https://doi.org/10.17323/cmd.2025.27725

DYNAMICS OF THE TERRITORIALIZATION OF CYBERSPACE: BETWEEN THE SANCTUARIZATION OF TERRITORIES AND THE PROJECTION OF POWER

Hafidi A.

PhD Student,
Mohammed V University
(Rabat, Morocco)
ahmed_hafidi@um5.ac.ma

Abstract:

This paper focuses on the debate between the sanctuarization of territories and the projection of power in cyberspace. It emphasizes the persistence of territorial logic in an environment where all notions of borders have been abolished in principle. It thus addresses this territorial revenge that will unfold on different levels, sometimes legitimately as sovereign claims, and sometimes encroaching on sovereignty and violating international law principles. The immediate impact of this confrontation is a veritable territorialization of cyberspace, which often results from states putting forward the argument that security is an imperative above all others. Compartmentalization is also motivated by the desire to protect national territories from surveillance by other states' intelligence services and the risks posed by data capture. States such as the US tend to deploy their cyberpower without regard for state borders. The use of extraterritoriality and the projection of force in cyberspace are the main manifestations of this approach.

Keywords: data localization, data sovereignty, territorialization, extraterritoriality, cyberpower

1. Introduction

Territory has always been a pillar of sovereignty, and this demarcation defines the scope of state prerogatives. This logic has come to prevail in cyberspace, which is considered an open space without borders. We can speak of a growing awareness at the state level. Revelations about surveillance practices on the internet have played a major role in this awakening. States are now beginning to worry about the future of their data. They are concerned about where it is stored and how it is processed.

The reactions of governments are not always formulated with the same determination, but, given the economic stakes involved in data circulation and the disadvantages that could result from any restrictions in this area, many developing countries do not have the capacity to initiate such measures, and the debate has not yet been raised. Nevertheless, the general context remains marked by claims of sovereignty that are most often thwarted by numerous constraints.

We believe that answering the following questions will help to outline the issues related to the territorialization of cyberspace and the debate surrounding it:

- How does this notion of territory extend into cyberspace and through what mechanisms?
- What are the issues surrounding the territorialization of cyberspace? To what extent is this fragmentation inevitable?
- What links can be established with the projection of power in cyberspace and its various variants?

To answer these questions, we will first examine the determination of state actors to locate and secure data, and the legitimacy of these approaches, which inevitably lead to the fragmentation of cyberspace. We will then look at how state power can be deployed in cyberspace through extraterritorial application of laws and projection of force.

2. Conceptual framework

This paper combines concepts from the field of international relations and draws heavily on neoclassical realism. A political approach is also used to analyze the concepts of cyberpower and territorialization while cross-referencing these with legal concepts derived from the principles of international law, such as the principle of sovereignty (synonymous with the exclusive jurisdiction of a state over its territory) and the principle of non-intervention (which limits the practice of extraterritoriality).

3. The persistence of territorial logic

The concept of territory, which is the foundation of traditional state sovereignty, has ultimately regained ground in cyberspace and become a determining factor in digital sovereignty. In this regard, the importance of locating data within a nation's territory should be examined considering the issues involved. Similarly, examining the territorialization of cyberspace allows us to measure its impact and assess its legitimacy.

3.1. Relevance of data localization

Sovereignty grants a state “eminent and exclusive power over its territory” (Lacoste, 2003, p. 357). As arbitrator Max Huber pointed out in the Palmas Island case, “Sovereignty in the relations between States signifies independence. Independence regarding a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State” (UN Reports of International Arbitral Awards, 2006, p. 838). Sovereignty, therefore, is a matter of “supreme and exclusive power” for the state (Lacoste, 2003, p. 357).

Due to the importance of territory in exercising effective sovereignty, measures to locate digital data within national borders have become widespread. This trend was further accelerated by Edward Snowden’s revelations about mass surveillance by US security services in 2013. The magnitude of this phenomenon has led us to speak of a post-Snowden era.

The European Court of Justice’s invalidation of the Safe Harbor Agreement on the transfer of personal data from the European Union to the United States in October 2015 confirms this awareness. Companies like Amazon and Microsoft have responded by proposing to open data centers in specific countries. The situation was so urgent that some countries asked for their data to be stored by domestic companies until those relocated data centers were ready on their territory.

