Centre for International Governance Innovation

Digital Policy Hub

Digital Policy Hub — Working Paper

The Cost of Control: Challenges and Trade-Offs of Digital Sovereignty

Gabrielle Lim

Fall term — 2025–2026 cohort

About the Hub

The Digital Policy Hub at CIGI is a collaborative space for emerging scholars and innovative thinkers from the social, natural and applied sciences. It provides opportunities for undergraduate and graduate students and post-doctoral and visiting fellows to share and develop research on the rapid evolution and governance of transformative technologies. The Hub is founded on transdisciplinary approaches that seek to increase understanding of the socio-economic and technological impacts of digitalization and improve the quality and relevance of related research. Core research areas include data, economy and society; artificial intelligence; outer space; digitalization, security and democracy; and the environment and natural resources.

The Digital Policy Hub working papers are the product of research related to the Hub's identified themes prepared by participants during their fellowship.

Partners

Thank you to Mitacs for its partnership and support of Digital Policy Hub fellows through the Accelerate program. We would also like to acknowledge the many universities, governments and private sector partners for their involvement allowing CIGI to offer this holistic research environment.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

About the Author

Gabrielle Lim is a Digital Policy Hub doctoral fellow and a Ph.D. candidate in the Department of Political Science at the University of Toronto and is affiliated with the Citizen Lab at the Munk School of Global Affairs and Public Policy.

Gabrielle's research stands at the intersection of technology, security and global governance. Her work examines how emerging technologies in outer space and cyberspace shape international relations, conceptions of sovereignty and the global commons. She was previously an Open Technology Fund Information Controls Fellow at Data & Society and studied at the Harvard Kennedy School's Shorenstein Center. You can read more about her at gabriellelim.com.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
cigionline.org

Policy Memo

The Cost of Control: Challenges and Trade-Offs of Digital Sovereignty

Gabrielle Lim

Bottom Line Up Front

Where liberal democratic states once pursued a policy of openness and global connectivity, they are now pursuing laws or policies related to digital sovereignty. This shift is due to states attempting to decouple from the United States. However, challenges will emerge due to the overly broad definition of digital sovereignty, which includes economic development, national security and normative goals.

The first set of challenges involves economic growth. As states seek to protect their own networks and data, they nonetheless will want access to other states' markets and data to boost their own domestic firms. A second set of challenges relates to global governance. How will the internet, which follows a multi-stakeholder approach, be reconciled with digital sovereignty's preference for centralization and state control? Lastly, a normative set of challenges will emerge as states attempt to reconcile potentially conflicting values and identities.

Key Points

- There are three core motivations driving digital sovereignty among Western liberal democratic states:
  - decoupling from the United States at a technical, economic and normative level;
  - domestic innovation and economic development; and
  - the pursuit of national identity and values separate from the United States.
- The rhetoric behind digital sovereignty in the West, however, bears a striking resemblance to the justifications given by China and Russia for cyber sovereignty, which have been used to crack down on freedom of expression and human rights.
- At time of writing, the values and norms associated with digital sovereignty are vague, potentially contradictory and may be used as window dressing as opposed to real change.

Recommendations

- **Sustain and increase engagement in both multilateral and multi-stakeholder fora:** Canada and like-minded states should continue to participate in multilateral (state-to-state) discussions, as well as foster ongoing multi-stakeholder engagement through the private sector and civil society.
- **Actively distinguish digital sovereignty from authoritarian cyber sovereignty:** Canada and its allies should ground their justifications for digital sovereignty in human rights, particularly around freedom of expression and freedom from undue surveillance.
- **Consider alternative frames to digital sovereignty:** Not all technology policy has to fall under digital sovereignty. Could a particular objective be better understood under innovation policy, privacy protection or even education?
- **Be explicit about what values we are promoting:** Do not default to "Canadian values" or "Western values." Name them instead (for example, the right to privacy, freedom of expression, self-determination) so that states and companies can be held accountable to their claims. This also helps create a vision for the type of internet and digital ecosystem we want moving forward, as opposed to simply one that has been decoupled from the United States.

Introduction

The internet has, since its inception, been primarily championed by liberal democracies as an open and cooperative space (Barlow 1996; Penney 2011). In a 2010 speech, then-Secretary of State Hillary Clinton proclaimed the internet to be "a new nervous system for our planet" and that then-President Barack Obama had made it his mission to ensure that the United States stands "for a single internet where all of humanity has equal access to knowledge and ideas" (Clinton 2010). Other liberal democratic states, often through their respective foreign affairs agencies or departments, have also followed suit. RightsCon,[1] the world's largest internet freedom and digital rights convention, has been sponsored by the Canadian, Dutch, Swedish and Taiwanese governments. That the internet should be open, free and grounded in human rights, was almost a given, especially when contrasted with Chinese and Russian notions of cyber sovereignty (McKune and Ahmed 2018; Mueller 2020; Qiao-Franco 2024).

