替代路徑、庫存和資訊透明度比單一高規格設施更重要。 |
| **J4** | 能源、海纜、雲服務、港口物流、金融支付與公共通信高度互相依賴，必須以“系統之系統”的方式評估級聯風險。 |
| **J5** | 社會信任是韌性的放大器。若政府資訊不一致、謠言治理過度政治化或民眾不知道應如何行動，再高的物理冗余也可能被認知混亂削弱。 |

# 究範圍、方法與限制

## 研究範圍

本報告以非軍事安全和社會韌性為核心，不對任何具體關鍵基礎設施的精確位置、薄弱點或防護缺口作分析。重點是制度層面的冗余、恢復、跨部門協調、公共溝通與供應鏈連續性。

## 研究方法

- 功能鏈分析：能源—通信—交通—金融—政府服務之間的依賴關係。
- 韌性指標法：關注冗余、恢復時間、替代能力、人員準備與資訊透明度。
- 公開演練觀察：分析 2026 年城鎮韌性演習所體現的政策優先項。
- 比較政策分析：參考日本等區域國家對網路、供應鏈與產業安全的制度化趨勢。

## 限制與不確定性

關鍵基礎設施的真實冗余和恢復能力通常涉及非公開資訊，公開演練也可能更側重展示而非完整驗證。本文因此以治理框架為主，不對具體系統的抗打擊能力作推斷。

# 目錄與閱讀提示

## 章節結構

| 章節 | 主要議題 |
| --- | --- |
| 一、韌性為何成為台海安全的核心變量 | 1.1 從“阻止攻擊”到“保證持續運作”；1.2 韌性具有威懾效應；1.3 “全社會”不等於“全民軍事化” |
| 二、能源與電力：韌性是組合問題 | 2.1 供應多元化與庫存；2.2 分布式與集中式系統的平衡；2.3 恢復時間比“零中斷”更現實 |
| 三、通信、海纜與網路安全 | 3.1 海底電纜是重要但非唯一鏈路；3.2 網路安全與資訊連續性；3.3 公共通信中的可信資訊 |
| 四、供應鏈、港口與經濟連續性 | 4.1 關鍵不是所有庫存都越多越好；4.2 企業連續性是國家韌性的底層單元；4.3 港口與物流需要“網路視角” |
| 五、社會信任、地方治理與演練 | 5.1 演練要從“展示流程”轉向“發現問題”；5.2 地方政府是恢復能力的關鍵節點；5.3 社會信任需要可驗證的透明度 |

**閱讀提示**

報告中的“高／中／低”“較高／中等／較低”等屬於定性風險判斷，用於比較不同風險因素，不是統計學機率。事實性內容盡量對應公開來源，分析性判斷由本報告負責。

# 一、性何成台海安全的核心變量

## 1.1 從“阻止攻擊”到“保證持續運作”

傳統安全政策偏重阻止對手採取行動，但現代混合威脅、網路攻擊、自然災害與供應鏈衝擊都表明，完全阻止所有擾動並不現實。韌性的目標是讓系統即使受到衝擊，也能維持最低核心功能、快速恢復，並避免局部故障擴散為社會性危機。

## 1.2 性具有威效應

如果對手相信低成本壓力無法迅速造成政治或社會癱瘓，脅迫工具的預期收益會下降。因此，韌性既是民生政策，也是威懾的一部分。不過韌性威懾的可信度來自長期制度和社會準備，而不是一次演習或單一設備。

### 1.3 “全社會”不等於“全民軍事化”

全社會防衛韌性可以包含急救、災害應變、通信備援、地方治理、企業連續性和資訊識讀等多種非軍事能力。有效設計應避免把所有民間活動軍事化，否則會降低公眾參與意願，也可能模糊人道與民用機構的角色。

## 二、能源與電力：韌性是組合問題

### 2.1 供應多元化與庫存

能源安全不能只看某一種能源佔比，而應同時觀察進口來源、儲備天數、發電結構、輸配電恢復能力和關鍵用戶優先級。對島嶼經濟體而言，港口、燃料接收和電網恢復是相互依賴的鏈條。

### 2.2 分布式與集中式系統的平衡

集中式系統效率高、管理成熟，但局部故障可能影響範圍更大；分布式電源和儲能能夠提升局部韌性，卻需要成本、維護和調度制度支持。政策目標應是建立可切換的組合，而不是簡單認為分布式必然優於集中式。

### 2.3 恢復時間比“零中斷”更現實

任何複雜系統都可能中斷。韌性指標應包括關鍵設施的備援電力持續時間、維修資源調度、黑啓動能力和公眾用電優先次序。公開透明的恢復目標能夠提高社會預期管理。

> **韌性原則**
>
> 韌性不是“讓所有系統永不失效”，而是減少單點故障、限制級聯、保住核心功能，並把恢復時間壓縮到社會可承受範圍內。

## 三、通信、海纜與網路安全

### 3.1 海底電纜是重要但非唯一鏈路

台灣對國際通信高度依賴海底電纜，但衛星、微波、不同登陸點與雲服務架構可以構成多層備援。政策重點應是多路徑、快速修復、供應商多元和跨境協調，而不是把單一技術視為“終極備份”。

### 3.2 網路安全與資訊連續性

網路攻擊的戰略目標可能不是長期摧毀系統，而是製造短時間資訊混亂、降低決策者對資料的信任。零信任架構、離線備份、事件響應和跨機構日誌共享等治理機制，比單純採購安全產品更重要。