When we talk about data localization, we automatically refer to the physical location of data in each territory. However, this concept has been extended to include other meanings. Thus, legal localization imposes applicable legislation as a condition, for example, in Brazil, a legal approach is imposed, translated as follows: “all operations involving the collection, storage, retention or processing of personal data must comply with Brazilian privacy law” (Cattaruzza et al., 2014, p. 102). This typology of localization also refers to logical localization to determine who can access the data.

These approaches generally aim to achieve data sovereignty, which is impossible without data security. However, this may encounter certain limitations that minimize its scope.

The “price” of security

Except in cases where security is non-negotiable, excessive security measures can hinder the normal functioning of institutions, penalize investment and fail to take advantage of the opportunities offered by big data (MacGregor, 2018). Companies may abandon high-demanding countries to operate in those where laws are less restrictive. A good security strategy would thus consist of “the ability to implement the level of security necessary for the user, taking into account the risks they are willing to accept” (Cattaruzza et al., 2014, p. 134). This leads to the question of finding the right balance.

Cloud computing and its challenges

Cloud computing covers a wide spectrum of tasks, ranging from the provision of necessary data storage infrastructure and software to information processing. At this level, a distinction should be made between technical aspects, which aim to integrate decentralized systems, and organizational aspects, which aim to outsource information processing.

Regarding this second level, cloud computing poses new challenges for data security and availability. Data location remains unknown, and uncertainties exist regarding the applicable regulations. The cloud has “gradually moved beyond the strictly technical realm to encroach on the political and strategic spheres” (Bômont & Cattaruzza, 2020, p. 149). This raises “issues of power and sovereignty” (*ibid*) that go far beyond operational aspects and involve strategic considerations.

Web giants and legal constraints

Physical location of data may in some cases be prohibited. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership trade agreements explicitly impose restrictions on data location. Article 14.15 stipulates that: “No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory” (Geist, 2018, p. 109). This article includes exceptions, but it favors the interests of digital giants, known for their defense of their “refusal to comply with any obligation to localize the storage of personal information” (Leterme, 2019, p. 20). This is a significant limitation on a state's sovereign right to independently define data protection measures.

The issue is even more sensitive for developing countries, some of which lack the necessary digital capabilities. Some authors have gone so far as to describe the exploitation of these countries’ local resources (digital data) as “cyber colonization” (Badaoui & Najah, 2021, p. 8). These countries find themselves powerless in negotiations within multilateral forums, particularly the World Trade Organization, where issues of e-commerce and “digital data” status continue to fuel controversy.

3.2. The territorialization of cyberspace: Contestation and legitimation

The divergent interests surrounding the governance of cyberspace inevitably lead to fragmentation. Two opposing approaches are at play: that of nation-states, which primarily emphasize security concerns, and that of large corporations, which seek to maximize their profits. “Actions by nation-states to maintain security and political control will lead to more blocking, filtering, segmentation, and balkanization of the Internet” (Anderson & Rainie, 2014, p. 5). The same fears are echoed in this statement by Catherine Lotrionte: “The danger is that governmental protection may lead to fragmentation of the Internet where states decide to wall themselves off from the Internet in an attempt to insulate their societies from the dangers that travel through the Internet” (Lotrionte, 2012, p. 845). States thus retain this reflex to protect traditional national space and strive to apply it in cyberspace.

The BRICS countries are facing a question of seeking a certain independence from the West. They have distinguished themselves by claiming sovereignty in cyberspace. In 2013, “BRICS decided to build their own internet infrastructure ‘hidden from the NSA’ – to enhance cybersecurity and to create a parallel cyber universe” (Kukkola et al., 2017, p. 17). The project aimed to “connect the BRICS countries with a new high-capacity underwater cable that goes from Brazil, around the Cape of Good Hope, northeast up to India, along the Chinese coast and up to Vladivostok in eastern Russia” (*ibid*). The scale of this project highlights the sovereignty issues it entails. Moreover, the BRICS countries have often proposed or taken concrete steps to assert their sovereignty, particularly in multilateral forums.

In this dynamic of territorialization of cyberspace, fears have been expressed about the possibility of undermining net neutrality. The principle of net neutrality “prevents any discriminatory treatment (positive or negative) of information, whether in terms of source, destination or content” (Escorne, 2020, p. 215), thus guaranteeing equal treatment for all information. The desire of some states to erect barriers, especially legal ones, may contribute to fragmentation of the internet, particularly its semantic layer.

