政治科學論叢／第 105 期／民國 114 年 9 月／頁 69-120

俄羅斯的網路主權概念之發展立法及未來之影響*

許菁芸**

摘　要

網路數位科技的快速發展改變了政府與公民互動的方式，賦予國家施加控制的新方式，越來越多的國家正在引入自己國家的網路主權概念。俄羅斯「主權網路法」於 2019 年 11 月 1 日生效，該法案授權「俄羅斯聯邦通訊、資訊科技和大眾傳媒監督局」（Roskomnadzor）監控全國個人網路跟公用網路的運作，只要遇到緊急狀況，俄國政府主管機構可以主動切斷與外界的聯繫，建立一個獨立於全球網路之外運作的國家網路。自從 2022 年俄烏戰爭爆發後，俄羅斯政府越來越多地利用網路數位技術作爲控制工具，爲維護其線上空間的主導地位並加強其控制，俄羅斯對網路言論的限制更加嚴格、監控力度加大，以及旨在透過嚴格法律的通過遏制異議。因此，本研究目的即是研究網路主權對俄羅斯的意涵、自 2012 年後網路主權的發展、立法與未來影響，並分析 2022 年俄烏戰爭後俄羅斯網路控制更形嚴峻之走向。

關鍵詞：俄羅斯、網路主權、俄網、主權網路法、資訊安全

---

* DOI:10.6166/TJPS.202509_(105).0003
本文爲國科會個人型專題研究計畫「俄羅斯網路主權研究」（111-2410-H-004-065-MY2）之研究成果。本文初稿曾發表於 2024 年 11 月 8 日舉辦之中華民國國際關係學會 2024 年會暨「新國際政經秩序之重構：軍事、民主、經濟與科技的多重挑戰」國際學術研討會。作者非常感謝本刊兩位匿名審查人對此論文悉心審閱並提供寶貴意見，提供本文修繕與更多延伸性的思考。

** 國立政治大學俄羅斯研究所教授兼所長，E-mail: june0130@nccu.edu.tw。

收稿日期：113 年 12 月 27 日；通過日期：114 年 6 月 23 日

壹、前言

全球網路治理在過去幾十年本著《網路空間獨立宣言》(The Declaration of the Independence of Cyberspace)，宣稱其爲無國籍空間，主張其治理不應遵守國家政府的法律的精神不斷發展（Barlow, 1996），但顯然已經到了一個分界點，越來越多的國家正在引入自己國家的網路主權概念，因爲網路數位科技的快速發展改變了政府與公民互動的方式，賦予國家施加控制的新方式。

網路有現實與虛擬的特性，結合了兩種不同的觀點。其一，網路被視爲具有位於各個國家邊界內的實體基礎設施的跨國和跨境網絡。作爲實體基礎設施，從網路服務供應商（Internet Service Providers，之後簡稱 ISPs）設備到數據中心，網路始終以領土爲界，並在空間上位於特定國家的管轄範圍內。因此，如何在物理基礎設施的層面上對虛擬網路進行治理，這不僅是由立法推動的，而且是由看似無害的高端科技來推動。其二、網路是一個全球性網絡，它實現了具有可滲透邊界的全球化國家、組織和社群的烏托邦願景，由於這種模糊性，網路以不同的方式對主權提出挑戰。

Google在2010年4月20日推出了「政府請求工具」(Government Requests tool)網頁，首次公開各國政府查詢特定使用者資料的次數，以及要求 Google 從其搜尋引擎、YouTube 等平臺移除特定內容的次數。根據 2011 年的統計，各國政府要求刪除訊息的國家排名依次爲德國、挪威、美國、巴西、韓國（中國數據無法得知），在要求提供網路用戶數據的國家排名依次爲美國、印度、法國、英國、德國（IThome, 2011）。然而在 2019～2020 年底公布的數據中，俄羅斯政府要求刪除訊息次數中，高達 18,656 次（2011 年僅有 4 次），刪除的物件高達 179,112 件，至 2024 年 6 月，俄羅斯政府要求刪除訊息次數（包含法院命令、相關政府部門、聯邦法第 276 號規定）高達 26,499 次，要求刪除的物件高達 328,357 件，排名都佔第一，遙遙領先其他國家（Google, 2024）。

俄羅斯網域（俄網，Рунет，以下簡稱 Runet）的起源可追溯至 20 世紀 80 年代末至 90 年代初，但直到 1994 年才正式擁有以「.RU」爲結尾的國家

域名。俄羅斯網路最初基本上是自發地、自下而上地發展起來的。在 2012 年之前，俄羅斯的全國網路普及率相對較低，約占全國人口的 49%，但其使用率正快速提升。根據國際電信聯盟（International Telecommunication Union, ITU）的統計，直至 2023 年，已成長至 92%（World Bank, 2023），且穩定成長中。隨著越來越多俄國人使用網路，以及網路世界中衝突的增多，俄國政府也開始認爲有必要推行所謂的「數位主權」（digital sovereignty），也稱爲網路主權。簡單來說，這指的是一國對其境內的數據和線上內容進行控制的權力。

2019 年 5 月 1 日，俄羅斯總統普京（Vladimir Putin）簽署了一項新法案，規定在緊急情況下，俄國政府主管機構可主動切斷與外界的網路連接，建立一個獨立於全球網路之外運行的國家網路。該法案於 2019 年 11 月 1 日正式生效。對於長期以來習慣於較少網路管控的俄羅斯而言，這無疑帶來了巨大影響，這項法案被稱爲「主權網路法」（Закон о «суверенном интернете»）。

關於俄羅斯主權網路法的創立目的，根據官方的說法，該法案主要是爲了俄羅斯內部網路的順利運行而實施的，如果有一天俄羅斯無法連結到國外網站，或國外網站停止對俄羅斯的服務合約的話，那俄羅斯則可以保證自己的網路依舊能夠順利運作（Замахина, 2019）。該法案授權「俄羅斯聯邦通訊、資訊科技和大眾傳媒監督局」（Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Роскомнадзор，以下簡稱 Roskomnadzor）監控全國個人網路跟公用網路的運作，識別對俄羅斯可能具有威脅的網站，要求並提供俄羅斯的 ISPs 安裝監控與封鎖軟體以對付這些可能存在的威脅。俄羅斯稱，自美國開始使用網路資訊戰後，該法案的實施可以確保俄羅斯國內的安全，且可減少「美國國家網路政策」（National Cyber Strategy of the United States of America）下「利用網路空間進行攻擊的可能性」（Фонд «Росконгресс», 2022）。

自從 2022 年俄烏戰爭爆發後，俄羅斯政府越來越多地利用網路數位技術作爲控制工具，克里姆林宮對其數位基礎設施追求「主權」反映了一個更廣泛的目標，即維護其線上空間的主導地位，減少對外國平臺的依賴，並加強其控制。這種轉變，尤其是在烏克蘭持續衝突的情況下，導致對網

路言論的限制更加嚴格、監控力度加大，以及旨在透過嚴格法律的通過遏制異議。

因此，本文研究目的如下：

1. 審視全球化網路與國家主權的關係，並探討網路主權的定義。
2. 藉由探討俄羅斯自 1999～2019 年的重要資訊立法法案的詞彙關注重點，探討俄羅斯對於網路主權的理解與認知。
3. 從俄羅斯網路發展、特點來分析俄羅斯 2019 年「主權網路法」，及該法案特點，並探討俄羅斯網路過濾、監控設備及其效應。
4. 分析 2022 年俄烏戰爭後俄羅斯網路控制、影響與未來發展。

貳、相關文獻探討

一、全球化網路與國家主權

20 世紀 90 年代，源自美國國防部 ARPANET（Advanced Research Project Agency Net），[1] 以光纜爲骨幹聯繫全球的網際網路，加速了全球化的發展，網路空間扮演全球化的關鍵角色（Hauben & Hauben, 1997）。藉由網際網路所構成的自由化、去中心化和無邊界性的網路空間，與國家獨立性、固有領土的特質有著顯著的不同。全球化網路時代的到來，開始削弱在國際政治中以國家爲中心的觀念，網路空間在全球相互依存的多中心國際體系的地位日漸突出，國家之間的相互依賴性日漸增強，但也造成了國際現實主義下在網路空間的衝突日漸增多的現象。而以國家爲主要行爲體的國家主權，便成爲捍衛的首要目標。

一般而言，主權指的是一個政治實體（political entity）在特定領土範圍

[1] 當前全球使用的國際網路，正是美蘇冷戰競爭的產物。1957 年，蘇聯成功發射首顆人造衛星後，美國爲應對冷戰局勢，國會授權國防部成立高等研究計劃署（Advanced Research Projects Agency, ARPA），並資助創建高等研究計劃署網路（Advanced Research Projects Agency Network），即阿帕網（ARPANET）。阿帕網由美國國防高等研究計劃署開發，是全球首個運行的封包交換網路，被視爲現代網際網路的起源。在 1990 年退役之前，阿帕網運行了 20 年，期間一直是美軍不可或缺的通訊工具。作爲首個實現 TCP/IP 通用網路協定的網路，阿帕網爲當今網際網路的技術發展奠定了基礎（Wright, 2021）。

內擁有至高無上權威的能力。儘管國家主權早已被國際社會視爲一項國際法原則，但當代主權學者 Hinsley (1966, pp. 1-9) 指出，雖然許多論述探討主權的取得、喪失或被侵犯的方式，但主權並非一個具體的事實（fact），而是一種關於政治權力如何運作以及應該如何運作的概念（concept）或主張（claim）（許菁芸、宋鎮照，2013，頁 57）。

主權原則強調每個國家內部都存在著一個中央權力，莫根索（Morgenthau, 1967, p. 315）提出：「在每一個政治系統中必須有一最後決策的絕對權力擁有者，其可能是一個人或一機構，但均需有絕對的權力去決定和執行其政策，及對行使政治權力負最終的責任。」在和平時期，憲法對權力的分配產生一種現象，也就是最高立法者和執法者的權力似乎不見了，但是在危機和戰爭時期，這種錯覺很快就消失了，取而代之，是最終的責任與絕對的權力重新被強調，因此，權力與自主、等級與民主之間的矛盾的解決通常是以犧牲民主原則爲代價（Camilleri & Falk, 1992, pp. 38-45）。

Beitz (1999, p. 236) 認爲現代歷史的主權概念具有雙重的特性，也就是內部主權（internal sovereignty）與外部主權（external sovereignty）的概念，Reinicke (1998, p. 66) 認爲，所謂外部主權是指國家在外部環境中與其他國家之間的關係及其在國際體系中的地位；而內部主權則是指國家在其領土範圍內，政府與公民、經濟以及各類具體團體和制度之間的關係。他進一步指出，在內部與外部主權的劃分基礎上，主權可以概念上分爲「合法的主權」（legal sovereignty）與「運作的主權」（operational sovereignty）（許菁芸、宋鎮照，2013，頁 59-60）。全球化網路的發展雖未挑戰到國家合法的內在主權（legal internal sovereignty），但是卻挑戰其內部的運作主權（operative internal sovereignty），因此，在全球化網路的發展中，國家遇到的根本挑戰來自內部而非外部。

二、網路主權的定義

資訊革命和全球向資訊時代轉變的過程帶來了很多新問題，每個國家都有各自改變政治制度和應對資訊革命挑戰的獨特方式，但網路空間是全球性的，其存在形式超越了主權國家的邊界，因而容易引發不同國家間理念和政策的衝突，網路與現實世界深度融合使得網路安全（cybersecurity）

成爲關乎國家安全的重要考量。

從廣義上講，主權是一個有爭議的多方面概念，網路治理是在網路的民主、跨國性質與各國政府試圖控制網路空間之間的拉鋸戰中發展起來的，因此全球網路治理背景下的「網路主權」通常被用來表示各國有意與跨國網路治理機構（如WGIF、IGF 或 ICANN）競爭。在有關全球網路治理方案中，大多數西方國家採用「網路中立」原則，此原則確保了每個使用者的平等訪問和通信速度，從而排除了任何操縱內容的可能性。西方國家將資訊時代的主權理解爲鼓勵通過安全的技術基礎設施進行全球資訊交流，並認爲國家在管理網路技術基礎設施方面的過度干預可能會威脅到全球網路的穩定性，從而破壞其全球影響力。

但是近十幾年來，網路主權的想法開始在民族國家中獲得越來越多的支持，2010年代，「網路主權」在全球媒體中具有相當負面的含義（Woodhams, 2019）。雖然在2000年代，中國的金盾計劃（Golden Shield program）（也稱爲萬里長城防火牆）是網路隔離的一個典型例子，多年來，很多威權國家已經制定了本國的主權網路法案。中國、伊朗和俄羅斯的網路隔離政策被視爲「分裂網路」（“Splinternet”）[2]（或稱網路巴爾幹化）的破壞性趨勢，網路主權的趨勢將會破壞全球數位經濟並侵犯言論自由和資訊獲取自由的人權。但是俄羅斯認爲政府不僅有責任保護網路基礎設施，而且有責任保護資訊本身，俄羅斯政府在2016年的《俄羅斯聯邦資訊安全綱領》（Доктрина информационной безопасности Российской Федерации (№ 646)）中將資訊安全理解爲俄羅斯公民之間「不擴散」外國資訊，並與外國分享「關於俄羅斯的適當資訊」，並包括政府對資訊的強有力控制，以促進國際資訊安全爲基礎。俄羅斯的資訊安全理念意味著政府對網路資訊資源的重大責任和控

[2] 一般認爲這個新名詞是在麻省理工學院教授馮埃爾斯泰恩（Marshall W. Van Alstyne）和布林約爾松（Erik Brynjolfsson）在 1997 年 3 月 1 日發表的《電子社群：全球村，還是網路巴爾幹國家？》（Electronic Communities: Global Village or Cyberbalkans）的論文中首次提出，意指全球網路已分裂成各懷利益心機的眾多群體，且任一子群的成員總利用網路傳播或閱讀僅吸引相同子群成員的訊息或題材（Van Alstyne & Brynjolfsson, 2005）。

制。[3] 因此，俄羅斯對於網路主權的理解，是強烈帶著「資訊安全」含意。

然而，在過去幾年中，歐盟國家等民主國家也開始激烈討論網路主權（Pohle, 2020）。不同的政體在討論網路主權時是否是同樣的定義？顯然不是。「網路主權」一詞仍然是一個備受爭議的詞，其解釋因國家而異，因此具有「衝突潛力」（conflict potential）（Thiel, 2021）。一方面，網路爲全球不同的參與者提供了巨大的機會。另一方面，它通過賦予大型社交媒體平臺等新的全球參與者權力，破壞了民族國家的主權，挑戰了國家現有規則。1990 年代和 2000 年代，全球網路爲民族國家帶來的好處大幅度地戰勝了對網路威脅的擔憂。然而，2011 年的阿拉伯之春後，世界各地的威權領導人意識到社群媒體的動員潛力已成爲對其統治的眞正威脅，因此他們越來越加強對各自國家網路的控制（Richter & Kozman, 2021）。2013 年，斯諾登（Edward J. Snowden）揭露美國情報機構對網路進行監控，[4] 引發了關於歐盟國家科技自主權的討論。