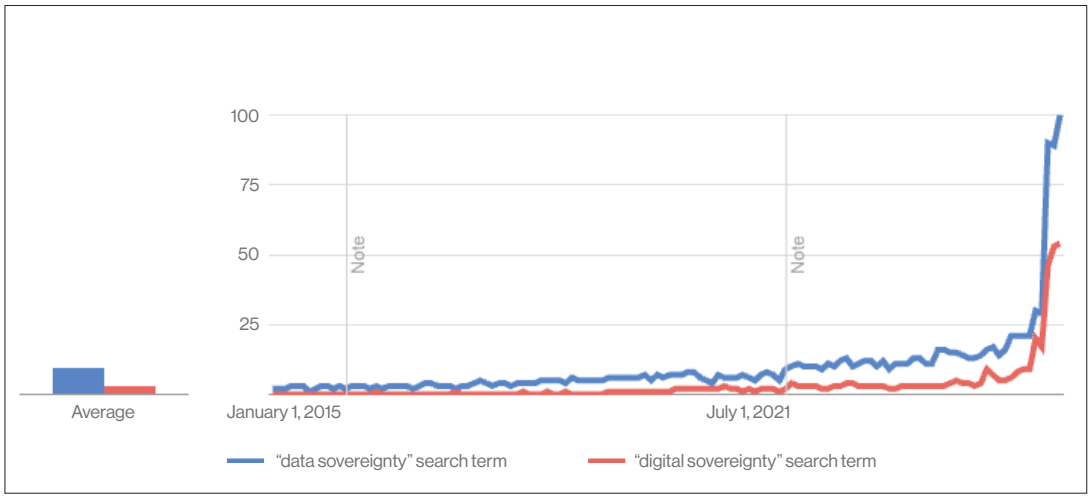
However, as high-profile cases of espionage, disinformation and a long slew of state-sponsored attacks mediated by the internet came to light, visions of a free and democracy-promoting cyberspace quickly gave way to fear and disdain for American "big tech" (that is, Facebook, Google and Twitter, among others) (Deibert 2019). This was especially true after the Edward Snowden disclosures (Bohaker et al. 2015; Clement 2018). The last few years have once again seen a renewed interest in digital sovereignty. What stands out, however, is the number of states taking concrete actions in response to perceived violations of sovereignty. According to Google Trends (see Figure 1), searches for "digital sovereignty" only rose around the beginning of 2025, reaching their peak in October 2025.

What explains this rapid trend? And why now and not during previous crises when our sovereignty was seen to be violated (for example, during the introduction of the US CLOUD [Clarifying Lawful Overseas Use of Data] Act 2018 or the Snowden disclosures of 2013)? This working paper explores this question by reviewing 23 liberal democratic countries to identify the motivations behind these actions and the values, objectives and definitions that states link to digital sovereignty. Of these 23 states, 12 states and three organizations (the European Union, the International Criminal Court [ICC] and the Group of Twenty [G20]) have passed laws, policies and strategies or issued declarations related to digital sovereignty in just a few short years. The other states are either covered by the European Union or are contemplating policies or laws related to digital sovereignty but have yet to issue anything official from the government.

In reviewing these 23 states, this working paper finds that the core drivers of digital sovereignty are a mix of US decoupling, economic development and the pursuit of domestic values and national identity. However, it also finds that because of the broad range of goals attributed to digital sovereignty, there will be several trade-offs and challenges for liberal democratic states, particularly Canada, in pursuing digital sovereignty.

1 See www.rightscon.org/sponsors/.

Figure 1: Google Trends Image for "Digital Sovereignty" and "Data Sovereignty" Search Terms



Source: See https://trends.google.com/trends/explore?date=2010-10-17%202025-11-17&q=data%20sovereignty,digital%20sovereignty.

Clarification on Definitions

Sovereignty is a conceptually cloudy term with myriad definitions to begin with (Barkin and Cronin 1994; Krasner 1999; Ruggie 1993), and digital sovereignty is no different. At the highest level, digital sovereignty refers to "some form of collective control of digital content and/or infrastructures" (Couture and Toupin 2019). How this plays out in policy making, infrastructure and technological development will vary according to the context, actors and interpretations of the term.

