Norwegian Institute of International Affairs

POLICY BRIEF – 2 / 2022

Digital Sovereignty

Benjamin de Carvalho

SUMMARY

Digital sovereignty is a relative newcomer, in spite of having become relatively well-entrenched in current policy discourses. In fact, as attacks on digital infrastructures – be they private or public – have become more fierce and frequent, it has become clear that the maintenance of national security largely presumes that a state is able to maintain its cyber security. Recourse to sovereignty in this matter also largely implies a willingness to deal with cybersecurity within the legal domain rather than the purely military one. Digital sovereignty does just that. It asserts national privilege as a matter of principle while at the same time keeping the issue at the level of criminal offence rather than a purely military one.

Hacking has always dovetailed the development of cyberspace. As new modes of communicating and gathering data have evolved, new modes of illicit information gathering have become increasingly powerful, to the extent that hacking, today, is perceived not only as a threat by large digital companies eager to safeguard user data, but also by states. In fact, as safeguards against cyber attacks have become increasingly strong, hacking has come to require such enormous resources that can only be mustered by states. From being a sphere largely devoid of state control, with the increase of cyber attacks cyberspace has become a sphere not only crucial to states, but in which they are largely involved. As a way to defend themselves against the threat of cyber attacks, then, states have had recourse to the conceptual arsenal which delineates their rights and prerogatives, namely those associated or derived from the concept of sovereignty. Paradoxically, then, the great power battle over the future of the cyberspace is fought with a conceptual arsenal dating back to Jean

Bodin's writings from 1579. Below, I engage with this, and probe some of the consequences of this usage. For, transposing sovereignty from terrestrial space to cyberspace is not entirely anodyne, as it contributes to frame the alternative policy responses by states. But while the problem cyber sovereignty is meant to address is largely that of national security, it also has ramifications for more general issues such as the governance of cyberspace. Where currents of thought about internet governance had hitherto come from a more libertarian strand shy of state influence, or, more analytically, read against a neo-medieval evolution of the international community, the notion of cyber sovereignty largely negates these, legitimating instead sovereign state intervention in the digital sphere.

Cyber Sovereignty

Digital sovereignty has been around enough that there is less need for a long conceptual definition here that for an understanding of the different uses of digital sovereignty and the consequences of these usages. Applying the term sovereignty to the digital sphere or cyberspace has clear consequences in terms of the types of policies it allows for and how it nests cyberspace within a specific constellation of power and control. Thus, mirroring the two aspects of sovereignty, namely absolute authority within borders and no interference from outside borders, we see that two clear and distinct usages of the concept have emerged within policy discourses dealing with control over the internet. On the one hand we have digital sovereignty within the traditional security realm which is meant to help states secure their infrastructure from (largely) outside threats. According to such an understanding, sovereignty is invoked as a bulwark against outside interference, resting on the claim that ultimately no other states have the right to meddle in the affairs of sovereign states. On the other hand, we see the concept of sovereignty used in conjunction with internal political challenges. Faced with opposition which not only informs itself through the internet, spreads information across national borders, but also uses cyberspace and social media to rally and organize its opposition to sitting powerholders, these in turn seek to limit the free access which hitherto had defined the internet, evoking their cyber sovereignty. In doing so, they create sovereign cyberspaces which differ from one another in content. China is famous for pioneering sovereign encroachments on the free space of the internet, but Russia and other more liberal states are following suit.

Although still of relatively young age, the term "digital sovereignty" has, in the last ten years or so, become firmly established in policy debates over the future of cyberspace to the point of being the center of gravity of many such debates about national ownership of the digital sphere. But, as noted above, linking the concept of sovereignty to cyberspace is not an innocent move. To be sure, sovereignty carries with it an element of control, and the debates about cyberspace in which sovereignty figures tend to gravitate around the issue of national control. Yet, sovereignty was established as a *specific* way of partitioning once more universal authorities with overlapping jurisdictions in favor of a specific *spatiality* of political authority. Thus, debates about digital sovereignty are about more than who ought to control what: they are about *terrestrializing* a hitherto floating space. Terrestrializing the internet also highlights the materiality of the internet. As such, although we cannot yet provide a definitive causal link between the increased consciousness of the materiality of the internet and the application of spatial political concepts to control it, it is nevertheless clear that the two correlate (see illustrations 1 and 2).