由上述分析可見，目前爲止「網路主權」仍然沒有一定的定義，被不同的政治體制以不同的方式解釋，其概念可以分爲以人民爲中心的網路主權，如 Kolozaridi 和 Muravyov (2021) 將國家的網路主權主張理解爲「主要功能是對抗霸權傾向的表現與修辭行爲」（performance, rhetorical acts whose primary function is to counter hegemonic tendencies）；或者它是以政府爲中心的網路主權，如 Wolff H. von Heinegg (2012, pp. 8-12) 認爲國家有權在其領土範圍內，對網路基礎設施與相關活動進行管理與監督，並依法行使管轄權。同時，應保障其境內的網路與通訊設施免受外國勢力干預。任何對該國網路基礎設施造成損害或威脅的行爲，皆可視爲對國家主權的侵犯。

隨著網際網路技術的迅速擴展與深度應用，各國日益面臨諸如網路安

---

[3] 俄羅斯聯邦早期在其官方文檔中並未使用「網路安全」（cybersecurity）一詞；相反，它使用的是「資訊安全」（information security）（下一章節說明）；而聯合國決議對於網路安全所使用的術語是「在國際安全的背景下審視資訊和電信領域的發展」（developments in the field of information and telecommunications in the context of international security）（United Nations General Assembly, 2015）。

[4] 斯諾登指控的主要是兩點：一、美國對中國發動了網路攻擊，竊取了他國情報；二、「美國政府利用他們正在秘密建造的這一龐大的監視機器，摧毀隱私、互聯網自由和世界各地人民的基本自由」（何清漣，2013）。

全、資料保護及跨境網路犯罪等日益複雜的挑戰。爲回應此類風險，主權國家逐步強化其對網路空間的治理能力，並將網路主權視爲維護國家利益與安全的關鍵策略。特別是資料在地化（data localization）的政策趨勢，已成爲威權或不自由國家網路治理的重要手段之一，反映出國家對數據流通與控制權的高度重視。這一發展不僅標誌著對網路自由與開放性的再評估，也預示著全球網路空間將逐步轉向以國家監督與規範爲核心的治理模式（Klimburg, 2017, pp. 31-42）。

三、俄羅斯對網路主權的理解與認知

俄羅斯對於網路主權的認知非常有趣，作者檢視了俄羅斯 1999 年至 2017 年間，截至《主權網路法》（2019）頒布前的以下七項針對網路政策綱領、戰略與文件：《俄羅斯資訊社會發展構想》（Концепция формирования информационного общества в России）（1999）、《俄羅斯聯邦資訊社會發展戰略》（Стратегия развития информационного общества в Российской Федерации）（2008）、《俄羅斯聯邦資訊安全綱領》（Доктрина информационной безопасности Российской Федерации）（2000、2016）、《2020 年前國際資訊安全領域國家政策基本原則》（Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года）（2013），以及《2014～2020 年資訊科技部門發展戰略及 2025 年未來前景》（Стратегия развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года）（2013），《2017～2030 年俄羅斯聯邦資訊社會發展戰略》（О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы (№ 203)）（2017），最後通過並頒布了 2019 年《主權網路》法案。藉由探討俄羅斯自 1999～2017 年的重要資訊立法法案的詞彙關注重點，可以分析出俄羅斯對網路主權的理解和在 2012 年前後的不同認知（Московский Либертариум, 1999; Независимая газета, 2000; НКЦКИ, 2013; Президент России, 2017; Российская газета, 2008, 2013a, 2013b; Совет Безопасности Российской Федерации, 2016）。

通過分析上述文件，俄羅斯官方對網路主權的認知，作者有幾項發現：

(一) 俄羅斯網路政策的關鍵詞彙：資訊安全（information security）

「網路」（internet）一詞在1999年《俄羅斯資訊社會發展構想》和2000年的《俄羅斯聯邦資訊安全綱領》中均未提及，而在2008年《俄羅斯聯邦資訊社會發展戰略》中僅提及3次。直到2013年頒佈之《2020年前國際資訊安全領域國家政策基本原則》，網路才在分析的文件中被提及。所有文件中使用最廣泛的詞彙是「資訊」（информация）、「資訊領域」（информационная сфера）和「資訊和通訊技術」（информационные устойчивые коммуникационные технологии）。2000 年《俄羅斯聯邦資訊安全綱領》強調了資訊領域在「維護和加強社會道德價值觀、愛國主義和人文主義傳統」（сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма）中的作用，而且第一次提到了俄羅斯在資訊科技（Information Technology，以下簡稱 IT）領域「加強國內資訊安全工具軟硬體開發生產」（интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации）的必要性（Независимая газета, 2000）。

1999 年的《俄羅斯資訊社會發展構想》看起來非常樂觀，並指出「俄羅斯向資訊社會過渡的主要戰略目標是創造發達的資訊和通訊社會環境以及俄羅斯整合至全球資訊社會」（Стратегической целью перехода к информационному обществу является создание развитой информационно-коммуникационной среды общества и интеграция России в мировое информационное сообщество）。在 2008 年的《俄羅斯聯邦資訊社會發展戰略》中，重點在於完善電子治理，以及參與國際規範和制定網路治理機制。

在 2000 年和 2006 年《俄羅斯聯邦資訊安全綱領》中，都沒有提到俄羅斯常在國際文件中使用的「網路安全」（кибербезопасность）。重點始終是資訊安全，也就是內容，而不是其傳輸渠道。根據這些文件，俄羅斯應該應對「資訊安全威脅」（угрозы информационной безопасности），尤其是「資訊戰」（Информационная война）。雖然「資訊戰」是《俄羅斯聯邦資訊安全綱領》的重要術語，但並未給出明確的定義。在俄羅斯聯邦資訊安

全的外部威脅中，列出了「一些國家發展資訊戰構想，隱含著創造對他國資訊領域造成危險影響的手段，破壞資訊和電信系統的正常運作、影響資訊安全及未經授權存取資料」（разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.）（Совет Безопасности Российской Федерации, 2016）。

與 1999 年《俄羅斯資訊社會發展構想》和 2008 年《俄羅斯聯邦資訊社會發展戰略》相比，2017年《2017～2030年俄羅斯聯邦資訊社會發展戰略》更加關注「發展國家數位經濟」（формирование национальной цифровой экономики）。該戰略中的一個重要詞彙是「關鍵資訊基礎設施」（критическая информационная инфраструктура），即國家機構和不同行業使用的資訊技術。爲了保護關鍵資訊基礎設施，國家必須支持並代表國家 IT 公司的利益。在 2017 年的發展戰略中，網路政策的主要目標之一是俄羅斯向「知識社會」（общество знаний）發展，該社會被定義爲「獲取、保存、生產和傳播可靠資訊，同時考慮俄羅斯聯邦的國家戰略優先事項，對於公民、經濟和國家的發展至關重要」（общество, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной информации с учетом стратегических национальных приоритетов Российской Федерации）（Президент России, 2017）。

尤其在 2013 年《2020 年前國際資訊安全領域國家政策基本原則》中，「國際資訊安全」（международная информационная безопасность）明確定義爲「全球資訊空間的一種狀態，在這種狀態下，個人、社會和國家在資訊領域的權利不會受到侵犯，並且排除了對國家關鍵資訊基礎設施組成進行破壞性和非法影響的可能性。」（состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также

деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.）（НКЦКИ, 2013）因此，作者認爲，俄羅斯對於網路主權的第一個認知是「資訊安全」。

(二) 網路主權：預防性的防禦策略

隨著時間的推移，戰略文件中俄羅斯網路政策背後的基本原理經歷了巨大的演變。1999 年的《俄羅斯資訊社會發展構想》提到了在全球化進程中保持獨立性的重要性，但全球化的整體基調是樂觀和對國際社會友好的，甚至被稱爲「大家庭」，其中提及「俄羅斯必須加入技術和經濟發達國家的大家庭，成爲世界文明發展的正式參與者，同時保持政治獨立、民族認同和文化傳統」（Россия должна войта в семью технологически и экономически развитых стран на правах полноценного участника мирового цивилизационного развития с сохранением политической независимости, национальной самобытности и культурных традиций）（Московский Либертариум, 1999）。

在 2000 年的《俄羅斯聯邦資訊安全綱領》中，資訊安全面臨的主要威脅清單並沒有那麼多，而且表述得相當模糊：從對人權的威脅到「俄羅斯精神復興」（духовное возрождение России），再到「對俄羅斯聯邦的國家政策的資訊支持」（информационное обеспечение государственной политики Российской Федерации），以及 IT 專家的人才流失，並且還強調了對俄羅斯 IT 生產的支持（Независимая газета, 2000）。

2008 年《俄羅斯聯邦資訊社會發展戰略》標誌著梅德韋傑夫（Dmitry Medvedev）總統仍然看好資訊和電信技術，當時資訊和電信技術已成爲全球「社會經濟發展的火車頭」（локомотив социально-экономического развития），因此國家必須確保「公民自由獲取資訊的機會」（обеспечение гарантированного свободного доступа граждан к информации）並開發電子政府服務（Российская газета, 2008）。

2012 年普京三任總統後，對於網路態度開始轉變——從參與到防禦。

2013 年《2020 年前國際資訊安全領域國家政策基本原則》開始提及促進俄羅斯在國際資訊安全領域的舉措。這點出資訊通信技術的重要性，

因爲資訊通信技術可以用作「資訊武器」（информационное оружие），「旨在詆毀主權、侵犯國家領土完整」（направленные на дискредитацию суверенитета и нарушение территориальной целостности государств）和「干涉主權國家內政和違反公共秩序」（вмешательство во внутренние дела суверенных государств, нарушение общественного порядка)的手段（НКЦКИ, 2013）。

2016 年的《俄羅斯聯邦資訊安全綱領》，與 2000 年相比，來自資訊及通訊技術（информационно-коммуникационные технологии，以下簡稱 ICT）的威脅清單變得更加清晰，其中包括網路犯罪、恐怖主義以及外國行爲者對俄羅斯受爭議性事件的宣傳等。此外，該文件稱，由於俄羅斯社會「大量引進外國資訊技術」，俄羅斯面臨成爲所謂「資訊武器」目標的風險。根據 2016 年的綱領，國家應該建立「資訊安全保障系統」（Система обеспечения информационной безопасности），通過「保護俄羅斯聯邦在資訊空間的主權」（защита суверенитета Российской Федерации в информационном пространстве）免受外部影響來對抗這些威脅。資訊安全不僅由國家當局提供，還須由國家媒體和 ISPs 提供（Совет Безопасности Российской Федерации, 2016）。

2017 年《2017～2030 年俄羅斯聯邦資訊社會發展戰略》強調「使用 ICT 時優先考慮俄羅斯傳統精神和道德價值觀，並遵守基於這些價值觀的行爲規範」（приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий）。也就是藉由 ICT 來實現俄羅斯傳統價值觀。但是，這些價值觀沒有進一步定義（Президент России, 2017）。

從 2013 年開始的戰略、綱領與文件愈多地提到各種抽象的外國威脅。2019 年「主權網路法」的解釋性備忘錄措辭更爲直接：它將美國列爲對俄羅斯網路持續性的威脅。該法案的制定是「考慮到 2018 年 9 月通過的美國國家網路安全戰略的侵略性質」（с учетом агрессивного характера принятой в сентябре 2018 года стратегии национальной кибербезопасности США）。根據該法案的備忘錄，俄羅斯被美國「毫無根據地指責」委託駭客攻擊，

並受到懲罰威脅。備忘錄暗示，這種懲罰可能會破壞該國的網路。因此，爲了保證「俄羅斯網路的永續運營」，必須採取預防措施。該法案實施了技術手段，以應對網際網路在俄羅斯聯邦境內運行的完整性、可持續性和安全性的威脅」（TACC, 2018）。因此，這些措施是針對外國威脅的預防性防禦策略。因此，作者認爲，俄羅斯對於網路主權的第二個認知是「預防性的防禦策略」。

綜而言之，對 1999 年至 2019 年官方文件中網路政策戰略敘述的分析表明，2011～2012 年左右發生了轉變：從主要將資訊全球化視爲經濟增長的機會和來源，轉變爲到關注因依賴西方技術和開放資訊空間的脆弱性而帶來的威脅。而上述的分析也與 Kolozaridi 及 Shubenkova (2016) 在他們的研究裡整理出官方論述裡關於網路政策的轉變相符合：1994 至 1999 年－幾乎不提及（limited mention）、2000～2011 年－網路作爲良善公益（internet as a “public good”）、2012～2014 年起－對社會及國家安全的威脅（threat to society, the state and security），至今也是如此。

參、俄羅斯網際網路與網路社群

一、俄羅斯網路使用現況

俄羅斯因地大人稀，網路的普及速率較慢，但這 10 年來，俄羅斯的網路連結持續擴大，4G 行動服務的擴張非常迅速。根據非政府研究組織列瓦達中心（Левада-Центр, 2019）的調查，到 2019 年第四季，整體網路普及率達到 76%，每天或每週至少使用幾次網路的俄羅斯人比例約爲 65%。根據俄羅斯 TMT 研究顧問公司（TMT Consulting, 2021），2020 年固定寬頻網路家庭用戶數與 2019 年相比增加了 2.6%，從 3,340 萬用戶增加到 3,360 萬用戶。家庭固定寬頻普及率約爲 61%，但在莫斯科達到 89%。根據國際電信聯盟 2022 年的數據，每 100 名居民中有 24.6 名爲固定寬頻用戶，而每 100 名居民就有 110 名行動寬頻用戶。2023 年俄羅斯網路普及率達 92.2%。俄羅斯政府的國家數位經濟計畫旨在 2024 年爲 97% 的家庭提供速度爲每秒 100 Mbps 或更高的固定寬頻網路連結（ITU Datahub, 2024）。

越來越多的俄羅斯用戶透過行動裝置使用網路。到 2019 年中，行動網

路連結的用戶群增加到 2.606 億，相當於俄羅斯總人口的 175% 以上，這意味著每人有多次行動上網。2019 年行動上網用戶達到 8,520 萬，占所有網路用戶的近 89%（Сухаревская, 2019）。

根據經濟學人智庫的 2021 年俄羅斯網路數據統計，3G 行動網路服務覆蓋率爲 87.7%，而 4G 網路服務覆蓋率也是 87.7%，較 2019 年的 77% 和 62% 大幅增加（Economist Intelligence Unit, 2021）。政府計畫要從 2020 年開始在莫斯科推出 5G 服務（TeleGeography, 2018）。然而，2021 年 3 月，俄羅斯安全理事會仍未同意將最適合 5G 服務的無線電頻率轉移給行動網路營運商，阻礙了 5G 網路的發展。目前，這些頻率是爲俄羅斯軍方保留的。2020 年 11 月，政府批准了到 2024 年的 5G 發展路線圖，其中撥款 2,000 億盧布（26 億美元）用於資助該計畫（РБК, 2020）。2022 年 1 月，Rostec 提出了與政府協議開發 5G 基地台的計劃，計劃於 2024 年開始生產（Медиа, 2022）。然而，當局將截至 2024 年的 5G 網路變頻資金從 430 億盧布（7.04 億美元）減少到 78.5 億盧布（1.3 億美元），這對 Rostec 計畫產生不利影響（Cnews, 2022）。對烏克蘭全面入侵後，美國和歐盟制裁的影響，以及電信設備製造商撤出俄羅斯市場，也對 5G 部署計畫產生了影響。