Other related terms include "cyber sovereignty" and "internet sovereignty," along with more technology-specific terms such as "AI sovereignty," "cloud sovereignty" and "data sovereignty." Whereas "digital sovereignty" is a broader term, "cyber" and "internet sovereignty" refer more specifically to a state's claim that all internet activities within its borders should be governed by its national laws and policies. In effect, this is an attempt to "territorialize" cyberspace (Shen 2016). More precise forms of digital sovereignty, as seen in concerns over cloud sovereignty (Osborne 2025) or AI sovereignty (Mügge 2024), refer more generally to state control over those specific technologies. This working paper will also include and analyze documents and policies related to these terms, as they are under the umbrella of digital sovereignty.

Background and Policy Relevance

The relationship between sovereignty and information technology has a rich scholarship (Deibert and Pauly 2019; Pohle, Nanni and Santaniello 2024; Pierucci 2025; Raymond 2012). What is missing from current discussions about sovereignty in the digital sphere, however, is a critical assessment of the potential risks of embarking on digital

sovereignty with regard to other norms and values that states may desire (for example, human rights or free markets), and how it may come into conflict with other interpretations of sovereignty (for example, Indigenous data governance).

It is also crucial to remember that sovereignty is not inherently a good thing. History has repeatedly shown that government actions are often sold as necessary for state survival (for example, to protect national security) and may be used to infringe on civil liberties and human rights (Bradshaw, Lim and Haque 2025; Deibert 2015; Scott 2020). Policies, products or services may therefore be sold to the public as being good for the nation under the guise of digital sovereignty when alternate options may be better. Moreover, many of the digital harms that are supposed to be addressed by digital sovereignty, such as foreign-influence operations, surveillance, data extraction and child safety, are not sure bets either. It is conceivable that Canada, instead of being under the thumb of American technology giants, is simply under the thumb of a few Canadian technology giants, such as other industries in this country (for example, grocery stores or movie theatres) (Hearn and Bednar 2024).

At the international level, claims of sovereignty — particularly ones championed by Western liberal states — carry rhetorical weight and can serve as a cover for ulterior motives that may lead to undue censorship, negatively impact innovation and fracture the internet (Internet Society 2021). At the extreme end, should every state demand complete or near-complete control over the digital activity that involves their citizens, a "splinternet" may emerge (York 2022). Canada's foreign policy and social identity have long been based on an open internet and on promoting human rights globally. The policies it chooses in the name of sovereignty will therefore have to be reconciled with its other goals.

Case Selection and Research Methodology

This working paper looks only at the top liberal democratic states, as identified by the Varieties of Democracy Database (2024). This study focuses on states with this regime type because much has already been written about authoritarian assertions of sovereignty over technology and cyberspace (Mueller 2020; Stadnik 2021; Sherman 2019). The risks to human rights, especially freedom of expression, and the desire of authoritarian states to control information flows within and even beyond their borders are already well documented (Al-Jizawi et al. 2022; Anstis, Al-Jiwazi and Deibert 2023). Assertions of sovereignty by liberal democratic states, however, are less discussed.

To identify how liberal democracies understand digital sovereignty, a systematic keyword search of each country was conducted through Google Scholar and Digital Policy Alert, a repository of policies related to technology enacted by the legislatures, judiciaries and executive branches of the G20, EU member states and Switzerland. For each policy, the author reviewed the official government or intergovernmental websites hosting information about the policy, as well as media reporting on these policies, to understand how states interpret and justify digital sovereignty. Both proposed and passed laws and policies are included in this analysis. In total, 23 states

and three organizations were assessed, resulting in 38 policy, legal or high-level strategy documents across 12 states, the European Union, the ICC and the G20.

Digital Sovereignty: Motivations and Drivers

From the reviewed set of policies, several clear drivers emerge that, when combined, explain much of the recent thrust toward digital sovereignty. They can broadly be summarized into three overlapping categories: US President Donald Trump and US decoupling; economic development; and the pursuit of regional values. It is important to note that they are not mutually exclusive but feed into each other. As states react to Trump and the current administration's protectionist, anti-liberal stance, they are also pushed to envision — or re-envision — a new digital world and internet that is not entirely dependent on the United States. To do so, domestic or regional values, along with economic development, are often invoked both as a justification and as an end goal.

US Decoupling and Distancing from Trump

First, the United States' control over cyber infrastructure has been a major concern for both US allies and rivals for a long time. However, it was not until Trump was elected president a second time that many of these concerns turned into concrete policy changes. This is, in part, due to high-profile incidents involving US control over essential technology, such as Ukraine's reliance on Starlink internet services in its fight against Russia (Millar 2025) or allegations that Microsoft locked out the ICC's chief prosecutor, Karim Khan, from his email accounts because of Trump's sanctions on the ICC (Quell 2025). As David Heinemeier Hansson (2025), a Danish entrepreneur and creator of the Ruby on Rails programming language, puts it: "That reality is that all American administrations have the power to disconnect any individual, company, or foreign government from digital infrastructure provided by American Big Tech."