Furthermore, current debates about digital sovereignty tend to take the term as a given, and do not acknowledge that different actors have different understandings of it. Not because they misunderstand each other, but because digital sovereignty is used by political actors as a legitimating device in a legitimation contest over the limits and amount of control of cyber space. Before turning to the relative newcomer of digital sovereignty, let us dwell a bit on the meaning of sovereignty, its trajectory and what it implies.

Sovereignty: A Brief Trajectory

The concept of sovereingty in its modern sense is generally taken to emerge in the writings of Jean Bodin. Bodin's definition is first and foremost concerned with domestic sovereignty; 'external' sovereignty in the sense of there being no authority above sovereigns is deducible from domestic absolute power. His definition has nevertheless exerted a great deal of influence on how the sovereignty of the state has been understood. As Cynthia Weber has argued, the common understanding of sovereignty in IR has long been 'taken to mean the absolute authority a state holds over a territory and people as well as independence internationally and recognition by other sovereign states as sovereign state'.

The conceptual centrality of sovereignty in International Relations (IR) cannot be overstated. Generally understood as the principle creating domestic authority, sovereignty is at the origin of the inside/outside divide, making it

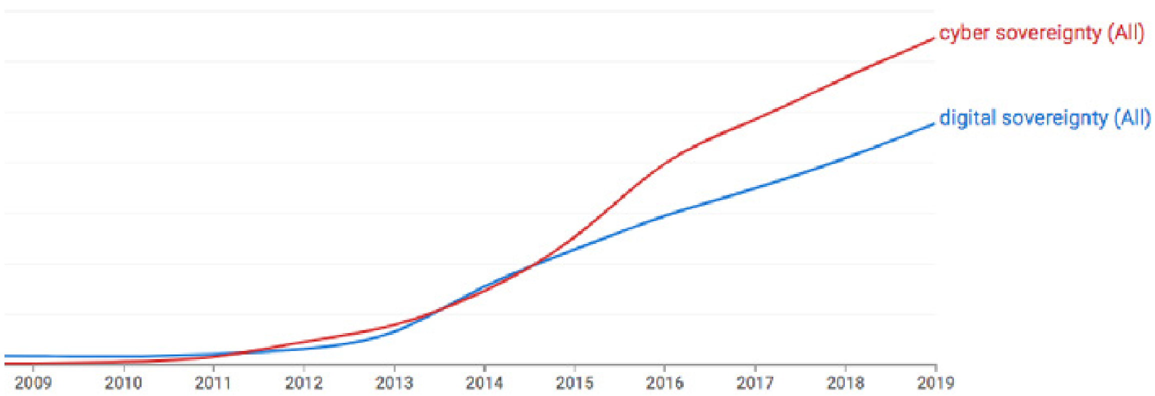

Illustration 1: Increase in usage of "cyber sovereignty"and "digital sovereignty" (source: Google Ngram)

constitutive of the (modern) international. As Gianfranco Poggi has argued, ‘the state’s sovereignty and its territoriality, jointly produce a most significant consequence: the political environment in which each state exists is by necessity one which it shares with a plurality of states similar in nature to itself’. Thus, the concept sovereignty is generally taken to consist of three distinct features, namely supreme authority, and (territorial) limits, and external recognition. Jointly, these are conceptually constitutive of the state. While defining the formal autonomy of the state as the basic unitary actor, the principle of sovereignty also demarcates the spatiality of the unitsW which constitute the system. Thus, while conceptually creating the main units of international politics (the ‘inside’), it also produces the international environment (the ‘outside’).