2023 年 11 月，俄羅斯政府批准了「2035 年電信發展的新戰略」（Стратегия развития отрасли связи до 2035 года）。根據該戰略，俄羅斯政府計劃從 2023 年到 2030 年開發和營運符合 5G 和最終 6G 標準的俄羅斯設備。第二階段，2031 年至 2035 年，政府計畫在所有人口超過 10 萬的城市部署 5G 網路（Правительство России, 2023）。2023 年 10 月，電信業者 MegaFon 與設備製造商 Bulat 簽署了 5,000 個電信基地台的合約（Интерфакс, 2023）。

在莫斯科、聖彼得堡等大都市，醫院、圖書館、學校和公共交通等機構中，公共網路連結相當普遍。但是在農村地區，公共網路連結的可用性仍然有限。

俄羅斯網路連結的成本從 2020 年開始大幅攀升，部分原因是法律實施所產生的成本，包括 Yarovaya 法和主權網路法。[5] 2021 年 11 月，俄羅斯四

[5] 2018 年頒布的《Yarovaya 法》要求業者安裝昂貴的設備來記錄和儲存網路上的使用者流量資料。此外，它還導致流量儲存量逐年增加，這進一步影響了成本。有關主權網路

大行動服務供應商－Beeline、Tele2、MegaFon 和MTS－宣布將不再允許用戶購買無限的網路方案（Cnews, 2021）。到 2023 年，營運商確實已停止提供無限的網路吃到飽方案，儘管有些業者專門提供無限的訊息吃到飽方案。2023 年 5 月，行動服務供應商 MTS、MegaFon、Beeline 和 Tele2 開始對網路「熱點」服務收費。2023 年 9 月 18 日，俄羅斯聯邦反壟斷局（Федеральной антимонопольной службы (ФАС)）要求俄羅斯此「四大」行動服務供應商存在違反反壟斷法的現象，必須停止網路「熱點」服務收費，雖然四大行動服務供應商皆宣稱會遵守規定（РБК, 2023），但是俄羅斯上網的成本仍是維持高昂，短期內不會改變。

二、俄羅斯的網路社群媒體

2000 年代俄羅斯網路社群媒體蓬勃發展，出現了許多社交媒體平臺，虛擬部落格變得與世界其他地區一樣重要。2001 年，協作網路社群維基百科的俄語版推出。2006 年，受歡迎的俄羅斯社群媒體網站（SNS）Odnoklassniki（Одноклассники）和 VKontakte（ВКонтакте，以下稱 VK）創建，主要是模仿美國網路社群平臺 Classmates 和 Facebook（Alexanyan, 2009）。2010 年和 2011 年，Facebook 和 Twitter 進入俄羅斯。

俄羅斯部落格的興起可能與 LiveJournal（Живой журнал）有關。這是俄羅斯投資者 SUP Media（後來與俄羅斯媒體集團 Rambler and Co. 合併）於 2006 年從美國公司收購的第一個大型 SNS。然而，自 2000 年代末以來，該平臺已成爲審查的對象，個人部落格和部落格文章開始被平臺本身和 Roskomnadzor 封鎖。

在政策層面上，俄羅斯部落格的鼎盛時期可以梅德韋傑夫（Dmitry Medvedev）的早期總統任期（2008～2012）聯繫起來。在上任之初，他就將網路作爲現代化計劃的重點之一：「梅德韋傑夫認爲網路不僅是一種手段，而且是他努力使國家〈現代化〉並減少國家依賴自然資源的象徵。」（Toepfl, 2012）梅德韋傑夫是俄羅斯第一位在 LiveJournal 上創建視訊部落

法還要求營運商在其網路上安裝深度資料包偵測（DPI）系統，以過濾使用者的網路流量。同樣的設備也被用來減慢、審查和限制對網站的存取。這會在之後的分析說明。

格並開設 Twitter 帳戶的總統。他也激勵俄羅斯官員熟悉新的資訊通信技術並在工作中積極運用。

2010 年時 LiveJournal 50% 的訪問者來自俄羅斯（LiveJournal, 2010），而該網站的俄羅斯用戶曾經有一度佔據約 45%，其中最有名的用戶包含俄國政治人物、已逝的反對派領袖納瓦爾尼（Aleksey A. Navalny）及前總統梅德韋傑夫，後者則成爲俄羅斯網路發展的象徵。梅德韋傑夫認爲網路發展可以幫助俄羅斯的經濟擺脫對石油及天然氣的依賴。然而經歷過阿拉伯之春、「佔領華爾街」運動及 2011～2013 年國內的大規模抗議活動後，俄羅斯政府意識到自由網路對政權的威脅，因爲該三運動的共同點在於：參與者都運用社群媒體做活動宣傳。

根據 White & McAllister (2014, pp. 72-84) 研究，在 2011～2013 年示威活動中，俄羅斯抗議者用臉書動員的人數大於使用 VK，主要原因是臉書能夠保證用戶的資訊安全；在抗議期間，很多 VK 上的社群被封鎖，其中包含納瓦爾尼創立的社團，後來 VK 的創始人杜洛夫（Pavel Durov）亦承認，當時他迫於來自俄羅斯聯邦安全局的壓力封鎖與抗議有關的社團。有趣的是，除了傳統鎮壓抗議者的方式之外，政府自己也開始利用 Twitter 及 Facebook 來污名化抗議者。

肆、俄羅斯的網路主權發展

在普京於 2012 年開始第三次總統任期之前，俄羅斯網路 Runet 基本上未受到嚴格監管。自 2000 年起，在傳統媒體審查日益嚴格的背景下，網路被視爲政治討論的自由平臺（Richter, 2007）。普京於 2000 年首次就任總統時曾承諾不對網路進行監控，因此直到 2012 年，俄羅斯的網路仍大部分保持未受政府干預的狀態（許菁芸、郭武平，2013，頁 64-69）。

俄羅斯很晚才加入了國家對網路進行更多控制的趨勢，許多學者認爲，俄羅斯網路政策的轉折點是在 2011～2012 年「爭取公平選舉」（“For Fair Elections”）抗議運動之後，才開始收緊網路監管機制，這在很大程度上是由網路上的社交媒體推動的，所以普京政權於 2012 年後開始重視網路主權。

所謂的「主權網路」法案於 2018 年底在俄羅斯推出時，被批評爲「線上鐵幕」（“online Iron Curtain”）（Schulze, 2019）。對該政策的廣泛批評和抗議甚至使俄羅斯立法者和親國家媒體將描述中的措辭從「網路主權」改爲「網路永續」（“sovereign internet” to “sustainable internet”）（Шимаев et al., 2019）。

一、2012 年後俄羅斯對於網路空間的立法

2011 年俄國家杜馬選舉後，2012 年爲了對網路平臺加強監管，俄羅斯政府採取相對應的措施，加強對國內網路企業的管理，透過制定俄戰略性企業名單，擬將廣播電臺、新聞出版機構、知名網路企業均納入管轄。其中，俄羅斯著名入口網站 Yandex、Mail.ru，以及著名社交網路平臺等都被列入國家戰略資產。

2012 年 7 月 30 日，俄羅斯修訂了聯邦法第 139-FZ 號條文「關於修改保護兒童免受損害健康和發展的資訊的聯邦法律及其他法令」（Федеральный закон Российской Федерации № 139-ФЗ «О внесении изменений в Федеральный закон О защите детей от информации, причиняющей вред их здоровью и развитию и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет»），該法是對 2006 年 7 月 27 日通過的第 149-FZ 號聯邦法「關於資訊技術和資訊保護法」（Федеральный закон № 149-ФЗ «Об информации, информационныхтехнологиях и о защите информации»）的修正，旨在建立一個黑名單系統，用於過濾網際網路上的非法內容，例如兒童色情、毒品、極端主義以及其他違反俄羅斯法律的資訊，該黑名單包括大量的 URL 和 IP 位址，並由一個非營利組織負責篩選。[6] 然而，此修正案引發了廣泛批評。許多人認爲，俄羅斯政府藉保護兒童之名，實際目的是加強網路監控和限制言論自由，通過黑名單過濾特定網站的訪問，類似於中國的防火長城。批評者指出，這與當時俄羅斯網路上的抗議者年齡層下降有關，政府試圖借此打壓異議聲音（Sputnik International, 2018）。俄文維基百科甚至

[6] 此非營利組織爲「網路安全聯盟」，將在後續章節說明。

在該法案於 2012 年 7 月 10 日進行國會二讀當天暫時關閉，呼籲網民關注法案的影響，因爲該法案生效後，俄文維基百科可能會被列入黑名單（許菁芸、郭武平，2013，頁 68-69；Википедия, 2012）。

再者，2012 年 7 月 21 日針對國外資金捐助的非政府組織，訂定聯邦法第 121-FZ 號「關於修訂調控爲外國代理人之非營利組織之特定立法」（Федеральный закон № 121-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента»），這就是所謂的「外國代理人（Foreign agent）法案」，任何有接受外國資金的組織或個人皆被定義爲外國代理人，其必須受到俄國政府嚴苛的審查並必須清楚標明其外國代理人之身份，避免外國勢力滲透俄國並藉此煽動人民思想，有些外國代理人網路媒體若有觸及當局政府的利益，也不免除被關閉之可能性，列入外國代理人清單的任何個人或組織都必須在其發布的每一條內容（文字、音訊或視訊）上標註「外國代理人」字樣，字體大小爲其餘內容的兩倍。他們還必須向司法部申報收入和支出。被指定的個人和媒體受到密切監視和控制（State Duma, 2022）。

2013 年 12 月 28 日通過，隔年 2 月 1 日生效，關於俄羅斯聯邦法第 398-FZ 號「關於修訂『資訊、資訊技術和資訊保護』聯邦法」（Федеральный закон № 398-ФЗ «О внесении изменений в Федеральный закон ‹Об информации, информационных технологиях и о защите информации›»），又稱爲 Lugovoy 法（закон Лугового）或「資訊傳播者」法案，該法律允許 Roskomnadzor 立即封鎖傳播大規模騷亂和其他極端主義資訊的網站，無需法院裁決（Российской газеты (RG.RU), 2013）。

2014 年 10 月 14 日，普京簽署聯邦法第 305-FZ 號法案「關於修訂『大眾傳播媒體』法」（Федеральный закон № 305- ФЗ “О внесении изменений в Закон Российской Федерации «О средствах массовой информации»”），對境外股東在俄羅斯媒體中持有 20% 的股份進行限制。同時還規定，非俄羅斯公民（不包括雙重國籍）無權擔任媒體（包括網路平臺）創辦人。時任俄羅斯國家杜馬主席納雷什金（Sergey Y. Naryshkin, Сергей Е. Нарышкин）指出，採取措施限制外國所有者在俄羅斯媒體資本當中所占的股份，將對俄

羅斯的國家主權穩固有一定的作用（TACC, 2016）。

2015 年 5 月 23 日，普京簽署了聯邦法第 129-FZ 號「關於修訂俄羅斯聯邦的特定立法法案」（Федеральный закон № 129-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»），又稱「不受歡迎組織法」（the Law on Undesirable Organizations），該法針對外國和國際非商業組織（Non Commercial Organizations，之後簡稱 NCOs）及其在俄羅斯的合作夥伴。根據「不受歡迎組織法」，如果檢察長或副檢察長認爲外國或國際 NCOs 對國家安全構成威脅，他們可以宣布該組織爲「不受歡迎組織」。俄羅斯禁止「不受歡迎組織」的任何活動，所有參與此類活動的人都將受到行政和刑事處罰（Российской газеты (RG. RU), 2015）。[7]

2016 年 7 月 6 日普京簽署了兩個法案：聯邦法第 374-FZ 號「關於修訂打擊恐怖主義聯邦法和俄羅斯聯邦關於制定額外措施以打擊恐怖主義和確保公共安全的某些立法法案」（Федеральный закон № 374- ФЗ «О внесении изменений в Федеральный закон ‹О противодействии терроризму› и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»）和聯邦法第 375-FZ 號「關於在制定反恐怖主義和確保公共安全的附加措施中修改俄羅斯聯邦刑法和俄羅斯聯邦刑事訴訟法」（Федеральный закон № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный

---

[7] 2021 年 6 月 28 日普京再次針對「不受歡迎組織」，簽署聯邦法第 232-FZ 號「關於修訂行政處罰法典」（Федеральный закон № 232-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»）：加重參與「不受歡迎組織」的行政責任。這意味著任何與「不受歡迎組織」合作的個人或組織都可能受到行政處罰，無論該活動發生在俄羅斯領土境內還是國外，如果當局認爲該組織「直接違背俄羅斯聯邦的利益」。俄羅斯公民仍然可以因在俄羅斯領土境內與此類組織合作而受到刑事起訴，而且，關於「領土」的定義已經擴大到網際網路空間（Официальное опубликование правовых актов, 2021）。而專門從事調查報導的網路媒體機構是克里姆林宮最喜歡的目標。已有三個已被列入「不受歡迎組織」和「外國代理人」名單：The Insider（反對派媒體）；Bellingcat（由研究人員、調查員和記者組成的網路媒體）；和 Istories（網路媒體）（Reporters Without Borders (RSF), 2024）。

кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»），兩項修訂法律又稱「Yarovaya」法案（Закон Яровой），[8] 其中包括許多嚴重損害線上隱私權和言論自由的條款，包含擴大執法機構的權利。其中一些條款加大了網路上的資訊公開程度，並造成人民的不安，其內容爲要求在俄的科技公司需存儲俄羅斯公民的用戶數據，包括要求電信公司保留語音訊息、短訊、聲音、影片等訊息的傳輸 3 年，而訊息本身僅保存 6 個月。Telegram、線上論壇、社交媒體平臺以及任何其他使用戶能夠相互交流的服務等數據及對話資料須保存至少 1 年，包含發送訊息的時間，與發送者及接受者的位置與詳細訊息等。網路和電信公司還被要求在沒有法院命令的情況下須按時向當局報告自己的相關數據以利提供安全的服務，包含電子郵件、公司加密金鑰、需解碼之不透明訊息等（Кузьмин, 2016）。

2017 年俄羅斯政府推出了多項從技術層面維護網路空間主權的法規，如 2017 年 7 月 26 日簽署的聯邦法第 187-FZ 號「關鍵資訊基礎設施安全法」（Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»）禁止沒有取得政府「資訊傳播者」資格的公司對一般人民提供傳遞訊息的服務，法律要求這些公司都得透過手機來識別用戶（類似實名制）。

2017 年 7 月 29 日簽署聯邦法第 276-FZ 號「關於對關於資訊、資訊技術和資訊保護的聯邦法的修正」（Федеральный закон № 276-ФЗ «О внесении изменений в Федеральный закон Об информации, информационных технологиях и о защите информации»）又稱「虛擬私人網路（Virtual Private Network，之後簡稱 VPN）法，又稱「VPN 法」，是限制使用匿名代理服務器和 VPN 的法律，允許俄羅斯政府可以直接指定接受國外資助的媒體機構爲「外國代理人」，該法還授權俄羅斯當局封鎖線上內容，包括被視爲發布「不受歡迎」或「極端主義」內容的社交媒體，其旨在防止外國代理人業務，包括 VPN 和匿名程序，如 TOR（實現匿名通訊的免費軟體）或 Opera