Yet this has almost always been the case. Trump, however, merely said the quiet part out loud. A prime example of this is the US CLOUD Act. Under this law, US authorities can request data from cloud service providers regardless of where the data is physically stored. This extraterritorial reach has rightfully made several states and the European Union uneasy, potentially running into conflict with other states' laws, such as the European Union's General Data Protection Regulation (GDPR) (European Data Protection Supervisor 2019) and Canada's privacy laws (Khoo and Robertson 2025). But the US CLOUD Act was passed back in 2018. Similarly, 80 percent of Europe's digital infrastructure relies on non-European providers (Mishra and Manger 2025). But this is not new either. The realization, along with Trump's bellicose rhetoric and anti-liberal actions, however, are.

It is also interesting to note here the countries that may have found it difficult to come around the digital sovereignty narrative. For example, in a discourse analysis of how Czechia interpreted, contested and eventually agreed to the European Union's push for digital sovereignty, Daniel Šitera and Jakub Eberle (2025) found that one of the main issues was that it appeared "anti-American," in addition to being protectionist.

Trump's Realpolitik on Display

Behind this decoupling lies another broader issue: the re-emergence of or, at least, the open acknowledgement of power politics (Verhelst, Leali and Taylor-Vaisey 2025). When the Danish government chose to drop Microsoft Office and Windows for open-source alternatives such as LibreOffice and Linux, it was partially in response to US aggression over Greenland, which Trump has said repeatedly he wants to unilaterally take over (Vaughan-Nichols 2025). When asked why Canadians did not care about the CLOUD Act until now, Canadian legal scholar Cynthia Khoo quipped, "The US hadn't yet threatened to annex us" (personal communications, 2025). Combined with ongoing disagreements over trade and tariffs, a flagging US response to the war in Ukraine and Trump's disdain for — and withdrawal from — international organizations such as the World Health Organization (The White House 2025), the United States has become an increasingly unreliable ally and a destabilizing global force.

Economic Development

Second, the push to decouple from the United States and Trump comes on the heels of the rise of artificial intelligence (AI). Although large technology companies such as Facebook and Google have always extracted and monetized their users' data, the growth of US companies such as Anthropic and OpenAI — the makers of popular chatbots such as Claude and ChatGPT, respectively — has cemented in the minds of many Australian, Canadian and European policy makers that the gains generated by these companies have been developed in an unfair manner. In an open letter to Canadian Prime Minister Mark Carney, several prominent civil society groups and individuals demanded that the Canadian digital public sphere not be turned into a "zone of extraction" (Zimonjic 2025).

However, states embracing digital sovereignty are also openly acknowledging that they need to compete in the same industry in which they are criticizing the United States for being extractive or monopolizing. The British Sovereign AI Unit and UK Compute Roadmap, for example, routinely stress that sovereign AI is primarily about economic development, with an explicit goal "to pull through the most successful UK-developed technologies into the commercial, at-scale deployments of AI Growth Zones. These zones will offer the scale, power, and integration needed to showcase British capability on a global stage" (Department for Science, Innovation & Technology 2025). If, according to mathematician Clive Humby, "data is the new oil" (quoted in Talagala 2022), then states are using digital sovereignty to ensure they get their share.

National Identity and Values

Third, although digital sovereignty, at the most basic level, is primarily about states attempting to achieve a reasonable degree of independent control over their technical infrastructure, data and networks, it is also bound up in norms, values and national identity. The push to decouple from the United States and Trump would be incomplete without a vision for the future. To this end, justifications for and interpretations of digital sovereignty have also included a range of normative statements.

For example, the European Union's Digital Services Act (DSA) and the GDPR, which seek to regulate how large platforms deliver content and data privacy, respectively, contain requirements that are rooted in norms and values, such as the rule of law (Chander 2023)

or personal data protection (Calabrese and Virah-Sawmy 2025). More recent policy documents from the European Union are even more explicit about promoting European values. In the Declaration for European Digital Sovereignty,[2] signed by all EU member states, digital sovereignty is defined as "ensuring that Europe can act independently and in a self-determined manner based on international law, its own laws, *values*, and security interests, while thriving to international cooperation with its partners that *share European values* and principles" (emphasis own). Similarly, when Canada introduced the AI Strategy Task Force in 2025, the government noted it will aim to "secure our digital sovereignty" and ensure that "AI advancements reflect Canadian values" (Innovation, Science and Economic Development Canada 2025). These statements have not gone unnoticed by the United States. Trump, in response to European legislation such as the DSA and the Digital Markets Act, posted on Truth Social, "As the President of the United States, I will stand up to Countries that attack our incredible American Tech Companies" (quoted in Wheeler 2025).

