測試與評估表

Tor 瀏覽器

1. 工具概述

姓名:	Tor 瀏覽器
類別:	瀏覽器
目的:	Tor 瀏覽器是一款免費的、注重隱私的網路瀏覽器，它使用 Tor 網路加密流量並保護用戶的線上匿名性。
日期	2025年4月2日
文件翻譯日期:	2025年9月7日
地位:	已部署 ☑ 營運中 - 積極運作/維護 ☐ 測試中 - 目前正在評估或試行 ☐ 不活躍/棄用 - 不再維護或運行
部署架構:	☐ 獨立軟體 - 完全在本地運行（例如，在電腦上運行並且不依賴外部伺服器） ☐ 具有獨立伺服器和用戶端元件的本機主機服務 - 自行執行後端/前端（例如，後端可以在本機網路上，也可以在雲端自行託管） ☑ 由第三方託管的本機用戶端服務 -您在設備上安裝客戶端，但它連接並依賴遠端伺服器（例如，Signal：安裝應用程式（客戶端），但 Signal 的伺服器處理訊息中繼等） **Tor** 瀏覽器是一款在電腦上本地運行但連接到 **Tor** 網路來瀏覽網頁的軟體。 ☐ 由第三方託管但也可以自行託管的服務
版本:	14.5a6

2. 安裝和設定

作業系統相容性	Windows、Linux、macOS、Android
安裝手冊:	Yes https://tb-manual.torproject.org/about/

安裝步驟:	1. 打開搜尋引擎並輸入**Tor**瀏覽器 或者“下載 **Tor** 瀏覽器”在搜尋欄中。 2. 點擊官方“下載 **Tor** 瀏覽器”連結來自**Tor** 專案網站。 3. 在下載頁面上，選擇適合您的作業系統(Windows、macOS、Linux 或 Android)的版本。 4. 點選下載按鈕並等待檔案下載完成。 5. 下載完成後，啟動安裝程序，選擇您的首選語言，然後選擇安裝的目標資料夾。 6. 請依照螢幕上的指示完成安裝程序。 https://gitlab.torproject.org/tpo/applications/tor-browser
提及是否需要命令列設定或特殊配置	Tor 瀏覽器不需要命令列設置，因為它帶有圖形安裝程式(命令列選項對於腳本、自動化或高級配置很有用，但不是必需的)。
常見安裝問題及修復:	1. 故障排除指南(由 Tor 提供)：https://tb-manual.torproject.org/troubleshooting/
使用者文件:	Yes
所需的技術知識	中級(普通用戶可以輕鬆安裝瀏覽器並開始使用它，但需要更多關於使用什麼配置或安全功能的技術知識)。

3. 測試與評估

類別	細節	分數
操作功能:	功能 ● Tor 瀏覽器履行了其預期功能，即妥善避免監視並確保線上隱私。它透過 Tor 網路中一系列由志工運作的中繼網路，來路由網路流量。每個中繼只知道其直接的前任和後繼，這使得追蹤到用戶的完整路徑變得極其困難——這種技術被稱為洋蔥路由。 ● Tor 通常運作不會中斷功能和錯誤。由於成千上萬的人為瀏覽器的運作和維護做出貢獻，因此大規模問題並不常見。 ○ 在測試期間，Tor 瀏覽器下載非常容易，網頁瀏覽也很直觀，無跡像或錯誤。 網路依賴: ● 沒有離線功能(這不是一個缺點，因為它是一個網路瀏覽工具)。 ● Tor 透過隱藏使用者的 IP 位址並透過志工管理的中繼網路引導，實現匿名通訊。	