[8] 「Yarovaya」法案是以其主要提倡者、議會下議院、執政的統一俄羅斯黨的國家杜馬成員雅羅瓦亞（Irina Yarovaya, Ирина Яровая）的名字命名。

（VPN 供應商）等網站曾經提供 VPN 服務讓人民可以訪問那些遭俄羅斯政府禁止的網站，而在此法條推出之後該 VPN 供應商也被視爲非法，法案同時還禁止搜尋此類關鍵字。該法律授權給 Roskomnadzor，使其能夠封鎖提供有關如何繞過政府禁止網站的相關媒體與網頁（如下載 VPN 的網頁）。它還授權給俄羅斯的執法機構，包括內政部和安全委員會，在確定違反該法律後，Roskomnadzor 將會將其公司（網站）劃入黑名單，禁止其在俄羅斯繼續提供可能的資源（Роскомсвобода, 2017）。[9]

由於 2017 年禁止 VPN 的使用和網路匿名（第 276-FZ 號）的法律，沒有規定對違規行爲要進行怎樣的罰款，因此 2018 年 6 月 27 日簽署的聯邦法第 155-FZ 號「關於行政處罰法修正案」（Федеральный закон № 155-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»）則引入了處罰措施，對違反「禁止 VPN 和網路匿名者」法律者，最高罰款爲公民 5,000 盧布，官員最高 5 萬盧布，但法律實體最高可被罰款 70 萬盧布。

因此，2018 年 Roskomnadzor 開始攔截上百萬個國家安全部門無法得到解密鑰匙的 IP 位址，這個攔截服務便用於銀行、網路購物平臺和搜尋引擎等。這樣促使更多網路使用者使用 VPN 去繞過這些阻礙，然而俄國官方也採取相應措施來對 VPN 進行相對應之管制。於同年政府更是制定法令要求國外訊息服務供應商與俄國電信業者簽署協議，強制要求無論新用戶或是舊用戶皆要用手機號碼進行身份認證，若沒有進行身份認證的匿名帳戶便無法使用此通訊軟體；有些使用者試圖購買非官方的 SIM 卡或租用短期的門號以便規避身份認證的程序。這項規範將會嚴重危害俄國網路使用者的資料保密性。

2019 年 3 月，Roskomnadzor 要求 VPN、匿名網站和搜索引擎營運商

---

[9] 2018 年 4 月，Roskomnadzor 阻止數以百萬計的網路 IP 企圖使用 VPN 來進入遭俄羅斯政府封鎖的網站，這也導致公司 Telegram 暫停了在俄羅斯的服務，同時與其相關的銀行、線上購物與搜尋皆造成中斷，這反而使俄羅斯更多的人民使用 VPN 來連上這些網站，一些 VPN 供應商報告說，俄羅斯在這一段時間的 VPN 銷售額增長了 1,000%。Roskomnadzor 的反應則是封鎖了 50 多個提供人們使用 Telegram 的 VPN 程式（Pertsev, 2018）。

確保他們的連線都必須要通過聯邦政府設立好的網路節點，以利 Roskomnadzor 定期更新禁止網站黑名單的資料。同樣在 3 月，該機構公布了透過更有效的自動控制系統，監控整個俄羅斯的網路使用狀況及網站的違法與否，而不是手動追蹤每個被封鎖網站的狀況。2019 年 6 月，Roskomnadzor 責令在 1 個月必須要改善各家網路公司的守法情況（包含使用相關節點、封鎖網站、不使用 VPN 等），並點名了 10 家相關的 VPN 供應商，其中包括俄國揚名國際的著名電腦防毒程式提供軟體：卡巴斯基（Kaspersky），因此卡巴斯基被迫遵守法律；而另一個 VPN 供應商 Avast SecureLine 則決定離開俄羅斯市場。然而仍有一些 VPN 協定與匿名網站依然在俄羅斯市場中營運，依舊免費提供給人民連結被俄 Roskomnadzor 封鎖的網站的通道，如 AmneziaWG、VLESS + Reality、VLESS over WS 和 CDN、Shadowsocks-2022、OpenVPN 或 Shadowsocks over Cloak，但是未來是否能繼續運作是不定數（Shakirov, 2024）。

二、2019 年《主權網路法》

現在已經很難追溯到俄羅斯「網路主權」這個概念何時出現，但我們可以從普京的一次演講中看到這個概念的輪廓。在 2014 年的媒體大會上普京說網路是美國中央情報局的發明，因此，爲了保證國家安全，應該將所有的網路數據從美國移到俄國境內，並有意通過實際舉措維護國內網路免遭「斷網」威脅（Путин, 2014）。俄羅斯自始至終認爲，國家網路主權享有對本國網路主體、網路行爲、網路設施、網路資訊、網路治理等的對內最高管理權和對外的獨立權。因此有些人會將「網路主權」與「主權民主」這兩個概念綁在一起。「主權民主的實質是維護國家主權、奉行獨立政策、不照搬西方模式，走俄式的發展道路，是俄羅斯政治民主化的階段性理念」（劉瑩，2014）。至於 Runet，它同樣不應該受外來的影響，Runet 只有俄羅斯當局與人民有權利發展、監督、管理的網路空間。

2019 年 11 月，普京頒布聯邦法第 90-FZ 號《關於通訊》和《關於資訊、資訊技術和資訊保護》的一系列修訂法案（Федеральный закон № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”»），

爲俄羅斯境內網路的集中國家管理創建了法律框架。俄羅斯網路新法規，其中大部分於 2019 年 11 月 1 日生效，部分於 2021 年 1 月生效，該一系列法案引起了國際相當的關注，並被公開描述爲俄羅斯的《主權網路法》。（Официальное опубликование правовых актов, 2019）「網路主權」理念是俄羅斯《主權網路法》的理論支撐，《主權網路法》旨在通過立法保護俄羅斯的網路主權不受侵犯。

有些人認爲除了 2011～2013 年的抗議活動之外，另一個導致該法律出現的事件是美國情報部門前僱員斯諾登（Edward Snowden）在 2013 年揭露了美國國家安全局（NSA）的大規模情報監聽項目。Stanislav Budnitsky (2021) 認爲俄羅斯通過該法案只是想要限制美國科技巨頭對網路的壟斷。

2019 年《主權網路法》主要內容可以概括爲以下四個方面：

1. Roskomnadzor 被賦予重要職權：一是，負責制定替代網域名稱系統的設計要求、建設流程和使用規則；二是，對俄羅斯境內所有網路流量實行全面監控；三是，負責維持 Runet 的穩定性，必要時可切斷一切俄羅斯網路與外部的聯繫。此外，還要求 Roskomnadzor 下設實施機構－「公共通訊網路監控中心」（Центр мониторинга и управления сетями общего доступа），搭建負責網路資訊的集中監控系統。每個 ISPs 都需要向 Roskomnadzor 提供網絡圖表（network diagram）。中心將監督國內 ISPs 安裝指定工具，對國內 ISPs 的通話資訊、傳輸內容進行分析，以確保俄羅斯網路的安全。
2. 新建網路基礎設施：創建一個獨立的國家區域網路系統，一個替代的網路域名系統（DNS）和自動位址解析系統，接收全國的二階域名，以便在緊急時刻取代現有網路域名系統服務系統，確保俄羅斯在無法連接國外伺服器時，仍能正常訪問本國網站。同時，要求俄羅斯境內涉及重大國家利益的相關機構網路應全部使用該系統。
3. 透過建立路由節點審核登記制度：所有通訊接入節點都須由 ISPs 通報 Roskomnadzor 審核備案，所有與外國網站間的流量交換通過的流量交換點必須登記註冊。規定俄羅斯 ISPs 有義務向監管部門展示，如何將網路資料流程引導至受俄政府控制的路由節點，使國內網路資料傳輸不經過境外伺服器，最大程度減少俄羅斯使用者資料向國

外傳輸。ISPs 有義務確保在發生威脅時集中管理流量的可能性，如應當在確定傳輸流量來源的通信網路上安裝技術設備「威脅防護技術措施」（“технические средства противодействия угрозам”, ТСПУ，之後簡稱 TSPU），TSPU 旨在使用深度封包檢測（deep packet inspection, DPI）技術（按資料封包內容對流量進行深度過濾）來過濾流量並阻止禁止的資源，Roskomnadzor 非正式地將該裝置稱爲「黑盒子」。對於根據相關聯邦法律進行採購的州、市、公司資訊系統的營運商，禁止使用位於俄羅斯聯邦境外的資料庫和技術方法。還規定俄羅斯國家機關和國有企業在網路上的資訊，將得到額外加密保護。

4. ISPs 有義務登記並使用這些由政府制定的通路，Roskomnadzor 將會禁止人民連結未經俄羅斯政府許可（被俄羅斯政府禁止或封鎖）的網站。組織開展脫離國際網路的演習，爲政府、ISPs 和網路行業內的關鍵人員提供培訓和演練，提升威脅識別和制定應對措施的能力（許菁芸，2023，頁 286-293；TACC, 2019）。

伍、俄羅斯網路過濾、監控設備及其效果

主權網路法案在國家杜馬通過之後，俄國網路便開始受到各種限制，而最常用的手段爲監控及封鎖。俄羅斯對網路的管控其中一個特點在於所謂的「技術及法律眞空」（techno-legal vacuums）：大部分與網路限制相關的法案缺乏具體的技術說明，ISPs 主要考慮經濟利益，因此他們需要「滿足」的對象不僅是政府，而更多是他們的客戶，因此常常與政府間的互動，會上有政策、下有對策，陽奉陰違（Ermoshina et al., 2022）。

一、SORM 系統及監控設備

自 20 世紀 90 年代以來，俄羅斯當局一直致力於建立並完善由設備、伺服器和流量監視系統所組成的網絡監控設備，即所謂的「調查行動運作系統」（СОРМ, Система оперативно-разыскных мероприятий，以下簡稱爲 SORM），SORM 是俄羅斯當局用於合法監聽電話、電子郵件、網際網路活動等資訊的系統，建立於 1995 年。當局規定所有 ISPs 必須強制安

裝該特殊監控系統，並使該國情報機構──聯邦安全局（FSB）能汲取並監控俄羅斯網路上的所有內容。2000 年普京上台後增設規定，除了俄羅斯聯邦安全局之外，其他安全部門（如警察、邊境巡警和海關、稅警、內政部等）都可以使用該系統。也就是說，網路從一開始發展就受到俄羅斯聯邦安全局（FSB）的監控。他們使用 SORM，並透過它監聽電話、檢查電子郵件、網路活動等等。SORM 系統目前發展至三代，SORM-1，開始使用於 1995 年，具電話監聽功能；SORM-2，於 1999 年啓用，增加監控網路之功能；SORM-3，始於 2014 年，除上述以上功能外，增加檢查後設資料（metadata）之功能，包含如時間、地點及訊息的內容，並具有深度封包檢測能力（DPI）。依照俄羅斯法律規定，所有的 ISPs 必須安裝 SORM 系統並費用自付，因此也導致很多較小的 ISPs 被迫退出市場。SORM 系統主要是由兩個部分組成的：第一個，位於當地俄羅斯聯邦安全聯邦分局的終端機（terminal）；第二個，位於 ISPs 的流量存儲系統。曾經有很長的一段時間，由於這些終端機不具互聯性（interoperability），這意味著它們不能直接連接到 ISPs，導致幾個供應商壟斷了不同地區的市場（Maréchal, 2017, pp. 33-35）。[10]

2016 年通過的「Yarovaya」法案受到來自許多 ISPs 的批評後，在 2018 年又一次修改：ISPs 必須存儲所有數據（後設資料爲期 3 年、語音、圖片及訊息爲 30 天），並每年將存儲時間延長爲 15%。然而，該法案更引起 ISPs 的反彈，主因在於安裝相關設備（包含 SORM）的成本過於高昂（最便宜爲 105,000 盧布、最貴爲 91,383,000 盧布）。有時候較小的 ISPs 爲了降低安裝 SORM 的費用而選擇聯合一起購買該設備。除此之外，認證程序相當複雜（除了法律層次之外，還要由不同機構進行一系列測試），並需要政府官員的參與，因此導致俄羅斯的網路環境更趨惡劣（Ermoshina et al., 2022）。

二、網路安全聯盟（Лига безопасного интернета）的運作

網路安全聯盟是一個俄羅斯類官方組織，旨在審查網路。該組織由 Marshall Capital Partners 基金（創立者爲馬洛費耶夫（Konstantin Malofeev,

[10] 如下諾夫哥羅德 Norsi-Trans、聖彼得堡的 Spectech 等。

Консантин Малофеев）[11]）和該國最大的電信營運商和科技公司，包括 Rostelecom、Beeline、卡巴斯基和 Mail.ru Group 合作，於 2011 年 1 月建立。該組織的最初目標是「消除網路上的有害內容」，例如兒童色情、與毒品有關的資訊以及與自殺有關的內容。然而，隨著時間的推移，它的範圍大大擴大，並開始針對任何被認爲對克里姆林宮有害的內容，包括 LGBTQ+ 內容和獨立音樂家。自 2017 年以來，該組織一直由米祖琳娜（Екатерина Мизулина）領導。[12]

2011 年，該組織成立了一個跨區域的青年組織「網路衛隊」（«Кибердружина»），該組織負責查找網路上的危險內容（Малахов & Балашова, 2011）。2011 年 5 月，網路安全聯盟跟俄羅斯最大的社群網站 VK 簽署了合作備忘錄。根據備忘錄內容，該組織的志願者可以在 VK 上尋找非法內容，並且將相關的訊息交給執法機關（Lenta.ru, 2011）。2012 年 7 月 28 日普京簽署第 139-FZ 號聯邦法律「關於修改保護兒童免受損害健康和發展的資訊的聯邦法律及個別法令」，根據該法律規定，網路安全聯盟會定期列出網站的「黑名單」跟「白名單」，被納入黑名單裡的網站會被 Roskomadzor 封鎖。

2014 年 8 月，該組織的執行董事達維多夫（Денис Давыдов）宣布，他們旗下的「網路衛隊」除了在網路上尋找不當內容以外，還要負責阻止資訊戰。他表示，「網路衛隊」的已有兩萬多來自俄羅斯、獨立國協跟東歐國家的志願工作者（TACC, 2014）。

近幾年來，網路安全聯盟開始以保護俄羅斯網路爲名，大力針對俄國娛樂圈的管制外，[13] 更提出禁止影音平臺 YouTube 在俄羅斯境內使用

11　馬洛費耶夫是俄羅斯企業家、網路電視平臺«Царьград ТВ»的創辦人、「俄羅斯世界」（Русский мир）積極的推廣者。

12　米祖琳娜是俄羅斯聯邦「公眾院」（Общественная палата）的成員、聯邦委員會議員伊蓮娜・米祖琳娜（Елена Мизулина）女兒。2024 年 1 月，歐洲理事會對網路安全聯盟及米祖琳娜實施制裁，原因是網路安全聯盟「幫助俄羅斯政府執行審查制度」，而米祖琳娜作爲組織領導人「有責任爲嚴重侵犯言論自由負責」（The Record from Recorded Future News, 2024）。