Broad and Vague Values

However, values and norms are often broad and can be difficult to define or measure. At best, they are loosely based on terms such as "human-centric" or "democratic." When EU decision makers say they are pursuing a specific policy to "protect European values," what does this actually mean? The European Union and even individual states are not monolithic and carry within them myriad values, often contradicting one another. France and Germany, for example, are two strong proponents of digital sovereignty (France 24, 2025). However, both countries value different things: Germany prioritizes the open market, while France prefers self-sufficiency and centralization (Pascarella 2025). Within Canada, state-centric notions of digital sovereignty may contradict with Indigenous or Quebecois conceptions of sovereignty (Paul 2023). This is not new territory. Canada, which is both multicultural and multinational, has a long history of countering US cultural hegemony while attempting to reconcile its own diverse set of values.

Trade-Offs and Challenges in the Pursuit of Digital Sovereignty

Considering the justifications given for digital sovereignty, liberal democratic states will have to navigate a set of potentially competing interests and values when pursuing their own agenda for digital sovereignty. This is particularly true when values (that is, human rights) conflict with economic development (that is, scaling up a large language module). The following serves as a discussion and does not encapsulate all the possible conflicts and trade-offs.

2 See *Declaration for European Digital Sovereignty*, 18 November 2025, online: <https://cdn.table.media/assets/europe/declaration-for-european-digital-sovereignty_final.pdf>.

Economic Challenges

Much of the discourse surrounding digital sovereignty is not simply about whether governments can control the data and networks they rely on to provide crucial services, but also whether they can compete globally and, more precisely, against American companies. This is where digital sovereignty becomes far messier as many of the policies to promote the domestic technology industry could be filed under innovation or economic development instead of sovereignty. It also leads to several questions and potential conflicts: Will a state's approach to digital sovereignty embrace protectionism or free markets? How will states simultaneously safeguard their citizens' data from extraction and exploitation while trying to access other states' data to scale up or compete globally? EU countries benefit from their large single market, but for states such as Canada, more work may have to be put into brokering bilateral agreements and ensuring domestic production provides products and services that are as good as those offered abroad.

Global Governance Challenges

The internet was built on multi-stakeholderism and multilateralism, whether through the International Telecommunication Union, the Internet Governance Forum or the vast network of civil society groups, government agencies and private-sector actors that jointly govern and administer it. Digital sovereignty as espoused by liberal democratic states may not affect this directly, but if more states assert their sovereignty over digital spaces, this may bleed into which values or norms take priority internationally. More precisely, how do liberal democratic states support freedom of expression and keep the internet open, while also pursuing a centralized notion of cyber governance that privileges the state?

Normative Challenges

Lastly and relatedly are a set of normative challenges that states will have to address. Digital sovereignty is not the only policy that states are pursuing at any given time. What happens when the norms and values pursued in the name of digital sovereignty conflict with other actions taken by the state? For example, minister of artificial intelligence and digital innovation, Evan Solomon, declared that digital sovereignty is "the most pressing policy and democratic issue of our time" and that our digital economy must be "free from coercion" (quoted in Wray 2025). Yet, in the same year, under Prime Minister Carney, Canada signed two economic and investment partnerships with the United Arab Emirates (UAE), with an emphasis on AI, despite the fact that the UAE is a known violator of human rights and not a democracy (Prime Minister of Canada 2025). In an opinion piece by Nicole Manger and Vidisha Mishra (2025), they warn that "in building autonomy at speed, [Europe] risks trading its rights-based governance legacy for a defense-centric model that could undermine the very democratic values it seeks to protect." This also applies to Canada, which has a national identity built on liberal values and human rights — one that it prides itself on both domestically and internationally.

Conclusion and Recommendations

Most policies, declarations and laws passed in the pursuit of digital sovereignty by liberal democratic states in the past few years represent a sea change in how cyberspace and the internet are conceptualized and governed. This move is prompted by Trump's bellicosity and the United States' slide into authoritarianism and power politics, alongside the rise of AI, which has forced states to scramble to get a piece of the "AI pie." However, economic development may come into conflict with some of the stated values or normative goals of these states. To mitigate this, there are some things that states such as Canada or the European Union can do.