4. The deployment of state power in cyberspace

States can deploy their power in cyberspace in various ways. They can use their legal system outside their borders, contrary to international law standards. In other scenarios, this deployment may take the form of the projection of force.

4.1. Extraterritoriality as a tool of power

Extraterritoriality refers to situations where “the powers of a State (legislative, executive or judicial) govern legal relationships outside the territory of that State” (Salmon, 2001, p. 491). Thus, states resort to extraterritoriality “either by extending the application of their national law to persons or situations beyond their strict borders, or by legislating specifically to regulate phenomena that by their nature transcend the concept of territory” (Rouxel, 2024, p. 3). These approaches run counter to the principles of international law, which "do not allow for exercising jurisdiction to enforce on the territory of another State without the consent of the latter, except under the terms of a treaty or other grounds in international law" (Osula, 2015, p. 732).

The Microsoft case illustrates this phenomenon of extraterritoriality in many ways. In this case, dating back to 2014, United States authorities asked Microsoft with customer data stored on another sovereign territory, Ireland. Microsoft refused, and the case went to the United States Supreme Court.

This case raises a fundamental issue: "the effects of the implementation of criminal proceedings by one state on the sovereign territory of another state" (Davis & Gunka, 2021, p. 52). This goes against the principles of international law. As Svantesson and Gerry (2015, p. 484) rightly noted, "we recognize that the prevalence of cybercrime is used as a justification for intrusive surveillance and over-regulation… Intrusive surveillance and over-regulation threaten the privacy rights of individuals." They went on to state that "the major issue in the Microsoft case that has caused so much intervention is the risk that competing interests at the individual, corporate, government and global levels will not be balanced" (*ibid*). They thus highlighted the irregularity of this case and its implications.

American web giants are also "less inclined to cooperate with the American justice system when data is not hosted on American territory" (Cattaruzza et al., 2014, p. 103), and the Microsoft case illustrates this well. This attitude seems understandable, given the desire to maintain customer confidence. However, "there may still be more coercive means available to the American authorities" (*ibid*). This deployment of power in cyberspace is becoming more concrete with the adoption of extraterritorial instruments.

Partly because of the Microsoft case against the USA, the Cloud Act, also known as the Clarifying Lawful Overseas Use of Data Act, which is the instrument par excellence for the extraterritorial application of US law, came into force on March 23, 2018. This act aligns with the Patriot Act and allows United States authorities to access data held by large American digital companies. It obliges "US service providers, by warrant or subpoena, to provide US authorities with the requested data stored on their servers, whether located in the United States or in foreign countries" (Bômont & Cattaruzza, 2020, p. 159). These actions encroach on the sovereignty of other countries and make efforts to localize data on national territories obsolete.

Although referring to American extraterritorial unilateralism is customary, the European Union is enacting extraterritorially reaching standards. The provisions of the General Data Protection Regulation, which came into force on May 25, 2018, highlight "a disturbing similarity with the rules introduced by the CLOUD Act" (Davis & Gunka, 2021, p. 60). Nevertheless, it remains to be seen whether the EU "has the power to take enforcement measures in a third country, i.e. to carry out material investigative acts, to sanction and impose fines" (Thelisson, 2019, p. 531). This is the whole question regarding the effectiveness of the extraterritorial clauses of this instrument. Other legislation has an extraterritorial dimension, sometimes even more aggressive (Davis & Gunka, 2021, p. 60), such as the English Crime Overseas Production Orders Act, which entered into force on February 12, 2019.

These extraterritorial practices illustrate an important aspect of the deployment of state power. Such behavior is at odds with the principles of international law, particularly regarding the sovereign equality of states and their exclusive control over their respective territories. Even more coercive forms can characterize the deployment of power in cyberspace.

4.2. Projecting force in cyberspace

"No conflict can anymore escape the context of information societies where they are waged" (Kukkola et al., 2017, p. 150). The centrality of cyberspace today means that nothing can be done without considering its characteristics and underlying dynamics. Cyberpower is one of the concepts most closely associated with this space. It is defined as "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain" (Nye, 2011, p. 82). The ubiquity of cyberpower implies that "[i]t can be used to produce preferred outcomes within cyberspace, or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace" (*ibid*), demonstrating the cross-cutting nature of this power and its impact beyond cyberspace.