	● 2G/3G 網路：不建議使用，因為速度慢、延遲高，這會使瀏覽和使用 Tor 的速度明顯變慢且可靠性降低。 在地化和語言支持 ● 語言：Tor 已發布並翻譯了多種語言版本。目前已有 32 種語言版本，其中 90% 至 100% 已翻譯。 ○ 中文（簡體與繁體）、泰語、越南語、韓語、日語 移動無障礙 ● 針對行動裝置可訪問性進行了最佳化，主要針對 Android 系統	
非技術用戶的可用性	易於安裝和部署 ● 安裝和設定有多容易？ ○ 對於按照上述步驟和提供的文件進行操作的使用者來說，基礎安裝相當簡單。對於設定 Tor 節點或其他隱私工具的使用者來說，安裝/設定會更加複雜。 ● 安裝指南、手冊和常見問題是否維護良好？ ○ 安裝指南、手冊和常見問題解答維護良好且相當廣泛，並且上面提供了手冊的連結。 ● 計算安裝過程的時間 ○ 30秒 使用者入門體驗 ● 它是否為首次用戶提供文件？ ○ Tor 維護一個相當大的文件庫，其中包括社群指南和技術說明，特別是針對初次使用者。 https://tb-manual.torproject.org/running-tor-browser/ 所需的技術經驗水平 ● 非技術用戶可以輕鬆使用該工具嗎？ ○ Tor 的設計旨在讓所有用戶都能訪問，無論其技術知識如何；然而，非技術用戶可能會發現導航和利用完整的匿名和安全功能更具挑戰性。 ■ 預設：Tor 嘗試不使用網橋進行連線。 ■ 在中國等審查嚴格的國家，直接聯繫往往已阻止——不僅在技術上，而且在政治上也存在風險。即使你的流量內容是加密和隱藏的，你存	

	取 Tor 網路本身就可能引起懷疑。當局可能不知道你在做什麼，但他們知道你在做什麼某物值得隱藏－僅此一點就會引起不必要的關注。 ■ 這可能會讓非技術用戶覺得 Tor 不安全，因為他們不了解橋接和可插拔傳輸協定（例如 obfs4）。此外，某些網橋或傳輸協定的配置並不直觀，而且文件也不夠完善。 ● 界面直覺嗎？ ○ Tor 瀏覽器的介面非常直觀，適合進階使用者使用。對於非技術用戶來說，隱私設定和安全功能一開始可能會有點混亂，但搜尋引擎卻非常直覺。	
安全和隱私強度	加密標準 ● 使用什麼安全協定？ ○ 多層加密（洋蔥路由）：每個資料包在隨機傳送到三個 Tor 節點之前都會經過三次加密。為了防止任何一個節點同時知道發送者和目的地，每個中繼都會移除一層加密，就像剝洋蔥一樣。 ○ 安全協定：TLS 1.2+ → 保護用戶端入口節點通訊、AES-256 → 加密中繼流量、RSA-4096 → 安全金鑰交換與中繼認證、SHA-3 → 資料完整性驗證、Diffie-Hellman → 完美前向保密（唯一會話金鑰）。 審查彈性 ● 抵制審查：Tor 內建了橋樑，幫助使用者繞過審查並在被封鎖的地區訪問 Tor 網路（更多資訊請參閱「為什麼這對專制環境中的公民社會有用？」部分）。 漏洞：抵禦已知威脅的能力 ● 存在一些潛在的漏洞。它們已通過 Cure53（網路安全公司）的安全評估，並於 2024 年 1 月發布（他們還提供了建議）。 ○ https://www.torproject.org/about/reports/ ■ 主要風險包括潛在的拒絕服務 (DoS) 攻擊、聊天服務中的用戶冒充以及 Android 應用程式中可能被未安裝修補程式的手機上的惡意軟體利用的漏洞。這些問題不會破	