13　例如，2022 年 7 月，俄羅斯著名的 Youtuber 與記者 Yury Dud（Юрий Дудь）被該組織舉報後，被法院以向未成年人宣傳非傳統性關係的罪名判處罰款 1,200,00 盧布，原因

（EurAsia Daily, 2022）或者想要將 LGBT 運動列爲「極端主義組織」（РАПСИ, 2022）。

自從俄羅斯在烏克蘭開始實施特別軍事行動以來，網路安全聯盟也開始在網路上尋找相關的假新聞。根據該組織的報告，光是從 2022 年 2 月至 2022 年 7 月他們就發現了有一千六百萬多則「污衊俄羅斯的假新聞」（Коммерсантъ, 2022b）。

三、Roskomnadzor 過濾網路與封鎖

早在 2008～2009 年 ISPs 時常被要求刪除與賭博或兒童色情相關的內容，但在 2014 年烏克蘭危機之後，俄羅斯聯邦安全局發佈了正式的黑名單：所有與極端主義、兒童色情、自殺、毒品、侵犯版權及呼籲上街參與抗議活動相關的網站進入該黑名單。

當時該過濾系統受到了全國網民的批評，因爲除了 Roskomadzor 之外，還有許多其他政府機構有權決定何種內容屬於非法，並通常利用該法律上的漏洞針對反對派。

電信業者被 Roskomadzor 要求有義務自費建立一個封鎖系統，並且必須封鎖 Roskomnadzor 黑名單登記冊中出現的網路資源。ISPs 通常被要求封鎖這些網站的網址（URL），但隨著黑名單的內容愈加擴大，封鎖過程也相對緩慢，爲解決該問題，2017 年起 Roskomnadzor 要求 ISPs 安裝高達 84,000,000 盧布，名爲 Revizor 的系統，該系統監控電信業者可用的資源，並僞裝成訂戶，故意在 Roskomnadzor 的違禁黑名單登記冊中請求連結資源。如果眞的給與連結資源，ISPs 就會被處以高額罰款。然而，如同以上提及的 SORM 系統，安裝該 Revizor 的成本過高，加上效率偏低，許多 ISPs 選擇繼續用其他方式進行封鎖。這時候市場上出現一些有能力提供相關技術的公司（如 SKAT 或 Carbon Reductor）。爲了吸引更多用戶，一些 ISPs 甚至會安裝類似於 VPN 的軟體，安裝之後，用戶可以連結被列入黑名單的網站，而 Revizor 系統不會發現（Russia. Post, 2023）。

自從俄國政府在 2019 年通過「主權網路法」之後，2020 年所有 ISPs

是他採訪了一位公開的男同志藝術家（Коммерсантъ, 2022a）。

皆被要求安裝 TSPU。到了 2021 年，政府首次全面使用該技術對 Twitter 進行所謂的 throtting（動態時鐘頻率調整，即限速）。有些研究者爲了了解該設備能識別哪些網路流量的類型進行了一系列實驗後發現，TSPU 能識別的網路協定包含 SNI、IP 及 QUIC。另外，TSPU 主要封鎖來自俄國境內的連結，並主要監督試圖連到資訊網站（如部落格、新聞媒體、社群媒體）的用戶。雖然目前用戶還能夠利用 VPN「翻牆」，繞過 TSPU 設立的限制，但以該技術所發展的速度及規模來看，作者對於未來的情況保持較悲觀的態度。

四、網路監控和審查的效應

(一) 俄羅斯近半人民對網路審查持正面態度

最近十年來，俄羅斯網路自由度呈現下降趨勢，而其背後原因在於許多與網路限制相關法律的出現。要注意的是，俄羅斯作爲「選舉式威權體制」國家（electoral authoritarianism）投入大量精力來證明其網路政策具有合理性，並符合人民需求。例如，2017 年杜馬以回應社會關於社群媒體上出現「死亡社團」[14] 的擔憂爲理由通過了一項與網路相關的法案（State Duma, 2017）。官方媒體作爲政治訊息傳播的主要載體通常協助政府塑造主流輿論，「包裝」政府政策，使得公民覺得杜馬所通過的法案有利於他們的利益。

根據 Pigman (2019) 的看法，俄羅斯政治菁英在制定與網路相關的政策時，主要考慮到三個網路威脅（cyberthreats），包含：對政權安全、對公共安全及對社會規範和價值的安全。第一個涉及到「外來勢力」透過數位方式（digital means）干涉內政，並有可能導致政變；第二個強調網路所提供

[14] 所謂的「死亡社團」是指圍繞藍鯨遊戲的陰謀論，這是一個在網際網路和媒體上流傳的說法。據稱，一款名爲藍鯨的遊戲會通過心理操控，誘導參與者在 50 天內完成一系列自殘任務，並在最後一天要求他們自殺。這一陰謀論最早於 2016 年 5 月出現在俄羅斯《新報》（Новая газета, 2016）的一篇名爲「死亡社團（18+）」（Группы смерти (18+)）的文章中。該文章將多起毫無關聯的青少年自殺事件與俄羅斯 VK 社群平臺上的「F57」組織聯繫在一起。然而，這篇報導後來遭到批評，因其試圖在缺乏因果關係的情況下強行建立聯繫，並且沒有證據顯示這些自殺事件是集體行爲的結果。

的自由會被恐怖主義組織或其他罪犯濫用，最後威脅到公共安全；第三個指網路上所傳播的令人反感或不符倫理道德的內容會破壞社會秩序。俄羅斯政府成功地利用這三種論點來「框架化」（framing）他們所通過與網路相關的法案。根據多個民調中心於 2016～2017 年的調查，49% 俄羅斯人支持網路審查，而 51% 相信政府列出「網站黑名單」有助於維持政治局勢的穩定（Левада-центр, 2016; ВЦИОМ, 2017）。從以上民調結果顯示，以俄羅斯官方媒體作爲唯一資訊來源（主要指電視新聞）的俄羅斯人對於政治審查表示更多的支持。

(二) 網路價格逐漸高昂且更封閉

對於 ISPs 而言，大規模網路監控最直接的後果是網路價格不斷地飆升。根據 FSB 的數據，全部相關的費用已達到 60 億美元。「Yarovaya」法案要求存儲一定期限內的資料不是唯一導致網路價格走高的關鍵因素，更由於 ISPs 所購買的大部分設備都是來自進口，俄羅斯在 2014 年遭遇西方的經濟制裁後在很大程度上受到影響，必須以更高的價格購買。

除此之外，當俄國網路由開放走向封閉的時候，許多專家開始討論俄國政府未來將 Runet 隔絕於世界之外的可能性。根據主權網路法，俄羅斯計畫建立自己的網域名稱系統（Domain Name System, DNS），如果位於國外的網路伺服器被中斷，ISPs 將會改變「訊息流」（information flow）的方向，使它直接連接到政府控制的路由點（routing points）。俄羅斯在 2018 印古什共和國（The Moscow Times, 2018）及 2019 年莫斯科的抗議活動期間已成功地切斷過境內特定地區的網路（Netblocks, 2019）。

不過，根據 SkyDNS 的說法，由於 Runet 目前過於依賴全球網路，所以未來近幾年不會看到它走向「中國網路模式」，因爲俄羅斯的網際網路從來都不是一個獨立的系統。俄羅斯擁有超過 5,000 個自治系統（Autonomous system, AS）、41 個網際網路交換點（Internet Exchange Point, IXP）、多個網際網路閘道器（international gateway）以及完全去中心化的 ISPs 市場，完全隔離 Runet 幾乎是不可能的，而 Telegram 封鎖失敗證明此觀點。[15]

[15] 2018 年 Telegram 拒絕按照俄羅斯法律的要求，允許政府訪問該平臺的加密數據。因

（Ermoshina et al., 2022; Phokeer, 2024）即使如此，俄羅斯封鎖網路政策仍舊會持續並進一步加重實施。

(三) 對網路用戶及異議人士的限制

根據自由之家（Freedom House）2022 年網路自由（Freedom on Net）報告，2017 年在俄羅斯每日有 244 網頁被封鎖，每 8 天就有人因涉及到網路犯罪行爲被逮捕而被判有期徒刑。最常見的罪名爲兒童色情、同性戀、毒品、分裂主義、恐怖主義之宣傳以及假訊息傳播，2021 年俄羅斯共有 162,295 個 IP 位址被封鎖（Freedom House, 2022）。2022 年入侵烏克蘭之後，俄羅斯當局加強了封鎖可能含有批評當局或入侵內容的網站和社群媒體平臺。據監測網路審查的非政府組織 Roskomsvoboda 稱，截至 2025 年 5 月，俄羅斯約有 223 萬個網路資源被封鎖（Роскомсвобода, 2025）。

除了逮捕並判刑之外，其他政府使用的能夠讓異議人士噤聲的手段還有罰金及封鎖。例如，莫斯科法院曾經有過好幾次下令納瓦爾尼刪除他在 YouTube上發佈的影片（關於前總統梅德韋傑夫或俄國寡頭傑里帕斯卡的貪污紀錄片後）。2021 年，法院還下令 Google 和 Apple 刪除納瓦爾尼的「智慧投票」（Smart Voting）應用程式（App）。納瓦爾尼及他的團隊之所以能夠成功避開政府的封鎖與限制，其中一原因是他們一直尋找法律上的漏洞以及利用各種各樣的技巧來迴避政府在網路上給他們設置的阻礙。例如，2014 年，納瓦爾尼的 LiveJournal 部落格被封鎖之後，納瓦爾尼團隊註冊了一個有很多子域名（subdomain）的域名（domain），因爲政府所使用的封鎖機制沒辦法封鎖所有的子域名。第二步是使更多用戶註冊自己的子域名。最後這 150～200 個子域名組成一個名爲「納瓦爾尼紅色按鈕」（Big Red

---

此，4 月俄羅斯政府封鎖了 Telegram，Telegram 卻使用了各種應變方法，包括透過 Amazon 和 Google 的雲端服務和路由器，以保持應用程式的正常運行。Roskomnadzor 發現自己處於尷尬境地，不得不封鎖至少 1,800 萬個 IP 位址，無意間卻干擾了銀行、交通、新聞網站和其他服務，引起了民眾的示威抗議。Amazon 和 Google 曾表示，俄羅斯政府曾要求取締 Telegram 用來繞過政府監控的「域名前移」技術（Domain Fronting），該技術透過在不同應用層使用不同域名的方式逃避審查。政府卻未能成功封鎖 Telegram，表明俄羅斯政府的想要完全限制網路是很難實現（Guardian, 2018）。

Button of Navalny）的系統。每次按紅色按鈕之後，它會跳到其中一個子域名的網頁，而用戶由此可以看到納瓦爾尼的部落格（Soldatov & Borogan, 2015）。

陸、2022 年俄烏戰爭後之網路與資訊控制

一、更多網路限制的立法

2022 年俄羅斯對烏克蘭採取特別軍事行動後，西方媒體與網路上有關戰爭的各種訊息爆炸，充斥全俄。普京隨即於 2022 年 3 月 4 日簽署了聯邦法第 32-FZ 號「關於修改俄羅斯聯邦刑法和俄羅斯聯邦刑事訴訟法第 31 條和第 151 條」（Федеральный закон № 32- ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации»），懲罰任何傳播「假新聞」（fake news）的人，尤其是傳播有關俄羅斯聯邦軍隊的「假新聞」，除了處以最高額 500 萬盧布的罰鍰外，最高可判處 15 年監禁。同日，Roskomnadzor 封鎖了多家外國媒體，包括 BBC News Russian、美國之音、RFE/RL、Deutsche Welle 和 Meduza，以及 Facebook 和 Twitter（Reuters, 2022a; Moscow Times, 2022a）。[16]

2023 年 3 月 18 日通過聯邦法第 75-FZ 號「關於修改通訊法第 56.2 條」（Федеральный закон N 75-ФЗ “О внесении изменений в статью 56.2 Федерального закона “О связи”），要求 ISPs 將語音訊息、簡訊、圖像、聲音、視訊或其他通訊資訊傳輸的數據保存三年，進一步提高用戶的成本（КонсультантПлюс, 2023）。

2022 年 3 月 30 日普京發布第 166 條總統令「關於確保俄羅斯聯邦關鍵資訊基礎設施技術獨立和安全的措施」（Указ Президента Российской

[16] 而在強大壓力下數間俄羅斯獨立媒體被迫暫停營運，例如《新報》（Новая газета），外媒陸續宣布暫停在俄羅斯的採訪、報導。俄羅斯獨立媒體中剩下的 2 家旗艦，自由主義的莫斯科回聲電臺（Ekho Moskvy）和數位化媒體新貴「Дождь」（Dozhd）也因爲確實報導烏克蘭問題而受到當局圍捕，於 2022 年 3 月停播。

Федерации от 30.03.2022 № 166 “О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации”），規定政府機構必須在 2025 年之前完全放棄使用外國軟體，促使俄羅斯加快實施「進口替代」政策，並鼓勵當地企業和國有企業轉向國內技術開發與使用（Официальное опубликование правовых актов, 2022）。[17]

2023 年 7 月，國家杜馬通過聯邦法第 406-FZ 號《資訊、資訊科技與資訊保護》和《通訊》法修正案（Федеральный закон от 31 июля 2023 года № 406-ФЗ “О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и Федеральный закон “О связи”）。規定從 2023 年 12 月 1 日起，禁止在要求用戶使用外國電子郵件服務進行註冊和身份驗證的俄羅斯網站上進行註冊。對於身份驗證，也禁止使用透過國外服務註冊的帳戶，例如 Google 或 Apple ID。該法律規定，可以透過電話號碼、透過政府服務入口網站、透過在俄羅斯服務中註冊的電子郵件或使用俄羅斯聯邦公民或法人實體擁有的其他 ID 服務（例如，透過 Yandex、VK、Odnoklassniki 帳戶）進行註冊。2023 年 9 月 1 日，《通訊法》新修正案生效。特別是涉及擴大終止和撤銷 ISPs 營業許可證的理由。不遵守透過 TSPU 傳輸流量的方案現在可能會導致 ISPs 許可證的終止（Ведомости, 2023）。

2023 年 11 月 16 日，國家杜馬一讀通過允許強力部門從數據庫中獲取數據的法案。強力部門（силовые ведомства）可以向任何資訊系統（如 ISPs 或通訊運營商）要求提供與這些部門員工相關的資料，以便進行確認、取出、刪除，以及恢復被刪除的資料。這些員工除了來自國防部、俄羅斯聯邦安全局、內務部、對外情報局（CBP）等強力部門，還包括法官。值得注意的是，當該法案還在處於審議階段時，俄國大數據協會（Accоциация больших данных，包含«Yandex», «VK», «Rostelecom»等公司）對此提出批

[17] 俄羅斯高達 90% 的企業和國家客户都在使用微軟（Microsoft），微軟已停止爲俄羅斯實體續訂其產品授權。目前俄羅斯最受歡迎的 Windows 作業系統替代品包括 Astra Linux，最初是爲該國的軍事和情報機構開發的（The Record from Recorded Future News, 2023）。