This space, which now occupies an important place in analysis and discourse on current threats, is particularly vulnerable. "The cyberinformation layer rests upon a physical infrastructure that is vulnerable to direct military attack or sabotage by both governments and non-state actors such as terrorists or criminals" (Nye, 2011, p. 85). The possibilities for destruction, like sabotage carried out in other areas, are no longer just theoretical assumptions. Physical infrastructure, such as fiber optic cables and routers, is a potential target.

Two factors further accentuate this vulnerability: the difficulty of attribution, which allows a high degree of anonymity for actions taken in this space, and the ease of access to and operation in this space. As Joseph Nye highlighted, "The barriers to entry in the cyberdomain, however, are so low that non-state actors and small states can play significant roles at low levels of cost" (Nye, 2011, p. 83). This could provide an opportunity for small states to somewhat alter the balance of power with stronger states. However, the greatest concerns arise when non-state actors seize this technology and project their power into cyberspace. This is a major challenge that states must face. This latter scenario is more complicated because non-state actors may operate from another country’s territory, with or without permission.

The sources of conflict in cyberspace are numerous and are only increasing and diversifying. Therefore, the international community “must work to preserve the normative principles of jus ad bellum and find opportunities to apply these principles in the cyber context” (Lotrionte, 2012, p. 828). As Catherine Lotrionte further explains, “States must work towards a harmonization of what each state understands to be a use of force in cyberspace. Agreement over the contours of sovereignty and self-defense in cyberspace will allow states to develop common terminology, improve predictability, and manage potential crises in the cyber domain” (Lotrionte, 2012, p. 828). These actions are fundamental and constitute a starting point for states to agree on a unified language and terminology that will allow them to better manage the challenges surrounding the use of force in cyberspace.

5. Conclusions

The territorial logic in cyberspace is shaped by several considerations, including the clash between sovereignty claims and the desire for expansion. Territory remains a reality in this clash, resisting the breaking down of borders that have characterized cyberspace. States take concrete actions in response to this, even if they are thwarted by private interests. The requirement for data localization has allowed for a certain “revenge of the territory.” However, this sovereign retreat contributes to the dearterialization of cyberspace and raises concerns about the future of net neutrality.

Contrary to this tendency towards the sanctification of territories in cyberspace, we see states deploying power beyond their borders, sometimes without much regard for the principles of international law. Extraterritorial application of laws and the projection of force beyond borders are flagrant manifestations of this, in and through cyberspace.

The international community is now more than ever called upon to regulate cyberspace and harmonize different national laws to achieve this difficult compromise between legitimate claims to sovereignty and the viability of cyberspace.

REFERENCES

Anderson, J., & Rainie, L. (2014). Net threats. Pew Research Center. http://www.pewinternet.org/2014/07/03/net-threats/

Badaoui, S, & Najah, R. (2021). Intelligence artificielle et cyber-colonisation : implications sur Afrique [Artificial intelligence and cyber-colonization: implications for Africa], Policy paper, Policy Center for the New South. https://www.policycenter.ma/sites/default/files/2022-08/PP_21-03_Badaoui-Najah.pdf

Bômont, C., & Cattaruzza, A. (2020). Le cloud computing : de l'objet technique à l'enjeu géopolitique. Le cas de la France [Cloud computing: from the technical object to the geopolitical issue. The case of France]. Hérodote, 177–178(2), 149–163. https://doi.org/10.3917/her.177.0149

Cattaruzza, A., Danet, D., Douzet, F., Desforges, A., Limonier, K., & Boulanger, P. (2014). La balkanisation du web : chance ou risque pour l'Europe ? Partie 2 [The Balkanization of the web: chance or risk for Europe? Part 2]. https://archives.defense.gouv.fr/content/download/326208/4482530/file/EPS2013-LaBalkanisationDuWeb-Part2.pdf

Cattaruzza, A., Danet, D., Douzet, F., Desforges, A., Limonier, K., & Boulanger, P. (2014). La balkanisation du web : chance ou risque pour l'Europe ? Partie 3 [The Balkanization of the web: chance or risk for Europe? Part 3]. https://www.archives.defense.gouv.fr/content/download/326209/4482539/file/EPS2013-LaBalkanisationDuWeb-Part3.pdf

Davis, F. T., & Gunka, C. (2021). Perquisitionner les nuages - CLOUD Act, souveraineté européenne et accès à la preuve dans l'espace pénal numérique [Searching the clouds - CLOUD Act, European sovereignty and access to evidence in the digital criminal space]. Revue Critique De Droit International, 1(1), 43–66. https://doi.org/10.3917/rcdip.211.0043