### 3.3 公共通信中的可信資訊

危機時民眾需要知道發生了甚麼、哪些服務可用、哪些資訊尚未確認。政府若過度承諾或頻繁修正，將損害信任。應建立“已確認—正在查證—不確定”的分層資訊發佈規則，並在平時就讓公眾熟悉。

## 四、供應鏈、港口與經濟連續性

### 4.1 關鍵不是所有庫存都越多越好

戰略庫存需要考慮保存成本、輪換、替代材料和供應商切換能力。對醫療、能源、食品、通信設備和工業耗材，應設置不同的最低服務目標。

### 4.2 企業連續性是國家性的底層單元

政府無法替代所有企業運營。更有效的方式是建立關鍵行業連續性標準，要求大型企業進行備援供應商、異地資料、現金流與員工替代安排，並透過審計或演練驗證。

### 4.3 港口與物流需要“網路視角”

港口受阻不一定意味著所有物流停止，關鍵在於其他港口、機場、陸路節點、倉儲與清關係統能否快速重新分配。韌性政策應測試切換速度和跨部門授權，而不是只關注單點防護。

## 五、社會信任、地方治理與演練

### 5.1 演練要從“展示流程”轉向“發現問題”

2026 年台灣城鎮韌性演習包含軍民聯合應變、關鍵基礎設施防護和全民防衛等主軸，並測試移動網路降速條件。此類演練的真正價值在於暴露跨部門資料不一致、權限不清與資源瓶頸。若演練只追求“順利完成”，反而會失去學習價值。

### 5.2 地方政府是恢復能力的關鍵節點

危機初期，地方政府往往直接處理避難、醫療、交通、物資和公共資訊。中央政策如果沒有與地方資源、民間組織和企業責任銜接，很難形成真正的全社會韌性。

### 5.3 社會信任需要可驗證的透明度

政府可以公開演練後的改進項、目標完成度與下一輪測試內容，而無需披露敏感安全細節。可驗證的透明度能夠減少“宣傳化”印象，也有助於企業和公眾理解自身責任。

### 韌性能力評估框架

| 系統 | 核心目標 | 優先指標 | 政策重點 |
|---|---|---|---|
| 能源 | 維持關鍵負載並快速恢復 | 備用時長、切換時間、維修資源 | 多元供應、儲能、恢復演練 |
| 通信 | 保持政府與公眾基本聯絡 | 多路徑、恢復時間、終端可用性 | 海纜+衛星+地面備援 |
| 網路 | 保持資料可信與關鍵服務 | 檢測時間、隔離時間、備份可恢復性 | 零信任、離線備份、事件響應 |
| 物流 | 保障關鍵物資流動 | 替代節點、庫存、清關速度 | 港口網路、供應商多元 |
| 社會治理 | 維持秩序與可信資訊 | 資訊一致性、地方協調、公眾參與 | 演練、風險溝通、志願體系 |

### “系統之系統”級聯風險

| 起始擾動 | 一級影響 | 可能的二級影響 | 主要緩衝器 |
|---|---|---|---|
| 電力中斷 | 通信/交通受限 | 支付、醫療、政府服務延遲 | 備用電源、分區恢復 |
| 通信異常 | 資訊延遲 | 謠言、調度困難、市場恐慌 | 多路徑通信、統一資訊發佈 |
| 港口受阻 | 物資延遲 | 工業與能源庫存下降 | 替代港口、庫存、空運 |
| 網路攻擊 | 資料可信度下降 | 服務停擺、決策延遲 | 離線備份、人工流程、分段隔離 |

## 結論與政策啓示

台灣韌性建設的政策重心應從“擁有多少備用設備”轉向“系統能否切換、恢復和協同”。能源、通信、網路、物流和政府服務之間存在強依賴，任何一個節點都可能透過級聯效應放大。2026 年的公開演練顯示跨部門韌性已成為安全政策的重要方向。下一階段更重要的是建立可衡量的恢復目標、企業連續性標準、地方政府協調機制和可信風險溝通，使社會準備成為長期制度，而不是危機時的臨時動員。

### 可操作的政策啓示（戰略層面）

- 建立跨部門統一風險圖景：軍事、外交、海事、經濟、通信和地方治理部門使用一致的事件分級與事實查核流程。
- 把“恢復能力”與“威懾能力”同時納入預算評估，避免只關注新增能力而忽視維護、備援、人員與制度成本。
- 強化危機溝通與公開資訊規範：區分已確認事實、分析判斷與尚未查證資訊，降低誤判和社會恐慌。

- 對高衝擊、低機率情景開展跨部門演練，同時為灰色地帶和中間狀態準備比例適當的政策選項。
- 保持地區合作的多層次結構：軍事安全之外，擴大海事安全、災害救援、供應鏈、網路與關鍵基礎設施韌性合作。

## 參考資料

以下資料均為公開來源；網頁資料的訪問與事件截點以 2026 年 8 月 11 日為準。引用僅用於事實查核與觀點對照，不表示本報告認同來源中的全部立場。

**[1]** 台灣地區總統府：Whole-of-Society Defense Resilience Committee 公開資料，2026。

**[2]** 台灣地區國防主管機關軍聞社：《漢光結合城鎮韌性演習 提升政府整體應處效能》，2026-08-06。

**[3]** 台灣地區國防主管機關：《2025 Quadrennial Defense Review》，2025。

**[4]** Japan Ministry of Defense: Defense of Japan 2026（網路安全、聯合運用與國防產業生產技術基礎相關章節）。

**[5]** IISS: Shangri-La Dialogue 2025 Full Report（危機管理、海洋安全與防務創新討論）。