	壞核心匿名網路本身，但凸顯了保持 Tor 工具更新並在安全設備上使用它們的重要性。 ■ 底線：對於日常用戶來說，Tor 仍然是最好的匿名工具之一——但就像任何技術一樣，它並非無敵。保持更新和謹慎使用至關重要。 與已知標準的比較 ● Tor 瀏覽器是最好的匿名軟體之一。領先的數位版權組織電子前沿基金會 (EFF) 經常將 Tor 推薦為保護隱私和抵制監控的關鍵工具。 資料最小化 ● 根據他們最近的審計，他們只收集必要的資料，並且這些資料被安全地儲存。 隱私權政策的可近性和清晰度 ● Tor 瀏覽器會阻止他人知道您造訪的網站。某些實體，例如您的網路服務供應商 (ISP)，或許能夠看到您正在使用 Tor，但他們無法得知您的存取目的。」（Tor 瀏覽器隱私權政策）	
維護/永續性	社群支持 ● 這裡有一個大型且活躍的論壇，其中有關於反饋、支持、新聞等的帖子，可以輕鬆獲得幫助和提出問題。 ● 然而，志工運作的中繼的數量和地理分佈對 Tor 的效率有顯著影響。這凸顯了本地中繼參與對效能提升的必要性。 ○ 在台灣，運行中繼的志工數量較少，這可能會使 Tor 瀏覽器變慢。 開發活躍狀態 ● 頻繁更新～每個月都有更新 ● 狀態頁面顯示 TorProject 各個站點的目前狀態，包括事件歷史記錄 ■ https://status.torproject.org/ 資金和贊助 ● 已揭露融資約 700 萬美元 ● 約 28.5% 的收入來自個人捐款者，反映出基層支持基礎的不斷擴大。 ● 贊助： ○ Open Technology Fund ○ Sida (Swedish International Development Cooperation Agency) ○ Craig Newmark Philanthropies	

	○ Ford Foundation ○ Fastly (provides in-kind support for hosting Tor updat	
性能/有效性和可靠性	測試環境設定： ● 裝置**:** 戴爾 XPS 15 ● 作業系統：**Windows** ● 網路：4G 使用者體驗觀察 ● 該工具透過瀏覽器搜尋時感覺相對流暢。 ● Tor 瀏覽器有時會很慢，但這是因為使用中繼網路增加了額外的安全性和隱私層。 速度和反應能力： ● Tor 使用大量中繼來傳輸流量，導致速度緩慢。速度通常比傳統上網方式慢，尤其是在訪問網路擁堵嚴重或流量高峰期。 ○ 例如：下載報告、存取安全通訊網絡，甚至打開包含大量文件的人權網站，速度都可能顯著降低。與25至100 Mbps的標準網路速度相比，Tor的下載速度僅為0.5至2 Mbps，比一般上網速度慢三到五倍。這在分秒必爭的環境下（例如網路管控和監控嚴格的地方）或執行時間緊迫的任務時可能會帶來困難。 https://surfshark.com/blog/tor-browser-slow 資源使用： ● Tor 佔用的資源量適中。由於需要中繼，它比標準瀏覽器消耗更多資源，儘管它對資源的要求並不高。當它用作中繼節點時，可能會消耗大量資源。 網路效能： ● 透過使用 Wireshark 等工具監控頻寬消耗來測試網路效率。 ● Tor 採用洋蔥路由機制，透過多個中繼反彈流量，因此增加了延遲並減少了頻寬。 ○ 100 毫秒 - 30 秒（延遲取決於使用情況） https://metrics.torproject.org/torperf.html?start=2025-01-01&end=2025-04-01&server=onion&filesize=50kb ■ 1-10 Mbps（頻寬） 可靠性 ● 由於社群規模龐大，整體而言很受歡迎。 ● 第三方網路安全審計展示了 Tor 的安全功能，並就弱點和改進方法提供了回饋。	