判，認爲這將會造成一定的商業風險，而負責個資保護的公司爲了避免資料外洩，需要增加額外的費用。俄國銀行協會（Ассоциация банков России）同樣表示反對，因爲這會違反憲法賦予俄國公民的權利，而法案裡的「恢復已刪除資料的權力」將會造成資訊安全威脅（Коммерсантъ, 2023; ТАСС, 2023）。

二、社群媒體的控制

(一) YouTube vs RuTube

YouTube 是美國 Google 旗下的影片分享網站。依據 Statista (2021) 報告，YouTube 是俄羅斯最受歡迎的平臺，而它的滲透率高達 85.4%。YouTube 之所以如此受歡迎的原因，首先是該公司的政策，當俄羅斯政府要求 Google 或者 YouTube 移除內容的時候，該公司通常不會滿足這些要求，而是先會自己進行審查，確認每項要求符合適用法律規定。所以儘管 Roskomnadzor 愈來愈頻繁地向 Google 提出各種關於有必要審查其內容的要求，但同時它被拒絕的次數也在增加。

其次，Google 在 2014 年關閉其在俄羅斯的分部。Nathalie Marechal (2017) 指出，在沒有俄羅斯分部的情況下，美國平臺有更多「迴旋餘地」來拒絕 Roskomnadzor 或者其他俄羅斯政府機關的請求。而且最近十年來，俄羅斯人對電視作爲訊息來源的信任度從 74% 下降至 43%（ФОМ, 2022）。

俄羅斯政府意識到這一點之後開始推廣早在 2006 年成立的 RuTube，但目前該平臺不具有任何競爭力。俄羅斯獨立調查媒體「重要記事」（Важные истории, 2022）[18] 及其他學者在他們的調查裡詳細地描述政府如何透過各種方式試圖吸引俄國網紅用 RuTube。然而，在 2017～2019 年，RuTube 主要的內容侷限於俄氣傳媒集團（Gazprom Media）旗下電視頻道

[18] 2021 年 8 月 20 日，俄羅斯司法部將在拉脫維亞註冊、出版《重要紀事》以及《重要紀事》主編的法人實體《IStories fonts》列入外國代理人媒體黑名單，納入的原因是與其他先前被視爲外國代理人的新聞出版物進行合作。2022 年 3 月 5 日，該刊物創辦法人實體《IStories fonts》被俄羅斯司法部列入不受歡迎組織名單。3 月 11 日，Roskomnadzor 封鎖了該《重要紀事》的網站，因爲該網站「發布了有關俄羅斯入侵烏克蘭領土不具社會意義的不可靠的資訊」（Интерфакс, 2022）。

（TNT、Match TV、Friday!）製作的主流電視節目。2022 年俄烏戰爭後，RuTube 與政府的緊密連結更導致對使用者的內容審查，而這將會直接影響到平臺上的公民記者。親政府的 RuTube 頻道，它們不是滿足觀眾對與官方不一樣訊息來源（alternative information）的需求，而是以滿足政府的要求爲優先。

(二) VK 國有化與管控

俄烏戰爭爆發後，俄國開始加強對國內網路的控制（如：封鎖 Twitter 和 Facebook），同時也開始將許多資源投入到本國社交媒體的發展上，尤其是 VK，希望可以吸引更多國內外的用戶。VK 成立於 2006 年，創辦人杜洛夫因爲拒絕提供用戶個資給 FSB，在 2014 年被 VK 的董事會撤換下來，而在 2021 年其很大一部分 VK 股份被 Gazprom（俄羅斯天然氣工業股份公司）的子公司 Sogaz 買下來。這一系列事件，加上政府對該社群平臺及整個網路越來越多的限制，引起許多用戶的批評，甚至導致幾波「退出 VK 運動」（“Исход из “ВКонтакте”）（Росинформ, 2021）。

VK 用戶最多的國家是俄羅斯，烏克蘭曾經是 VK 用戶第三大國，但從 2017 年開始，VK 在烏克蘭國內被禁用。

俄烏戰爭後，在俄羅斯 VK 主要封鎖被獨立媒體（包含白俄羅斯及烏克蘭）發布的訊息，以及與 LGBTQ+ 或俄烏戰爭相關的內容。許多影片因被封鎖的用戶或社團上傳而被封鎖，這些用戶通常在 VK 上公開批評普京或表示反戰立場。Knockel, Dalek, Meletti 和 Ermoshina (2023) 蒐集了 300 多篇被俄國法庭公佈的判決書當作封鎖 VK 上內容的理由；與戰前比，在 2022 年 2 月至 10 月期間，要求刪除「不妥當」內容的法律命令的數量增加 30 倍。

在俄羅斯，VK 所使用的審查及限制內容的方式非常多元。例如，搜索涉及到與 LGBTQ+ 相關的社團或用戶時，VK 會使用「關鍵詞過濾」（keywords filtering）來屏蔽與此相關的搜索結果。另外一個方式是直接封鎖特定的用戶或社團，因爲這樣其他用戶沒有辦法搜到其上傳的影片，這也是 VK 下架影片最常用的方式。

除此之外，VK 通常利用法律來證明他們所實施的審查或限制具有正當

性。用戶通常可以看到內容被移除具體的原因，通常是根據法院／授權聯邦執行機構之決定，導致該內容在俄羅斯聯邦境內被封鎖。

2024 年的總統大選期間，VK 和 Odnoklassniki 成爲主要克里姆林宮的宣傳平臺，而負責製作相關的內容政府交給「獨立的非商業組織《對話》」（Автономная некоммерческая организация «Диалог»）。此外，《對話》與另外一個名爲《俄羅斯－充滿機會的國家》（«Россия – страна возможностей»）的平臺開設自己的人才培訓課程，目的是培訓一批親政府的新媒體工作者。2020 年，它們主要負責在社交平臺上推廣修憲（Коммерсантъ, 2021）。俄烏戰爭期間，該組織製造了大量抹黑烏克蘭的假消息。

三、加強網路審查與 VPN 控制

自 2011 年至 2023 年，俄國的網路自由連續 12 年下滑，而導致此結果的，一方面是網路相關法律的改變，另一方面，審查的內容類型一直在增加。

2022 年 2 月 24 日俄羅斯啓動其特殊軍事行動後，俄羅斯境內的 VPN 需求量爆增，下載的次數超過三年的三倍（從 2021 年的 12,585,576 次增加至 2022 年的 33,540,600 次），而 2023 上半年的下載量又下降至 3,366,919 次。與 VPN 相比，TOR 使用得相對少，大約只有 VPN 的十分之一。在 15 個最流行的 VPN 中，已經有 8 個定期遭受 Roskomnadzor 的封鎖，原因是它們都使用 OpenVPN 協定，[19] 而根據近幾年的研究，OpenVPN 較容易被破解（Роскомсвобода, 2023）。

儘管在 2022 年 Roskomnadzor 已經封鎖了大部分獨立媒體、人權組織及政治組織的網站，但與去年比，在 2023 年被封鎖的內容仍然增加了 85%，並延伸到與環保和教育相關的領域。另外，隨著被封鎖的內容類型增加，俄國出現更多不需要經過訴訟程序也能夠要求 Roskomnadzor 進行封鎖，例如，2022 年，俄羅斯檢察署被賦予這樣的權力；同年，有大約 3.4 萬網

[19] VPN 是一種保護網際網路連線的服務，而 OpenVPN 則是協助 VPN 服務達到此目的的通訊協定之一。主要 VPN 協定爲 OpenVPN, Wireguard, Shadowsocks, IKEv2, V2Ray（NordVPN, 2024）。

站因爲匿名檢舉而被列入「有待封鎖」的名單裡，而在 2022 年前 10 年裡，只有十幾個這樣的案例。

2023 年俄國通過了新的法案，計畫從 2024 年 3 月開始，給予 Roskomnadzor 將 VPN 從 Apple Store、Play Market 等平臺上刪除的權力（РИА Новости, 2023）。除此之外，各種網站的封鎖不僅限制用戶的資訊來源，還影響到獨立媒體的工作。有些媒體表示，當受訪者看到媒體的網站被 Roskomnadzor 列爲黑名單時，他們通常選擇拒絕受訪。其次，網站的封鎖導致媒體的讀者和觀眾沒有辦法捐款給這些媒體，導致獨立媒體無法運作。

值得指出的是，爲了讓沒有 VPN 或 TOR 的用戶看到它們的內容，許多媒體選擇將它上傳到其他目前還沒有被封鎖的社群媒體（如 YouTube 或 Telegram），以及不斷地建立新的鏡像網站（mirror sites）。[20] 不過，最近兩年來，Roskomnadzor 封鎖鏡像網站的速度取決於事件發生於國內、國外事實，例如，俄羅斯傭兵組織瓦格納集團在 2023 年 6 月發動兵變期間，有些鏡像網站在出現不到兩分鐘後就被封鎖。這種反應速度，以及越來越全面的 TSPU 使用，估計在未來幾年裡，俄羅斯網路審查規模的擴大及相關技術水準的提升對於網路自由言論是有相當損害（Роскомсвобода, 2023）。

柒、結論

隨著網際網路的發展，人類對於網路的依賴性比過去更高，意識到此事的俄羅斯政府不敢輕忽網路對於國家的影響力，像是過去的阿拉伯之春便是透過網路串聯阿拉伯國家的人民，進而推翻當局政府。爲避免此情況在俄羅斯發生，對於網路主權的掌控、監管機制的建立更顯其重要性，俄國政府對於網路控管的核心便是「打擊極端主義、分裂主義、恐怖主義」

[20] 鏡像網站（mirror sites）是原始網站內容的複製版本，通常擁有不同的網址（URL），但承載的資料與原站相同或極爲相似。建立鏡像網站的主要目的包括：(1) 保存網頁資訊，特別是在原站可能關閉的情況下；(2) 提供替代連結，以存取遭到封鎖或無法瀏覽的內容，藉此規避對主站的審查；(3) 保存具有歷史價值的資料，防止資訊流失。在俄羅斯，許多民眾建立鏡像網站的首要目的，即是爲了對抗政府對主站內容的封鎖與審查行動。

以維護國家主權，像是政府會關閉有極端主義傾向的網站。此外，壓制反政府聲浪在網路上散佈、訂定「外國代理人」法案以更嚴苛的標準審查部分組織或個人、監管通訊軟體的資料等皆爲俄國政府採取的相應措施，然而普遍被歐美國家認爲是箝制民主的聲音，扼殺了人民意見表達的自由。

普京政府致力於讓俄國網路獨立於西方，以免西方勢力滲透並洗腦俄羅斯人民，再者，也要加大控管網路資訊，若有涉及腥羶色、反政府的資訊會被政府所阻攔，甚至用各種方法降低這些資訊的能見度。在 2016 年更是通過了「Yarovaya」法案，要求 ISPs 必須保留用戶的訊息一段時間，以便 Roskomnadzor 進行監管之事宜，用戶的隱私也無法得到完全的保障；2019 年通過「主權網路法」修正案，更是增加了俄羅斯境內的網路審查、過濾機制，若不願意配合者輕者則接受罰款，情節嚴重者則必須接受刑罰，種種網路相關修正案和規範無疑讓政府的權力更擴張。儘管受到歐美國家的嚴厲譴責，中國和俄國仍積極著手於網路主權之相關合作，或許未來俄羅斯本土會面臨資訊來源單一化、言論自由受到箝制等威脅，但對於政府來說維持國家主權完整，避免網路勢力分裂國家才是優先考量的。

俄羅斯聯邦 Roskomnadzor 嚴密監督各式媒體與通訊軟體，嚴格控管國家應該發送給人民的消息，也同時監看人民與人民之間的通話，但是有許多俄國人對於所謂的政府對資訊產業施壓或網路監控，並無感覺，甚至認爲俄羅斯網路孤城僅只是假議題。但是，關於此點，作者認爲許多俄國人本身就不會去造訪被俄羅斯嚴密監控的網站，因而不會觸碰到被政府控制的這類領域，但從 2012 年普京訪中與習近平會面後，加上 2014 年克里米亞事件後對相關播報新聞媒體的嚴格監控，到 2017 年修正案提出，都很容易可以看出俄羅斯對於網路與輿論的掌控越來越嚴密。而普京也認爲俄羅斯網路孤城的建立勢在必行，而且是在國家安全的前提之下。在 2019 年「主權網路法」公布後，人權觀察組織（Human Rights Watch, HRW）表示，俄羅斯大幅擴大法律法規，加強對網際網路基礎設施、線上內容和通訊隱私的控制，和日益孤立於 www 網域這些措施將嚴重削弱俄羅斯人民在網路上行使人權的能力，包括言論自由、通訊自由和獲取資訊的自由（HRW, 2020）。

2022 年俄烏戰爭爆發後，克里姆林宮在俄羅斯網路上封鎖了 Twitter、

Facebook、Instagram、BBC 新聞、自由電臺和美國之音。俄羅斯最後一家獨立媒體被迫關閉，Meduza 也被禁止。俄羅斯迅速而徹底地進入了數位孤立（digital isolation）狀態，隨著莫斯科試圖封鎖異議並控制其入侵烏克蘭的報導，俄羅斯網際網路言論自由的空間也更壓縮了，幾乎所有獨立媒體和記者都被禁止、封鎖和／或宣布爲「外國代理人」或「不受歡迎組織」。除了有線國有頻道外，所有私人擁有的獨立電視頻道均被禁止播放。俄羅斯版 Euronews 於 2022 年 3 月 22 日被 Roskomnadzor 暫停。廣播電臺也有同樣的情況。倖存下來的媒體因爲被禁止的主題和文字而面臨著非常嚴格的自我審查，西方社群網路也逐漸被封鎖，外國媒體記者或被拒絕入境，或被驅逐出境，俄羅斯獨立報導的記者或被逮捕、或被捕期間遭到毆打、或面臨高額罰鍰，或是遭到不明襲擊，俄羅斯已經被認爲是記者工作最危險之地。俄羅斯甚至使用包括臉部辨識（facial recognition）在內的生物辨識技術來監視和鎮壓莫斯科和其他俄羅斯主要城市的記者，這對該國的言論自由構成了重大威脅（International Press Institute, IPI, 2022）。

再者，俄羅斯網路孤城的構築狀況加劇，其中一點爲俄羅斯進行的全國斷網測試成功（禁止瀏覽外國網站），頗有超越中國網路長城的趨勢，雖然許多外媒都表示該孤城的建立有所困難，且成效不佳，在高度全球化、網路資訊普及化的當代，俄羅斯採這樣的作法不僅讓俄國的資訊無法與全球相連接，造成資訊不對等的狀況，也會阻礙俄國本身內部資訊產業的發展，與外國資訊產業的進駐困難程度。例如，2024 年 1 月 30 日晚，俄羅斯經歷了大約兩個小時的網路癱瘓，情況十分嚴重，甚至連被譽爲「俄羅斯 Google」的最大搜尋引擎「Yandex」也與國內數十家主要知名網路公司一起失去連線。連專門追蹤網路中斷情況的知名網站「www.failure.rf」也無法運作。多年來，俄羅斯當局和 Roskomnadzor 逐步構建法律和技術基礎設施，其最終目標是監控和控制 Runet。其中一些措施旨在掌控國內最大的網路公司，例如 Yandex，並對其在引導俄羅斯民眾搜尋有關烏克蘭戰爭的新聞和資訊時進行干預與限制（Meduza, 2024）。

此外，很多俄羅斯網路用戶努力透過使用 VPN 保持與外部的聯繫。VPN 允許人們可以繞過特定國家限制的輔助遠程服務器連接到網路空間，但是很多的 VPN 使用是需要透過線上付費，在目前西方國家將俄羅斯逐出

SWIFT 系統，民眾可能會遇到線上支付問題，包括 VISA 卡、Master 卡和美國運通卡，這迫使許多人求助於免費 VPN，但是免費 VPN 服務參差不齊，並且可以出售有關用戶的使用資訊，這反而會讓俄羅斯人在網路上的個資安全成爲疑慮。

綜言之，在俄羅斯政府加大控管媒體與網路平臺、社群的措施下，部分西方科技公司爲抵制莫斯科當局侵略行爲選擇自主退出俄國市場，可能無形之中成爲莫斯科當局箝制言論自由的幫凶。經濟的制裁、自危的獨立媒體、孤立的網路，俄羅斯的公民社會逐漸萎縮中。

參考書目

NordVPN (2024)。**OperVPN 說明：定義、如何運作以及安全性**。10 月 10 日。https://nordvpn.com/zh_tw/blog/openvpn-shi-shenme/ [NordVPN (2024). *OpenVPN Shuoming: dingyi, ruhe yunzuoyi ji anquanxing*, October 10.]