- **Commit to a multi-stakeholder approach to internet governance:** Doing so will ensure a values-based approach does not fall by the wayside, maintain an open channel of communication between states and civil society, and enshrine accountability and transparency between states and those who are governed. The Internet Governance Forum, for example, was set up as a multi-stakeholder forum precisely to prevent any single entity from exerting undue control over the internet (Malcolm 2008). However, multi-stakeholderism should not be the objective but rather the process by which goals may be achieved, such as security or freedom of expression (DeNardis and Raymond 2013).

- **Actively distinguish digital sovereignty from authoritarian cyber sovereignty:** Liberal democratic states should not abandon their promotion of an open, secure and accessible internet. However, the discourse around digital sovereignty bears remarkable similarity to the discourse around cyber sovereignty as it is used by authoritarian states such as China and Russia. To this end, Canada and its allies should ground their justifications in human rights, particularly around freedom of expression and freedom from undue surveillance.

- **Find alternative frames to justify the same policies:** Not all technology policy has to fall under digital sovereignty. Depending on the objective, actors involved and other contextual factors, other frames may be better suited, such as innovation policy, education policy or privacy policy.

- **Avoid defaulting to "Canadian values" or "Western values"; be explicit about what values we are promoting:** If states are justifying a new technology, service provider or procurement policy using normative language, they should be clear about what those values are instead of nationalizing a vague set of norms. And in many cases, such as shifting from Microsoft to an open-source platform for privacy and security reasons, there may be no need to link to values either.

Acknowledgements

Many thanks to CIGI for the opportunity to delve into and write about digital sovereignty. I would also like to thank Ron Deibert, Samantha Bradshaw, Nathaniel Sukhdeo and Kyle Volpi-Hiebert for their thoughtful and constructive feedback.

Works Cited

Al-Jizawi, Noura, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft and Ron Deibert. 2022. *Psychological and Emotional War: Digital Transnational Repression in Canada*. Citizen Lab Research Report No. 151. Toronto, ON: University of Toronto. https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/.

Anstis, Siena, Noura Al-Jizawi and Ronald J. Deibert. 2023. "Transnational Repression and the Different Faces of Sovereignty." *Temple Law Review* 95 (4): 641–60. www.templelawreview.org/essay/transnational-repression-and-the-different-faces-of-sovereignty/.

Barkin, J. Samuel and Bruce Cronin. 1994. "The state and the nation: changing norms and the rules of sovereignty in international relations." *International Organization* 48 (1): 107–30. https://doi.org/10.1017/S0020818300000837.

Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." Electronic Frontier Foundation, February 8. www.eff.org/cyberspace-independence.

Bohaker, Heidi, Lisa Austin, Andrew Clement and Stephanie Perrin. 2015. *Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World*. Toronto, ON: University of Toronto. https://utoronto.scholaris.ca/server/api/core/bitstreams/71fe734f-e8fa-4270-9237-56bbb0c6a095/content.

Bradshaw, Samantha, Gabrielle Lim and Monzima Haque. 2025. "The Global Spread of Misinformation Laws." *International Journal of Communication* 19 (2025): 2424–46. https://ijoc.org/index.php/ijoc/article/view/21937.

Calabrese, Sofia and Roy Virah-Sawmy. 2025. "If Europe Wants Digital Sovereignty, It Must Reinvent Who Owns Tech." Tech Policy Press, November 18. https://techpolicy.press/if-europe-wants-digital-sovereignty-it-must-reinvent-who-owns-tech.

Chander, Anupam. 2023. "When the Digital Services Act Goes Global." *Berkeley Technology Law Journal* 38 (3): 1067–88. https://btlj.org/wp-content/uploads/2024/01/0006_38-3_Chander.pdf.

Clement, Andrew. 2018. "Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building." Data Governance in the Digital Age Essay Series, Centre for International Governance Innovation, March 26. www.cigionline.org/articles/canadian-network-sovereignty/.

Clinton, Hillary Rodham. 2010. "Remarks on Internet Freedom." US Department of State, January 21. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

Couture, Stephane and Sophie Toupin. 2019. "What does the notion of 'sovereignty' mean when referring to the digital?" *New Media & Society* 21 (10): 2305–22. https://doi.org/10.1177/1461444819865984.

Deibert, Ron. 2015. "Authoritarianism Goes Global: Cyberspace Under Siege." *Journal of Democracy* 26 (3): 64–78. https://doi.org/10.1353/jod.2015.0051.

– – –. 2019. "The Road to Digital Unfreedom: Three Painful Truths About Social Media." *Journal of Democracy* 30 (1): 25–39. www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/.

Deibert, Ronald J. and Louis W. Pauly. 2019. "Mutual entanglement and complex sovereignty in cyberspace." In *Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin Isin and Evelyn Ruppert, 81–99. London, UK: Routledge.