部署注意事項:	開源與透明度: ● 該代碼可供獨立驗證。 雲端部署與本地部署: ● 專為本地使用而設計，不需要 AWS/Azure。 ● 可以在雲端伺服器上運行，但像 Tor 中繼或出口節點，而不是典型的 Web 瀏覽器。 ● Tor 目前已部署完畢，因此用戶如果想使用它就無需重新部署，並且會得到積極維護（每隔幾週進行一次安全更新，每年進行一次重大更新），與 Firefox ESR（擴展支援版本）更新保持一致。 依賴項: ● 不，Tor 瀏覽器本身不需要 Docker、Python 或資料庫。 ● 然而，Tor 網路和相關服務可能存在依賴關係: ○ 為網路提供動力的 Tor 守護程序 (tor) 是用 C 語言編寫的，不需要 Docker 或資料庫。 ○ 一些 Tor 工具和腳本（例如洋蔥服務管理）可能使用 Python 或其他腳本語言。 ○ 在伺服器上執行 Tor 中繼或出口節點不需要資料庫，但可能需要特定的系統配置。 部署後維護 ● Yes，部署後很容易維護。 ● 如果程式碼分叉，修改瀏覽器介面與 Firefox ESR 類似，難度不大。但如果嘗試修補安全/網路更改，則需要更多專業知識。 合併/可持續性: ● 原始專案對貢獻的開放程度如何？ ○ Tor 專案是開源的，歡迎大家貢獻程式碼。原始碼可以在 GitLab 上找到: https://gitlab.torproject.org/。 ○ 開發人員可以透過提交修補程式、錯誤修復或新功能來做出貢獻。 ○ 該專案有公共問題追蹤、開發者指南和審查變更的活躍維護者。 ● 將更改提交回主存儲庫是否容易？ ○ 中等難度－雖然歡迎貢獻，但 Tor 有嚴格的安全和隱私要求。 ○ 程式碼變更在合併之前要經過廣泛的審查。 ○ 一些貢獻（尤其是與安全相關的貢獻）需要對網路安全和匿名系統有深入的了解。	

	○ 貢獻者應遵循 Tor 專案的程式指南。	

4. 測試場景

- 場景 **1**
  IP洩漏測試
  https://ipleak.net/

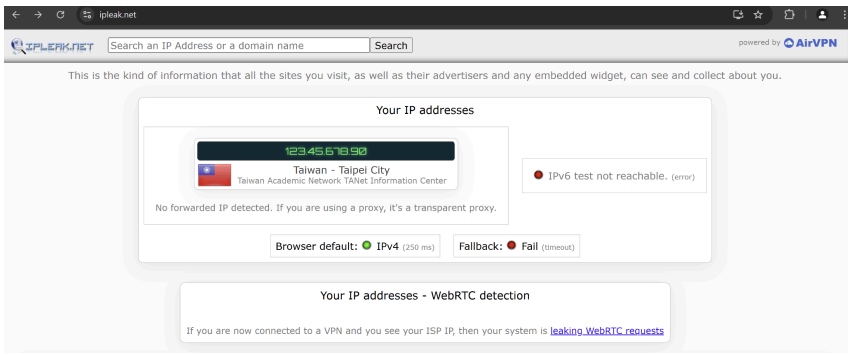


圖 *1*:使用 Google Chrome 的公共 IP 位址(出於安全原因，實際 IP 以馬賽克呈現)