Until the 1990s, then, in International Relations, sovereignty had been treated as unproblematic and fixed, its definition more or less universally agreed-upon, and often with reference to an overall phrase like F. H. Hinsley’s statement that ‘at the beginning, at any rate, the idea of sovereignty was the idea that there is a final and absolute political authority in the political community; and everything that needs to be added to complete the definition is added if this statement is continued in the following words: ‘and no final authority exists elsewhere’. From the early 1990s, such definitions became contested by historically-oriented social constructivists seeking to demonstrate the contingent meaning of sovereignty through changing social constructions – relying both on contingent discursive articulations and at the same time producing changing distinctions between ‘inside’ and ‘outside.’

With the constructivist push in the mid-1990s, emphasis was put on the inherently constructed nature of sovereignty, and the effects of discourses on authority and sovereignty. Tracing the genealogy of sovereignty, Jens Bartelson famously made the case that the concept of sovereignty should be understood as integral to neither the internal nor the external sphere of politics. Rather, Bartelson argued, it is what makes the distinction between the two spheres of politics possible. Thus, sovereignty is best conceptualized, as Bartelson argued, as a frame or parergon which ‘cannot be a member of either class. It is neither inside, nor outside, yet it is the condition of possibility of both. [T]here is a ceaseless activity of framing, but the frame itself is never present, since it is itself unframed’. What sovereignty frames, then, is a matter of historical contingency.

Digital Sovereignty: Where Does it Come from and What does it mean?

While cyber security may be the latest form of national security issue deploying digital sovereignty to address it keeps the issue from fully “securitizing”. Yet, as noted above, *what* digital sovereignty consists of exactly is still open to interpretation and will vary according to usage. As Pohl and Thiel have recently argued (2020), “Its specific meaning varies according to the different national settings and actor arrangements but also depending on the kind of self-determination these actors emphasise. Focusing on this last factor, we can systematise digital sovereignty claims by distinguishing whether they address the capacity for digital self-determination by states, companies or individuals. What the different discursive layers resulting from this variety of claims share is their prescriptive and normative nature; rather than referring to existing instruments or specific practices, they usually formulate aspirations or recommendations for action.”

That sovereignty was to be introduced in matters of regulation of cyberspace is in a way not surprising, even though it does not entirely make sense. While cyberspace is spatial in name only, as opposed to the terrestrial space surrounding us, the fact that it was categorized as ‘space’ also opens up for spatial metaphors to be employed in its governance. Sovereignty, in that sense, fit the bill.

Digital Sovereignty and the Future Governance of Cyberspace

But there are other reasons why sovereignty made sense in terms of conceptualizing of the governance challenges facing cyberspace. Not least in the way we conceptualized the history of cyberspace, which has clear parallels with how we conceptualize of the break between medieval and modern forms of spatial political authority. Since the early invention of the internet, the story goes, strong voices have been calling for cyber exceptionalism, that cyberspace was a different realm from other spaces. This strand of cyber libertarianism greatly distrusted state institutions and resisted attempts at regulating the field. Faced with digital innovations, especially those allowing for more commercial exploitation of the internet, this full rejection of state regulation gave rise to a middle (muddled) road, namely multi-stakeholder internet governance. While more regulatory in nature, this view still rejected centralized political authority. Whatever the view, both these strands of thinking about organizing the internet cannot overcome