Escorne, C. (2020). Les enjeux de la neutralité du Net aux États-Unis [The stakes of Net Neutrality in the United States]. Hérodote, 177–178(2), 215–234. https://doi.org/10.3917/her.177.0215

Geist, M. (2018). Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. Centre for International Governance Innovation. https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security/

Kukkola, J., Ristolainen, M., & Nikkarila, J. (2017). Game changer: Structural Transformation of Cyberspace. https://www.researchgate.net/publication/321767657_GAME_CHANGER_Structural_transformation_of_cyberspace

Leterme, C. (2019, November). Qui captera « l'or du XXIème siècle » ? Bataille autour des données numérique [Who will capture the "gold of the XXI century"? Battle over digital data], Monde diplomatique. https://www.monde-diplomatique.fr//2019/11/LETERME/60937?id_article=60937

Lacoste, Y. (2003). De la géopolitique aux paysages: dictionnaire de la géographie [From geopolitics to landscapes: a dictionary of geography]. Armand Colin.

Lotrionte, C. (2012) State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights, 26 Emory Int'l L. Rev. 825. https://scholarlycommons.law.emory.edu/eilr/vol26/iss2/12

MacGregor, I. (2018). Big data: The Canadian opportunity. Centre for International Governance Innovation.
https://www.cigionline.org/articles/big-data-canadian-opportunity/

Nye, J. S. J. (2011). The Future of Power. PublicAffairs.

Osula, A. (2015). Transborder access and territorial sovereignty. Computer Law & Security Review, 31(6), 719–735. https://doi.org/10.1016/j.clsr.2015.08.003

Rouxel, Q. (2024). L'extraterritorialité du droit comme instrument de puissance dans les relations internationales : comparaison Etats-Unis, Union européenne, Chine depuis la fin de la Guerre froide [The extraterritoriality of law as an instrument of power in international relations: comparison between the United States, the European Union, China since the end of the Cold War]. Histoire. Université Michel de Montaigne – Bordeaux III. https://theses.hal.science/tel-04631742v1

Salmon, J. (Ed.) (2001). Dictionnaire de droit international public [Dictionary of public international law]. Bruylant / Agence universitaire de la Francophonie.

Svantesson, D., & Gerry, F. (2015). Access to extraterritorial evidence: The Microsoft cloud case and beyond. Computer Law & Security Review, 31(4), 478–489. https://doi.org/10.1016/j.clsr.2015.05.007

Thelisson, E. (2019). La portée du caractère extraterritorial du Règlement général sur la protection des données [The scope of the extraterritorial character of the General Data Protection Regulation]. Revue internationale de droit économique, XXXIII(4), 501–533. https://doi.org/10.3917/ride.334.0501

United Nations reports of international arbitral awards (2006). Island of Palmas case (Netherlands, USA), 4 April, 1928, 2, 829–871.
https://legal.un.org/riaa/cases/vol_ii/829-871.pdf

ДИНАМИКА ТЕРРИТОРИАЛИЗАЦИИ КИБЕРПРОСТРАНСТВА: МЕЖДУ ЗАЩИТОЙ ТЕРРИТОРИЙ И РАСПРОСТРАНЕНИЕМ ВЛАСТИ

Хафиди А.

аспирант,
Рабатский университет Мохаммеда V

(Рабат, Марокко)

ahmed_hafidi@um5.ac.ma

Аннотация:

В статье рассматривается взаимосвязь между защитой территорий и распространением власти в киберпространстве. Подчеркивается, что даже в среде, где традиционные границы отсутствуют, территориальная логика все еще играет важную роль. Это приводит к территориальной мести, проявляющейся на разных уровнях – от законных суверенных притязаний до посягательств на суверенитет и нарушения международного права. Результатом этой конфронтации становится территориализация киберпространства. Государства часто утверждают, что безопасность является их первостепенной задачей, и это приводит к разделению киберпространства на зоны влияния. Они стремятся защитить свои национальные территории от слежки и перехвата данных со стороны иностранных разведывательных служб. США, как правило, не обращают внимания на государственные границы при использовании своих киберсил. Они применяют экстерриториальность и силу в киберпространстве, что является основным проявлением их подхода.

Ключевые слова: локализация данных, суверенитет данных, территориализация, экстерриториальность, кибердержава