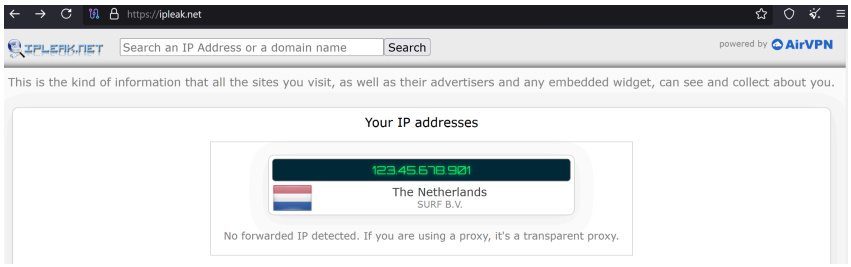
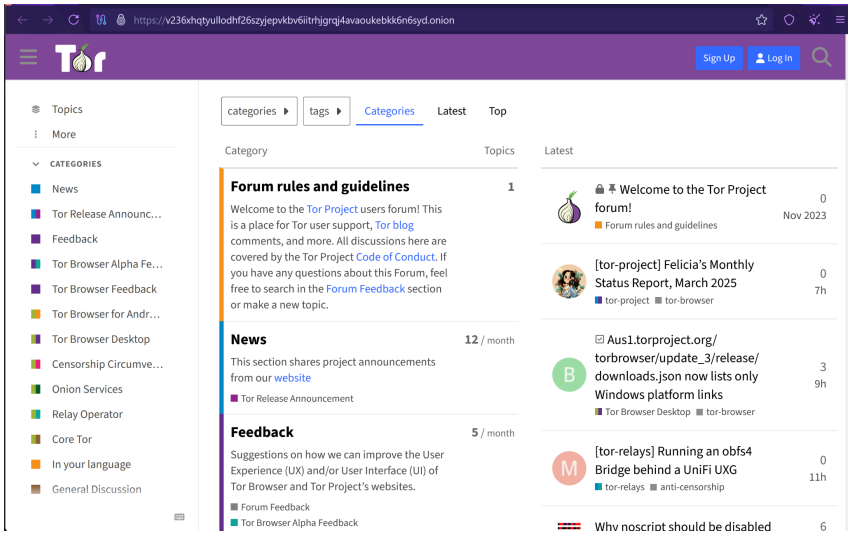


圖 *2*:使用 Tor 的公共 IP 位址(出於安全原因，實際 IP 以馬賽克呈現)

- 視窗:開啟命令提示字元(Win + R，輸入 cmd，按 Enter)，然後輸入**ipconfig** 並在活動網路連線下尋找 IPv4 位址。
- 蘋果:打開終端機並輸入**ipconfig** 取得地址**en0**(乙太網路使用 en1)，然後記下您的私人 IP。
- **Linux**:打開終端機並輸入**ip a**，然後尋找網際網路 在您的活動網路介面下。
- 如上圖 1 所示，Chrome 不會封鎖或封鎖我的真實 IP 位址，這使得它可被追踪，並洩露詳細的地理位置資訊。除了侵犯隱私之外，這種曝光還能讓我在短距離內被定位。這嚴重威脅了那些希望保持匿名的記者、活動人士和人權捍衛者的安全和隱私資訊。
- 如上圖 2 所示，Tor 有效地掩蓋了我的真實 IP 位址，防止被追蹤到。Tor 透過多個加密橋接器傳遞我的連接，而不是洩漏我的實際位置，幾乎不可能確定我的確切位置。這提高了安全性，最重要的是保護了隱私，為必須保持匿名的記者、活動家和人權倡議者提供了至關重要的保護。

• 場景 **2** 洋蔥服務範例	Tor 服務目錄(例如 Ahmia 和 Hidden Wiki)列出了各種洋蔥服務。您也可以使用索引洋蔥服務的搜尋引擎。 
5. 見解和建議	

主要發現	優勢:
	• 易於下載和使用
	• 可以隱藏IP位址
	• 個人可以提交合併請求(相當於 GitLab 中的拉取請求),這遵循 Tor 的貢獻指南和嚴格的安全標準。
	• 並非所有變更都會被接受,安全性和匿名性是首要任務。
	• 小修復(如 UI 更改)可以與審查合併。
	• 網路和加密等修改在被接受之前需要更廣泛的審查和測試。
	• 設定 → 連接 → 橋接:
	  ○ Tor 內建了橋樑,幫助使用者繞過審查並在被封鎖的地區存取 Tor 網路。
	  ○ 通常,Tor 用戶端連接到公開的入口節點,但網橋充當未公開列出的隱藏入口點,這使得審查和阻止它們變得更加困難。
	  ○ Tor 瀏覽器包含一些稱為「可插拔傳輸」的特定類型的橋接器,它們可以幫助隱藏您正在使用 Tor 的事實。
	  ○ obfs4:
	  ■ 讓你的 Tor 流量看起來像是隨機資料。在審查嚴格的地區可能無法正常工作。
	  ■ 偽裝 Tor 流量以防止深度套件偵測 (DPI) 偵測到它。