DeNardis, Laura and Mark Raymond. 2013. “Thinking Clearly About Multistakeholder Internet Governance.” Paper presented at GigaNet: Global Internet Governance Academic Network, Annual Symposium. https://doi.org/10.2139/ssrn.2354377.

Department for Innovation, Science & Technology. 2025. “UK Compute Roadmap.” Policy Paper. July 17. www.gov.uk/government/publications/uk-compute-roadmap/uk-compute-roadmap.

European Commission. 2025. “Cloud Sovereignty Framework.” October. Version 1.2.1. https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf.

European Data Protection Supervisor. 2019. “EDPB-EDPS Joint Response on the US Cloud Act.” July 10. www.edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-response-us-cloud-act.

France 24. 2025. “EU must avoid becoming tech ‘vassal’ of US and China, Macron says.” November 18. www.france24.com/en/live-news/20251118-merz-macron-to-push-for-european-digital-sovereignty.

Hearn, Denise and Vass Bednar. 2024. *The Big Fix: How Companies Capture Markets and Harm Canadians*. Toronto, ON: Sutherland House.

Heinemeier Hansson, David. 2025. “Denmark gets more serious about digital sovereignty.” June 3. https://world.hey.com/dhh/denmark-gets-more-serious-about-digital-sovereignty-7736f756.

Innovation, Science and Economic Development Canada. 2025. “Government of Canada launches AI Strategy Task Force and public engagement on the development of the next AI strategy.” News release, September 26. www.canada.ca/en/innovation-science-economic-development/news/2025/09/government-of-canada-launches-ai-strategy-task-force-and-public-engagement-on-the-development-of-the-next-ai-strategy.html.

Internet Society. 2021. “Enablers of an Open, Globally Connected, Secure and Trustworthy Internet.” November 8. www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/.

Khoo, Cynthia and Kate Robertson. 2025. “Canada-U.S. Cross-Border Surveillance Negotiations Raise Constitutional and Human Rights Whirlwind under U.S. CLOUD Act.” The Citizen Lab, February 24. https://citizenlab.ca/2025/02/canada-us-cross-border-surveillance-cloud-act/.

Krasner, Stephen D. 1999. *Sovereignty: Organized Hypocrisy*. Princeton, NJ: Princeton University Press.

Malcolm, Jeremy. 2008. *Multi-Stakeholder Governance and the Internet Governance Forum*. Perth, Australia: Terminus.

Manger, Nicole and Vidisha Mishra. 2025. “Can Europe Build Digital Sovereignty While Safeguarding Its Rights Legacy?” Tech Policy Press, December 5. https://techpolicy.press/can-europe-build-digital-sovereignty-while-safeguarding-its-rights-legacy.

McKune, Sarah and Shazeda Ahmed. 2018. “The Contestation and Shaping of Cyber Norms Through China’s Internet Sovereignty Agenda.” *International Journal of Communication* 12 (2018): 3835–55. https://ijoc.org/index.php/ijoc/article/view/8540.

Millar, Paul. 2025. “Musk says he won’t turn off Ukraine’s access to Starlink communications system.” France 24, March 9. www.france24.com/en/europe/20250309-live-australia-says-would-consider-sending-troops-to-join-peacekeeping-mission-in-ukraine.

Mueller, Milton L. 2020. “Against Sovereignty in Cyberspace.” *International Studies Review* 22 (4): 779–801. https://doi.org/10.1093/isr/viz044.

Mügge, Daniel. 2024. “EU AI sovereignty: for whom, to what end, and to whose benefit?” *Journal of European Public Policy* 31 (8): 2200–25. https://doi.org/10.1080/13501763.2024.2318475.

Osborne, Emily. 2025. “What Does a ‘Sovereign Cloud’ Really Mean?” Tech Policy Press, October 20. https://techpolicy.press/what-does-a-sovereign-cloud-really-mean.

Pascarella, Enrico. 2025. “Berlin and Paris: diverging visions of digital sovereignty at the European Council.” Eunews, October 24. www.eunews.it/en/2025/10/24/berlin-and-paris-diverging-visions-of-digital-sovereignty-at-the-european-council/.

Paul, Morgan. 2023. “Looking to the Future: Indigenous Data Sovereignty and Policy in Canada.” *Pathfinder: A Canadian Journal for Information Science Students and Early Career Professionals* 4 (1): 54–67. https://doi.org/10.29173/pathfinder71.

Penney, Jonathon W. 2011. “Internet Access Rights: A Brief History and Intellectual Origins.” *William Mitchell Law* Review 38 (1): 10–42. http://open.mitchellhamline.edu/wmlr/vol38/iss1/11.