何清漣（2013）。點評中國：「斯諾登事件」的多重效應。**BBC 中文網**，6 月 17 日。https://www.bbc.com/zhongwen/trad/focus_on_china/2013/06/130617_cr_snowden [He, C.-L. (2013). Dianping zhongguo: Snowden shijian de duochong xiaoying. *BBC zhongwen wang*, June 17.]

許菁芸（2023）。**普京政權二十年（2000-2020）：中央再集權之延續與轉變**。五南。[Hsu, J.-Y. (2023). *Russia under Vladimir Putin for 20 years (2000-2020): Continuity and change of recentralization*. Wu-Nan Book Inc.]

許菁芸、宋鎮照（2013）。地緣政治與國家主權的關係研究－以車臣和科索沃獨立省思臺海兩岸問題。**政治學報**，(56)，55-78。[Hsu, J.-Y., & Soong J.-J. (2013). An analysis on the relations between geopolitics and state sovereignty - Comparative case studies on Chechnya, Kosovo and Taiwan. *Chinese Political Science Review*, (56), 55-78.]

許菁芸、郭武平（2013）。俄羅斯聯邦「競爭性威權」混和體制下之公民社會「管理」與民主走向。**政治科學論叢**，(55)，33-84。[Hsu, J.-Y., & Kwo, W.-P. (2013). The management of Russian civil society and democratic development under competitive authoritarianism. *Taiwanese Journal of Political Science*, (55), 33-84.]

陳曉莉（2011）。**Google 揭露各國政府索取個資數據**。iThome，10 月 27 日。https://www.ithome.com.tw/news/70495 [Chen, H.-L. (2011). *Google Jielu geguo zhengfu*

suoqu gezi shuju, October 27.]

劉瑩（2014）。**普京的國家理念與俄羅斯轉型**。北京大學出版社。[Liu, Y. (2014). *Putin's national concept and Russia's transformation*. Peking University Press.]

Alexanyan, K. (2009). Social networking on Runet: The view from a moving train. *Digital Icons: Studies in Russian, Eurasian and Central European New Media*, *1*(2), 1-12.

Antoniuk, D. (2023). Russia wants to isolate its internet, but experts warn it won't be easy. *The Record from Recorded Future News*. October 17. https://therecord.media/russia-internet-isolation-challenges

Barlow, J. P. (1996). A declaration of the independence of cyberspace. *Electronic Frontier Foundation*. https://www.eff.org/cyberspace-independence

Beitz, C. R. (1999). *Political theory and international relations*, (2nd ed.). Princeton University Press.

Budnitsky, S. (2020). Russia's great power imaginary and pursuit of digital multipolarity. *Internet Policy Review*, *9*(3), 1-25. https://doi.org/10.14763/2020.3.1492

Camilleri, J. A., & Falk, J. (1992). *The end of sovereignty? The politics of a shrinking and fragmenting world*, (1st ed.). Edward Elgar.

Cnews (2021). *Операторы лишили россиян безлимитного интернета*. 30 Ноября. https://www.cnews.ru/news/top/2021-11-30_operatory_iz-za_svoej_prihoti [*Operators deprived Russians of unlimited Internet*. November 30.]

Cnews (2022). *Власти в пять раз сократили расходы на поиск 5G-частот в России*. 2 февраля. https://www.cnews.ru/news/top/2022-02-02_vlasti_v_pyat_raz_sokratili [*Authorities have cut spending on finding 5G frequencies in Russia fivefold*. February 2.]

Economist Impact (2022). The inclusive internet data (3i) 2022. https://impact.economist.com/projects/inclusive-internet-index/2022

Ermoshina, K., Loveluck, B., & Musiani, F. (2022). A market of black boxes: The political economy of internet surveillance and censorship in Russia. *Journal of Information Technology & Politics*, *19*(1), 18-33.

EurAsia Daily (2022). *Лига безопасного интернета потребовала запретить YouTube в России*. 11 марта. https://eadaily.com/ru/news/2022/03/11/liga-bezopasnogo-interneta-potrebovala-zapretit-youtube-v-rossii [*The Safe Internet League has*

demanded that YouTube be banned in Russia. March 11.]

Freedom House (2022). *Freedom on the net 2022*. Retrieved Octorber 30, 2024, from https://freedomhouse.org/country/russia/freedom-net/2022

Google (2024). *Google transparency report*. Google, https://transparencyreport.google.com/government-removals/overview

Hauben, M., & Hauben, R. (1997). *Netizens: On the history and impact of Usenet and the Internet* (1st ed.). Wiley IEEE Computer Society Press.

Human Rights Watch (2020). *Russia: Growing internet isolation, control, censorship*, June 18. https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

International Press Institute (2022). Russia: Facial recognition software used to target journalists. June 23. https://ipi.media/russia-facial-recognition-software-usedto-target-journalists/

ITU Datahub (2024). *Russia, active mobile broadband subscriptions. Russia, fixed-broadband subscriptions*. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Klimburg, A. (2017). *The darkening web: The war for cyberspace*. Penguin Press.

Knockel, J., Dalek, J., Meletti, L., & Ermoshina, K. (2023). Not OK on VK: An analysis of in-platform censorship on Russia's VKontakte. *Citizen Lab Report No. 169, University of Toronto*, July 26. https://tspace.library.utoronto.ca/bitstream/1807/129345/1/Report%23169-not-ok-on-vk.pdf

Kolomychenko, M. (2018). Russia stifled mobile network during Ingushetia Protests. *The Moscow Times*. November 16. https://www.themoscowtimes.com/2018/11/16/russia-stifled-mobile-network-during-protests-a63523

Kolozaridi, P., & Muravyov, D. (2021). Contextualizing sovereignty: A critical review of competing explanations of the internet governance in the (so-called) Russian case. *First Monday*, *26*(5), 1-21. https://doi.org/10.5210/fm.v26i5.11687

Kolozaridi, P., & Shubenkova, A. (2016). Internet as a matter of social policy in Russian official discourse: A 'good' or a 'threat'? *Журнал исследований социальной политики (The Journal of Social Policy Studies)*, *14*(1), 39-54.

Lenta.ru. (2011). *Кибердружинники возьмутся за детское порно "ВКонтакте"*, 25 мая. https://lenta.ru/news/2011/05/25/vleague/ [*Cyber Squads to tackle child*

porn on VKontakte. May 25.]

LiveJournal. (2010). *Statistics*. Retrieved November 20, 2023, from http://www.livejournal.com/stats.bml

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian internet policy. *Media and Communication*, *5*(1), 29-41. https://doi.org/10.17645/mac.v5i1.808

Meduza (2024). *The Russian internet's domain problems and how the war in Ukraine narrows the Kremlin's options for online controls*. February 1. https://meduza.io/en/feature/2024/02/01/the-russian-internet-s-domain-problems-and-how-the-war-in-ukraine-narrows-the-kremlin-s-options-for-online-controls

Morgenthau, H. J. (1978). *Politics among nations: The struggle for power and peace* (5th ed.). Alfred A. Knopf.

Moscow Times (2022). Facebook, Multiple Media Sites Partially Down in Russia – AFP, NGO. March 4. https://www.themoscowtimes.com/2022/03/04/facebookmultiple-media-sites-partially-down-in-russia-afp-ngo-a76750

Netblocks (2019). *Evidence of internet disruptions in Russia during Moscow opposition protests*. August 3. https://netblocks.org/reports/evidence-of-internet-disruptions-in-russia-during-moscow-opposition-protests-XADErzBg

Pertsev, A. (2018). Russia's ban on Telegram has politicized the workspace overnight. Carnegie Russia Eurasia Center. April 23. https://carnegieendowment.org/posts/2018/04/russias-ban-on-telegram-has-politicized-the-workspace-overnight?lang=en

Phokeer, A. (2024). How isolated is the russian internet? Consequences of the war in Ukraine. *Pulse*, June 7. https://pulse.internetsociety.org/blog/how-isolated-is-the-russian-internet-consequences-of-the-war-in-ukraine

Pigman, L. (2019). Russia's vision of cyberspace: A danger to regime security, public safety, and societal norms and cohesion. *Journal of Cyber Policy*, *4*(1), 22-34. https://doi.org/10.1080/23738871.2018.1546884

Pohle, J. (2020). Digital sovereignty: A new key concept of digital policy in Germany and Europe. *Konrad Adenauer Stiftung*, December 15. https://www.kas.de/en/web/guest/single-title/-/content/digitale-souveraenitaet

Reinicke, W. H. (1998) *Global public policy* (1st ed.). Brookings Institution Press.

Reporters Without Borders (RSF) (2024). Russia: Independent media are the primary

targets of Kremlin laws against “foreign agents” and “undesirable organisations”. August 1. https://rsf.org/en/russia-independent-media-are-primary-targets-kremlin-laws-against-foreign-agents-and-undesirable

Reuters (2022). Russia blocks access to BBC and Voice of America websites. 04 March. https://www.reuters.com/business/media-telecom/russia-restricts-accessbbc-russian-service-radio-liberty-ria-2022-03-04/

Richter, A. (2007). Post-Soviet perspective on censorship and freedom of the media. *UNESCO Moscow Office*. https://unesdoc.unesco.org/ark:/48223/pf0000153744

Richter, C., & Kozman, C. (Eds.). (2021). *Arab media systems*. Open Book Publishers. https://www.openbook publishers.com/product/1281

Russia. Post (2023). The state against the internet: How censorship is becoming more effective. September 7. https://russiapost.info/society/state_internet

Schulze, E. (2019). Russia just brought in a law to try to disconnect its internet from the rest of the world. *CNBC*, November 1. https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html

Shakirov, S. (2024). What should Russians do if VPNs are banned? The Moscow Times. June 14. https://www.themoscowtimes.com/2024/06/14/what-should-russians-do-if-vpns-are-banned-a84090

Soldatov, A., & Borogan, I. (2015). *The red web: The struggle between Russia’s digital dictators and the new online revolutionaries*. Hachette Book Group.

Sputnik International (2018). *What you need to know about Washington’s so-called ‘Kremlin Report’?* January 30. https://sputniknews.com/20180130/kremlin-report-analysis-1061196283.html

State Duma (2022). New law on activities of foreign agents. http://duma.gov.ru/en/news/54760/

State Duma. (2017). Законопроект № 145507-7 «О правовом регулировании деятельности социальных сетей и о внесении изменений в отдельные законодательные акты Российской Федерации». 10 апреля. https://sozd.duma.gov.ru/bill/145507-7 [Bill No. 145507-7 “On the legal regulation of the activities of social networks and on amendments to certain legislative acts of the Russian Federation”. April 10.]

Statista (2021). *Leading social media platforms in Russia as of 3rd quarter of 2020, by*

penetration rate. https://www.statista.com/statistics/867549/top-active-social-media-platforms-in-russia/

TeleGeography (2018). *Deputy PM sees commercial 5G in major cities in 2021 (but Moscow maintains 2020 vision)*. September 7. https://www.commsupdate.com/articles/2018/09/07/deputy-pm-sees-commercial-5g-in-major-cities-in-2021-but-moscow-maintains-2020-vision/

The Guardian (2018). Russia blocks millions of IP addresses in battle against Telegram app. April 17. https://www.theguardian.com/world/2018/apr/17/russia-blocks-millions-of-ip-addresses-in-battle-against-telegram-app

Thiel, T. (2021). Das problem mit der digitalen Souveränität [The problem with digital sovereignty]. *Frankfurter Allgemeine Zeitung*, January 25. https://zeitung.faz.net/faz/unternehmen/202101-25/4b6c5ef358b56fe3c17d9912315df988/?GEPC=s3

Toepfl, F. (2012). Blogging for the sake of the president: The online diaries of Russian governors. *Europe-Asia Studies*, *64*(8), 1435-1459.

ТАСС (2016). *В России вступает в силу закон об ограничении иностранного капитала в СМИ*. 1 января. https://tass.ru/ekonomika/2564266 [TASS (2016). *Law on limiting foreign capital in the media comes into force in Russia*. January 1.]

United Nations General Assembly (2015). *Developments in the field of information and telecommunications in the context of international security*. https://germun.de/wp-content/uploads/2023/01/GerMUN_2023_Updates_GA.pdf

Van Alstyne, M., & Brynjolfsson, E. (2005). Global village or cyber-balkans? Modeling and measuring the integration of electronic communities. *Management Science*, *51*(6), 851-868.

von Heinegg, W. H. (2012). *Legal implications of territorial sovereignty in cyberspace* [Conference presentation]. 2012 4th International Conference on Cyber Conflict, June 5-8, Tallinn, Estonia.

White, S., & McAllister, I. (2014). Did Russia (nearly) have a Facebook revolution in 2011? Social media's challenge to authoritarianism. *Politics*, *34*(1), 72-84.

Woodhams, S. (2019). The rise of internet sovereignty and the end of the world wide web? *The Global Post*, April 23. https://theglobepost.com/2019/04/23/internet-sovereignty

World Bank (2023). Individuals using the internet (% of population) - Russian

Federation. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=RU

Wright, G. (2021). ARPANET. *TechTarget*, November 1. https://www.techtarget.com/searchnetworking/definition/ARPANET

Важные Истории (2022). *Секс, ложь и видео*. 2 февраля. https://istories.media/investigations/2022/02/09/seks-lozh-i-video/ [Important Stories (2022). *Sex, lies and video*. February 2.]

Ведомости (2023). *Путин ввел запрет на регистрацию на российских сайтах по иностранной почте*. 31 июля. https://www.vedomosti.ru/technology/news/2023/07/31/987785-putin-vvel-zapret-na-registratsiyu-na-rossiiskih-saitah [Vedomosti (2023). *Putin has introduced a ban on registration on Russian websites using foreign mail.* July 31.]

Википедия (2012). *Забастовка русской Википедии*. https://ru.wikipedia.org/wiki/Забастовка_русской_Википедии [Wikipedia (2012). *Russian Wikipedia strike*.]