	○ 雪花： ■ 例如，透過 Snowflake 代理路由您的連接，使其看起來像您正在進行視訊通話。 ■ 基於志工的逃避，使用志工的瀏覽器作為代理 ■ 由於代理不斷變化，因此很難阻止 ○ 溫柔的蔚藍色： ■ 讓你看起來像是在連接到微軟網站，而不是使用 Tor。在審查嚴格的地區可能有效，但速度通常很慢。 ■ 基於雲端的規避，透過雲端服務路由流量 ■ 比 obfs4 慢，但在限制性更強的環境中也能工作。 ○ 橋樑的好處： ■ 繞過 Tor 被屏蔽的審查 ■ 防止 ISP（網際網路服務供應商）跟踪 ■ 洋蔥服務（通常稱為暗網）是使用 .onion 網域的網站，只能透過 Tor 網路存取。如果公共安全節點被屏蔽，洋蔥服務就無法使用。網橋充當秘密入口點，允許用戶繞過這些屏蔽，匿名連接到洋蔥服務。 ■ 如果某個國家阻止 Tor 訪問，記者或活動家可以使用網橋連接並安全地訪問洋蔥網站（例如，隱私工具、舉報人平台或獨立新聞來源）。 ■ 透過建造橋接器，幫助他人存取自由開放的網路。這是一個基於志願者的節點，旨在幫助受審查國家/地區受審查的用戶連接到 Tor。這支持網路自由，增強專制政權下活動人士、記者和研究人員的隱私。 ○ 洋蔥服務： ■ 允許匿名託管網站和服務，而無需透露位置或 IP 位址（例如 example.com->asdf123.onion，只能透過 Tor 瀏覽器存取） ■ 當造訪這樣的網站時，您的請求將透過多個中繼進行路由，從而使網站所有者和訪客保持匿名。 ■ 使個人能夠開展工作而不必擔心被追踪，包括非政府組織、民間團體和舉報人。 ■ 這促進了限制網站和隱私的國家抵制審查，因為沒有中央權威機構知道誰擁有或查看該網站。

	弱點: ● 根據 2024 年第三方審計,「文件可以改進, 以明確對用戶隱私的承諾, 並避免任何潛在的資料外洩」以及「應實施正式的程式碼審查流程, 重點關注所有變更對隱私的影響。該流程應包括同行評審、自動隱私檢查和定期審計, 以確保在開發過程中始終如一地考慮隱私問題。」 ● 如果網站發現您的螢幕解析度與其他使用者不同, 則可能會限制搜尋結果。因此, 不建議以全螢幕模式執行 Tor, 也不建議安裝任何瀏覽器擴充功能。 ● 儘管 Tor 僅保護 Tor 瀏覽器內的通訊安全, 但許多用戶誤以為它會加密所有資料。Tor 不涵蓋任何其他應用程序, 例如 Zoom 或 Spotify。 ● Tor 有助於保護您的線上隱私, 但如果您的裝置已被感染, 它就無法保護您 - 例如有人在您的電腦上安裝了鍵盤記錄器或螢幕錄製惡意軟體。 ● 使用 Tor 時請勿登入個人帳戶(Gmail、Facebook、Instagram 等)或下載文檔, 因為它會破壞匿名性。
建議的改進	● 使用者介面改進:使用者介面改進以提高清晰度和導航 i. 增強暗模式支援和可訪問性選項。 ● 文件:逐步安裝指南、技術使用者教學課程 i. 為技術使用者提供更多互動式教學(例如, 設定 Tor 中繼或洋蔥服務)。
替代工具:	Brave, Mullvad, Librewolf
授權:	Mozilla 公共授權
成本/資源影響	總成本: ● Tor 的所有功能都是免費的 ● 無需訂閱。
為什麼這對威權環境中的公民社會有用?	● 平台保護/審查: ○ 中國等國家的國家防火牆會阻止造訪討論民主、人權和獨立新聞的網站。由於這些地區的當局禁止已知的 Tor 節點, Tor 因其典型的設置而經常無法存取。使用者必須依賴 Tor 網橋, 它們是未公開的中繼器, 不在公共目錄中。然而, 深度資料包偵測 (DPI) 甚至可以識別並阻止這些中繼器。 ○ 為了規避審查並對抗審查, Tor 提供了像 obfs4 這樣的可插拔傳輸協議, 它可以透過使 Tor 流量看起來像是隨機資料來欺騙深度資料包檢測 (DPI) 系統。即便如此, 像中國國家防火牆這樣的先進審查系統也能夠識別並阻止 obfs4。