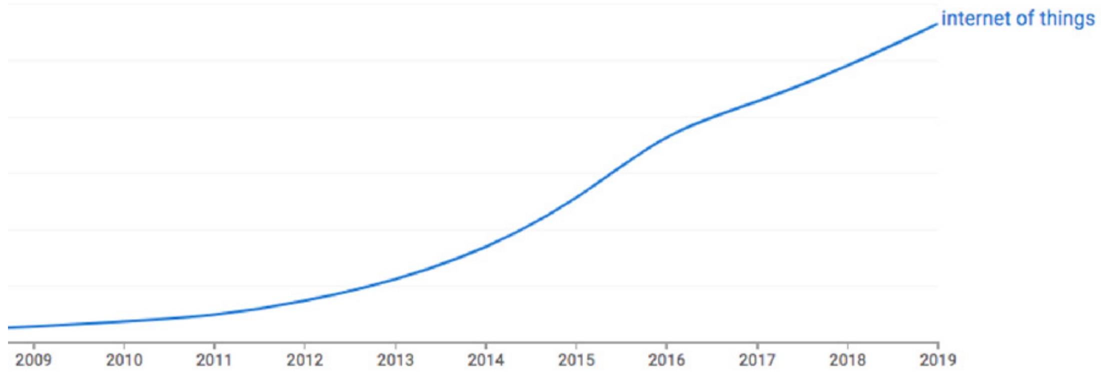

Illustration 2: Increase in usage of “internet of things” (source: Google Ngram)

certain clear coordination problems and cannot give rise to binding agreements, which many states are now calling for in order to guarantee a minimum of security. Note that it should not be forgotten that internet was a state creation, and that different states today have differing views and ideas about what the central val. To the USA, for instance, it is largely individual freedom, whereas Russia China have traditionally emphasized is security and a safe internet, while the EU has tended to emphasize national autonomy and the safeguard of individual rights.

As noted above, this description is not far from the traditional view of medieval structures of political authority against which sovereignty was seen as the ultimate remedy. Nor are they very far from the neo-medieval label applied to systems of international governance which many around the turn of the millennium heralded as the main political innovation of globalization. Against these structures, for better or worse, sovereignty offers the promise of accountability. At the same time, as most of the cyber infrastructure today is largely private but also become a national security issue the safeguard of data has become a sovereign matter. Distinction between state control and multi-stakeholder: latter also under pressure because market centralization, from businesses. Whereas most traffic today goes over networks of the likes of Amazon, Google, or Microsoft, anti-hegemonic evocations of digital sovereignty by larger autocratic states is largely about controlling that flow: curtailing big tech and making a state alternative to big tech. The safeguard of individual rights, then, analogous to traditional sovereignty, has become largely dependent on the benevolence of sovereigns.

Where does this leave states in terms of possible policies? Until now, claims to digital sovereignty have been raised mainly by greater powers such as Germany and France, the EU, Russia and China. Thus far, digital sovereignty has largely been a discursive device, a claim certain states have made. In fact, turning from discourse to practice – to enforcing digital sovereignty, so to speak – is not a self-evident move. Nor is it necessarily the case that all states will see it as worthwhile in economic terms, as the price of full control over a state's infrastructure can be exorbitant – possibly available only to great powers. For small states, then, if what we are seeing today is a trend of renationalization of the internet, the problem they face is potentially a lack of resources to own and control their own infrastructure and data. Choosing sides and partners, then, becomes all the more important. For developing countries, the choices and strategies of small states may be good ones to follow.

Finally, on a more conceptual note, it should be noted that while applying sovereignty to the "non-spatial" cyberspace has a number of consequences, including creating "insiders" and "outsiders" in cyberspace, this also has consequences for the concept of sovereignty itself: where sovereignty in its traditional understanding is a matter of binary control (a state is either sovereign or it is not), digital sovereignty defies that binary. In fact, digital sovereignty as a claim by states can be seen as less about a claim to full control over infrastructure than about certain key parts of it. In that sense, sovereignty does not only affect the future governance of cyberspace, but its application may contribute to new understandings of sovereignty as degrees of control.

Implications for developing countries

As a security strategy, full digital sovereignty as in unabridged and exclusive ownership and control over one's own digital infrastructure and data is a strategy only few states have the resources to contemplate and aspire to. A careful assessment of key components one wishes to control nationally – be that infrastructure or data – should form the baseline of a more financially sober strategy, to be combines with efforts at keeping remaining infrastructure under multinational or global jurisdiction.

Benjamin de Carvalho is a Senior Research Fellow at the Norwegian Institute of International Affairs (NUPI) in Oslo. He has written extensively on changes in the concept of sovereignty.

NUPI Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from shortterm applied research to more long-term basic research.

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | info@nupi.no

Photo: Hillebrand Steve, USFWS