ВЦИОМ (2017). *Пресс-выпуск №. 3347. Забанить соцсети?* 10 апреля. https://wciom.ru/index.php?id=236&uid=116150 [VTsIOM (2017). *Press release No. 3347. Ban social networks?* April 10.]

Замахина, Т. (2019). В Совфеде разъяснили порядок работы системы доменных имен в РФ. *Российская газета*, 19 апреля. http0s://rg.ru/2019/04/19/v-sovfede-raziasnili-poriadok-raboty-sistemy-domennyh-imen-v-rf.html [Zamakhina, T. (2019). The Federation Council clarified the operation of the domain name system in the Russian Federation. *Rossiyskaya Gazeta*, April 19.]

Интерфакс (2022). *РКН объяснил блокировку сайтов "Голоса", Amnesty International и "Важных историй"*. 11 марта. https://www.interfax.ru/russia/827718 [Interfax (2022). *Roskomnadzor explained the blocking of the websites of "Voice", Amnesty International and "Important Stories"*. March 11.]

Интерфакс (2023). *"Мегафон" подписал с "Булатом" контракт на поставку до 5 тысяч базовых станций*. 12 октября. https://www.interfax.ru/business/925502 [Interfax (2023). *Megafon signed a contract with Bulat for the supply of up to 5 thousand base stations.* October 12.]

Коммерсантъ (2014). *Владимир Путин: интернет возник как проект ЦРУ, так и развивается*. 4 апреля. https://www.kommersant.ru/doc/2459649 [Kommersant (2014). *Vladimir Putin: the Internet arose as a CIA project and is still developing*. April 4.]

Коммерсантъ (2021). *АНО «Диалог» и АНО «Россия — страна возможностей» запустили программу обучения представителей «новых медиа»*. 26 августа. https://www.kommersant.ru/doc/4958083 [Kommersant (2021). *ANO Dialog and ANO Russia — Land of Opportunities launched a training program for representatives of "new media"*. August 26.]

Коммерсантъ (2022a). *Лигу интернета обезопасили от связи*. 10 февраля. https://www.kommersant.ru/doc/5206856?query=лига%20безопасного%20интернета [Kommersant (2022a) *Internet League secured from communications*. February 10.]

Коммерсантъ (2022b). *«Лига безопасного интернета» сообщила о миллионах фейков о спецоперации*. 19 июля. https://www.vedomosti.ru/politics/news/2022/ 07/ 19/931988-liga-bezopasnogo-interneta-soobschila-o-millionah-feikov [Kommersant (2022b). *"Safe Internet League" reported millions of fakes about a special operation*. July 19.]

Коммерсантъ (2023). *Законопроект о доступе силовиков к базам данных прошел первое чтение*. 16 ноября. https://www.kommersant.ru/doc/6339053 [Kommersant (2023). *The bill on security forces' access to databases passed the first reading*. November 16.]

КонсультантПлюс (2023). *Федеральный закон "О внесении изменений в статью 56.2 Федерального закона "О связи" от 18.03.2023 N 75-ФЗ (последняя редакция)*. 18 марта. https://www.consultant.ru/document/cons_doc_LAW_442354/ [ConsultantPlus (2023). *Federal Law "On Amendments to Article 56.2 of the Federal Law "On Communications" dated 18.03.2023 N 75-FZ (latest revision)*. March 18.]

Кузьмин, А. (2016). Под закон Яровой подпадают все облачные сервисы и интернет-магазины. *Русбейс*, 11 июля. https://rb.ru/opinion/yarovaya-pack/ [Kuzmin, A. (2016). Yarovaya's law covers all cloud services and online stores. *Rusbase*, July 11.]

Левада-центр (2016). *Доверие СМИ и цензура*. 18 ноября. https://www.levada.ru/2016/11/18/doverie-smi-i-tsenzura/ [Levada Center. (2016). *Trust in the Media and Censorship*. November 18.]

Малахов, А., & Балашова, А. (2011). В интернете запустят кибердружины. *Коммерсантъ*, 02 февраля. https://www.kommersant.ru/doc/1580520 [Malakhov A., & Balashova, A. (2011). Cyber squads to be launched on the Internet. *Kommersant*, February 2.]

Медиа (2022). *Ростех представил Михаилу Мишустину отечественную базовую станцию 5G*. 20 января. https://rostec.ru/media/news/rostekh-predstavil-mikhailu-mishustinu-otechestvennuyu-bazovuyu-stantsiyu-5g/ [Media (2022). *Rostec presented a domestic 5G base station to Mikhail Mishustin*. January 20.]

Московский Либертариум (1999). *Концепция формирования информационного общества в России (№ 32)*. https://libertarium.ru/68568.html [Moscow Libertarium (1999). *Concept of formation of information society in Russia (No. 32)*.]

Независимая газета (2000). *Доктрина информационной безопасности Российской Федерации (N Пр-1895)*. https://www.ng.ru/politics/2000-09-15/0_infodoctrine.html [Nezavisimaya Gazeta (2000). *Doctrine of Information Security of the Russian Federation (N Pr-1895)*.]

НКЦКИ (2013). *Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (N Пр-1753)*. [*Basic principles for state policy in the field of international information security to 2020*] *(N Pr-1753)*. https://safe-surf.ru/specialists/normative-materials/dokumenty-strategicheskogo-planirovaniya/1109/ [NKTsKI (2013). *Fundamentals of the state policy of the Russian Federation in the field of international information security for the period up to 2020 (N Pr-1753)*.]

Новая газета (2016). *Группы смерти (18+)*. 16 мая. https://novayagazeta.ru/articles/2016/05/16/68604-gruppy-smerti-18 [Novaya Gazeta (2016). *Death Groups* (18+). May 16.]

Официальное опубликование правовых актов (2019). Федерального закона от 1 мая 2019 года № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”» http://publication.pravo.gov.ru/document/view/0001201905010025 [Official Publication of Legal Acts (2019). Federal Law of May 1, 2019 No. 90-FZ “On Amendments to the Federal Law “On Communications” and the Federal Law “On Information, Information Technology and Information Protection”.]

Официальное опубликование правовых актов (2022). *Указ Президента Российской Федерации от 30.03.2022 № 166 “О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации”*. http://publication.pravo.gov.ru/Document/View/0001202203300001?ysclid=ljx06hx0mf985727638 [Official Publication of Legal Acts

(2019). *Decree of the President of the Russian Federation of 30.03.2022 No. 166 "On measures to ensure technological independence and security of the critical information infrastructure of the Russian Federation"*]

Официальное опубликование правовых актов (2021). Федеральный закон от 28.06.2021 № 232-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях". http://publication.pravo.gov.ru/Document/View/0001202106280033 [Official publication of legal acts (2021). Federal Law No. 232-FZ of June 28, 2021 "On Amendments to the Code of the Russian Federation on Administrative Offenses"]

Правительство России (2023). *Правительство утвердило Стратегию развития отрасли связи до 2035 года*. 4 декабря. http://government.ru/news/50304/ [Government of Russia (2023). *The Government approved the Strategy for the Development of the Communications Industry until 2035*. December 4.]

Президент России (2017). *О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы (№ 203)* http://www.kremlin.ru/acts/bank/41919 [President of Russia (2017). *On the strategy for the development of the information society in the Russian Federation for 2017-2030 (No. 203)*]

РАПСИ (2022). *Лига безопасного интернета предлагает признать ЛГБТ-движение экстремистской организацией*. 25 апреля. https://rapsinews.ru/legislation_news/20220425/307909356.html [RAPSI (2022). *The Safe Internet League proposes recognizing the LGBT movement as an extremist organization*. April 25.]

РБК (2020). *Правительству предложили направить на развитие 5G в России 200 млрд*. 17 ноября. https://www.rbc.ru/technology_and_media/17/11/2020/5fb40c989a7947abd4977fa3 [RBC (2020). *The government was offered to allocate 200 billion for the development of 5G in Russia*. November 17.]

РБК (2023). *«Билайн», «МегаФон» и Tele2 перестанут взимать плату за раздачу интернета*. 30 октября. https://www.rbc.ru/business/30/10/2023/653ee0f79a7947161fd553ff [RBC (2023). *Beeline, MegaFon and Tele2 will stop charging for Internet distribution*. October 30.]

РИА Новости (2023). *РКН сможет блокировать все VPN-сервисы с марта 2024 года, заявили в Совфеде*. October 3. https://ria.ru/20231003/vpn-1900174800.html [RIA Novosti (2023). *Roskomnadzor will be able to block all VPN services from March 2024, the Federation Council announced*. October 3.]

Росинформ (2021). *“Исход из “ВКонтакте”: как российская соцсеть сдает позиции и… пользователей*. 17 февраля. https://rosinform.press/ishod-iz-vkontakte-kak-rossijskaya-socset-sdaet-pozicii-i-polzovatelej/ [Rosinform (2021). *“Exodus from VKontakte: how the Russian social network is losing ground and... users*. February 17.]

Роскомсвобода (2017). *Закон о принуждении VPN и поисковиков фильтровать трафик и запросы вступил в силу*. 1 ноября. https://roskomsvoboda.org/post/zakon-o-prinuzhdenii-vpn-i-poiskovikov-fi/ [Roskomsvoboda (2017). *The law on forcing VPNs and search engines to filter traffic and requests came into force*. November 1.]

Роскомсвобода (2023). *VPN в России: от блокировки сервисов к блокировке протоколов*. 14 ноября. https://roskomsvoboda.org/en/post/vpn-in-russia-2023/ [Roskomsvoboda (2017). *The law on forcing VPNs and search engines to filter traffic and requests came into force*. November 1.]

Роскомсвобода (2025). *Мониторинг реестров*. 19 мая. https://reestr.rublacklist.net/ru/ [Roskomsvoboda (2025). *Monitoring of registers*. May 19.]

Российская газета (2008). *Стратегия развития информационного общества в Российской Федерации (N Пр-212)* https://rg.ru/documents/2008/02/16/informacia-strategia-dok.html [Rossiyskaya Gazeta (2008). *Strategy of the information society development in the Russian Federation (N Pr-212)*.]

Российская газета (2013a). *Президент подписал закон о блокировке экстремистских сайтов*. 30 декабря. https://rg.ru/2013/12/30/president-block-site.html [Rossiyskaya Gazeta (2013a). *The President signed a law on blocking extremist website*s. December 30.]

Российская газета (2013b). *Стратегия развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года (№ 2036-р)*. https://rg.ru/documents/2013/11/08/texnologii-site-dok.html [Rossiyskaya Gazeta (2013b). *Strategy for the development of the information technology industry in the Russian Federation for 2014-2020 and for the future until 2025*. December 30.]

Российской газеты (2015). Федеральный закон от 23 мая 2015 г. N 129-ФЗ “О внесении изменений в отдельные законодательные акты Российской Федерации”. 26 мая. https://rg.ru/documents/2015/05/26/fz129-dok.html [Federal Law of May 23, 2015 N 129-FZ “On Amendments to Certain Legislative Acts of

the Russian Federation". May 26.]

Совет Безопасности Российской Федерации (2016). *Доктрина информационной безопасности Российской Федерации (№ 646)*. http://www.scrf.gov.ru/security/information/document5/ [Security Council of the Russian Federation (2016). *Doctrine of information security of the Russian Federation (No. 646)*]

Сухаревская, А. (2019). В России за полгода выросло число сотовых абонентов. *Ведомости*, 11 сентября. https://www.vedomosti.ru/technology/articles/2019/09/11/811031-viroslo-chislo-abonentov [Sukharevskaya, A. (2019). The number of mobile subscribers in Russia has grown in six months. *Vedomosti*, September 11.]

ТАСС (2014). *С информационными войнами в интернете будут бороться кибердружинники*. 22 августа. https://tass.ru/obschestvo/1394465 [TASS (2014). *Cyber Squads to fight information wars on the Internet*. August 22.]

ТАСС (2018). *В Госдуму внесли законопроект об автономной работе Рунета*. 14 декабря. https://tass.ru/obschestvo/5914675 [TASS (2018). *A bill on the autonomous operation of the Runet was submitted to the State Duma*. December 14.]

ТАСС (2019). *Роскомнадзор определил функции Центра мониторинга и управления сетями общего доступа*. 27 июня. https://tass.ru/obschestvo/6598198 [TASS (2019). *Roskomnadzor has defined the functions of the Center for Monitoring and Management of Public Access Networks*. June 27.]

ТАСС (2023). *Комитет ГД поддержал законопроект о доступе силовиков к базам данных для их изменения*. 10 ноября. https://tass.ru/obschestvo/19255583 [TASS (2023). *The State Duma Committee supported the bill on access of security forces to databases for their modification*. November 10.]

ФОМ (2022). *Источники информации. Телевидение. Предпочтительные источники информации. Уровень доверия новостям*. 17 Февраля. https://fom.ru/SMI-i-internet/14688 [FOM (2022). *Sources of information. Television. Preferred sources of information. Level of trust in news*. February 17.]

Фонд «Росконгресс» (2022). *Милитаризация киберпространства: как пройти идеальный шторм*. 16 июня. https://forumspb.com/news/news/militarizatsija-kiberprostranstva-kak-projti-idealnyj-shtorm/ [Roscongress Foundation (2022). *Militarization of Cyberspace: How to Survive the Perfect Storm*. June 16.]

Шимаев, Р., Полетаева, П., & Румянцева, А. (2019). Отключить рубильник уже не получится»: Госдума утвердила закон о безопасном и устойчивом интернете.

RTД на русском, 16 апреля. https://russian.rt.com/russia/article/621991-gosduma-zakon-suverennyi-internet-rossiya [Shimaev, R., Poletaeva, P., & Rumyantseva, A. (2019). “It’s No Longer Possible to Turn Off the Switch”: The State Duma Approves a Law on a Safe and Sustainable Internet. *RTD in Russian*, April 16.]

The Development, Legislation, and Future Implications of Russia's Concept of Internet Sovereignty*

*Jing-yun Hsu***

Abstract

The rapid development of digital network technologies has transformed the way governments interact with citizens, and has been providing states with new means of exercising control. An increasing number of countries have been introducing their own concepts of internet sovereignty. Russia's "Sovereign Internet Law" came into effect on November 1, 2019. This law authorizes the "Federal Service for Supervision of Communications, Information Technology and Mass Media" (Roskomnadzor) to monitor the operation of both private and public networks nationwide. In the event of an emergency, Russian government authorities are empowered to proactively sever external connections and establish a national network that operates independently of the global internet. Since the outbreak of the Russo-Ukrainian War in 2022, the Russian government has increasingly utilized digital network technology as a tool of control. To maintain its dominance in the online space and strengthen its grip, Russia has intensified restrictions on online speech, expanded surveillance efforts, and passed stringent laws aimed at suppressing dissent. Therefore, the purpose of this study is to examine the implications of internet sovereignty in Russia, examine the development, legislation, and future impact of internet sovereignty since 2012, and analyze the increasingly stringent trajectory of Russia's internet control following the 2022 Russo-Ukrainian War.

Keywords: Russia, Internet Sovereignty, Runet, Sovereign Internet Law, Information Security

---

* DOI:10.6166/TJPS.202509_(105).0003

** Professor & Director, Graduate Institute of Russian Studies, National Chengchi University. E-mail: june0130@nccu.edu.tw