Pierucci, Federico. 2025. “Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace.” *Digital Society* 4, 27. https://doi.org/10.1007/s44206-025-00189-4.

Pohle, Julia, Riccardo Nanni and Mauro Santaniello. 2024. “Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices.” *Policy & Internet* 16 (4): 666–71. https://doi.org/10.1002/poi3.437.

Prime Minister of Canada. 2025. “Prime Minister Carney secures new agreements with the United Arab Emirates to expand trade and attract new investment into Canada.” News release, November 21. www.pm.gc.ca/en/news/news-releases/2025/11/21/prime-minister-carney-secures-new-agreements-united-arab-emirates.

Qiao-Franco, Guangyu. 2024. “An Emergent Community of Cyber Sovereignty: The Reproduction of Boundaries?” *Global Studies Quarterly* 4 (1): ksad077. https://doi.org/10.1093/isagsq/ksad077.

Quell, Molly. 2025. “Trump’s sanctions on ICC’s chief prosecutor have halted tribunal’s work, officials and lawyers say.” PBS News, May 15. www.pbs.org/newshour/world/trumps-sanctions-on-iccs-chief-prosecutor-have-halted-tribunals-work-officials-and-lawyers-say.

Raymond, Mark. 2012. “The Internet as a Global Commons?” Governing the Internet: Chaos, Control or Consensus Opinion Series, Centre for International Governance Innovation, October 26. www.cigionline.org/publications/internet-global-commons/.

Ruggie, John Gerard. 1993. “Territoriality and Beyond: Problematizing Modernity in International Relations.” *International Organization* 47 (1): 139–74. www.jstor.org/stable/2706885.

Scott, James C. 2020. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven, CT: Yale University Press.

Shen, Yi. 2016. “Cyber Sovereignty and the Governance of Global Cyberspace.” *Chinese Political Science Review* 1 (1): 81–93. https://doi.org/10.1007/s41111-016-0002-6.

Sherman, Justin. 2019. “How Much Cyber Sovereignty Is Too Much Cyber Sovereignty?” Council on Foreign Relations, October 30. www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.

Šitera, Daniel and Jakub Eberle. 2025. “Diluting digital sovereignty: Czechia’s quiet selective adaptation to EU digital politics.” *Journal of Contemporary European Studies*, 1–23. https://doi.org/10.1080/14782804.2025.2549578.

Stadnik, Ilona. 2021. “Seeking a new order for global cybersecurity: the Russian approach to cyber-sovereignty.” In *Routledge Companion to Global Cyber-Security Strategy*, edited by Scott N. Romaniuk and Mary Manjikian, 153–64. London, UK: Routledge.

Talagala, Nisha. 2022. “Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires.” *Forbes*, March 2. www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/.

The White House. 2025. “Withdrawing The United States From The World Health Organization.” January 20. www.whitehouse.gov/presidential-actions/2025/01/withdrawing-the-united-states-from-the-worldhealth-organization/.

Vaughan-Nichols, Steven. 2025. “Why Denmark is dumping Microsoft Office and Windows for LibreOffice and Linux.” ZDNET, June 11. www.zdnet.com/article/why-denmark-is-dumping-microsoft-office-and-windows-for-libreoffice-and-linux/.

Verhelst, Koen, Georgio Leali and Nick Taylor-Vaisey. 2025. “G7 embraces ‘realpolitik’ to work around disruptive Trump.” *Politico*, June 18. www.politico.eu/article/g7-embraces-realpolitik-neutralize-disruptive-donald-trump-no-ukraine-declaration/.

Wheeler, Tom. 2025. “Donald Trump’s digital mercantilism.” Commentary. Brookings, October 8. www.brookings.edu/articles/donald-trumps-digital-mercantilism/.

Wray, Sarah. 2025. “Canada aims to integrate digital sovereignty into government decision-making.” *Global Government Forum*, November 11. www.globalgovernmentforum.com/canada-aims-to-integrate-digital-sovereignty-into-government-decision-making/.

York, Dan. 2022. “What Is a Splinternet? And Why You Should Be Paying Attention.” *Internet Society* (blog), March 23. www.internetsociety.org/blog/2022/03/what-is-the-splinternet-and-why-you-should-be-paying-attention/.

Zhang, Marina Yue. 2025. “The public goods case for Australia’s digital sovereignty.” *The Interpreter*, April 2. www.lowyinstitute.org/the-interpreter/public-goods-case-australia-s-digital-sovereignty.

Zimonjic, Peter. 2025. “70 leading Canadians, civil society groups ask Carney to protect Canada’s ‘digital sovereignty.’” CBC News, September 2. www.cbc.ca/news/politics/open-letter-mark-carney-digital-sovereignty-1.7623128.