	○ 為了解決這個問題，使用者需要請求透過 Tor 的 BridgeDB 服務或電子郵件分發的私有（未列出的）obfs4 橋接器。 ■ Tor 的 BridgeDB 服務（網站可能被封鎖，因此電子郵件選項可能更可靠） ■ 發送電子郵件至：bridges@torproject.org ● 主題行和正文：寫“取得傳輸 **obfs4**」 ● 重要提示：您必須使用 Gmail 位址傳送電子郵件。（其他電子郵件提供者可能會被阻止或拒絕。） ■ 要配置，請開啟 Tor 並按一下“設定連線**…**”而不是“連接」。然後，貼上橋接線路（如果橋接線路停止工作或被阻塞，請定期切換橋接線路）。 ○ 例如，北京的一位非政府組織員工可以手動配置 Tor，使用自訂 obfs4 網橋，以便在嘗試存取受限制的國際人權網站時避開國家防火牆的偵測。這確保了與海外合作夥伴的安全合作、宣傳資源以及持續獲取外部新聞。 ● 透過洋蔥服務進行身分保護： ○ 面臨被捕或報復風險的活動人士和舉報人可以使用洋蔥服務無需透露其位置即可託管或存取內容。例如，記錄緬甸軍事暴行的非政府組織可以創建一個.onion網站，安全地收集平民證詞，保護雙方免受IP監控和域名被封鎖的威脅。 ○ Tor 加密資料並匿名化其路徑，使專制政府更難追蹤通訊或確定誰在受監控的情況下存取了哪些內容。對於在伊朗等國家工作的公民團體來說，這非常有幫助，因為在這些國家，網路服務供應商有義務監控流量並報告可疑行為。透過洋蔥服務，Tor 可以讓這些組織安全地發送加密電子郵件、共享文檔，並使用 Signal 或 ProtonMail 等被禁止的程式。 ● 也建議在啟動 Tor 瀏覽器之前使用可用的 VPN（如果在該國不違法的話），以使防火牆更難檢測和阻止 Tor。 ● 如果 obfs4 橋接器不起作用，請嘗試 Snowflake（基於 WebRTC 的傳輸）或 Meek（基於雲端的傳輸）橋接器。 ○ WebRTC 技術比其他傳輸方式更能抵抗阻塞。 ○ 基於雲端的傳輸很難被阻止，因為它將 Tor 流量偽裝成到知名雲端提供者（例如 Google 或 Amazon Web Services）的常見 HTTPS 流量，並且在審查技術先進的地區可能是一種非常有效的選擇。

	○ 如果這些仍然不起作用, 您可能需要使用 Tor 的官方橋接設定指南來設定 Tor 橋接器(如果您可以存取國外的伺服器)。