Global: Jurnal Politik Internasional

Volume 21 | Number 2 Article 6

12-26-2019

Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy

Abid A. Adonis
Paris School of International Affairs, Sciences Po, abid.adonis@sciencespo.fr

Global: Jurnal Politik Internasional Vol. 21 No. 2. Page 262-282. DOI: 10.7454/global.v21i2.412
 E-ISSN: 2579-8251

CRITICAL ENGAGEMENT ON DIGITAL SOVEREIGNTY IN INTERNATIONAL RELATIONS: ACTOR TRANSFORMATION AND GLOBAL HIERARCHY

Abid A. Adonis
Paris School of International Affairs,
Sciences Po
Email: abid.adonis@sciencespo.fr

Abstrak

Dalam dua puluh tahun terakhir, isu kedaulatan digital kian mengemuka dalam perdebatan formulasi kebijakan sebagai reaksi terhadap aktivitas Tiongkok dalam upaya tata kelola internet, kasus Snowden, dan beragam tindakan korporat-korporat digital yang tidak akuntabel. Meningkatnya perhatian aktor-aktor internasional terhadap isu keamanan, ekonomi, proteksi data, dan sosio-politik menciptakan diskursus baru mengenai kedaulatan digital yang memiliki konsekuensi politis pada tingkat global. Hal ini mendorong terjadinya debat intelektual dalam berbagai literatur akademis mengenai pengaruh kedaulatan digital terhadap politik internasional. Artikel ini, secara kritis, meninjau perkembangan literatur mengenai kedaulatan digital. Tinjauan literatur ini mengklasifikasi literatur secara taksonomis ke dalam empat tema utama: perkembangan konseptual dari kedaulatan digital; aktor-aktor dalam kedaulatan digital; kedaulatan digital dan tata kelola internet global; dan isu-isu kategoris dalam kedaulatan digital. Artikel ini berargumen bahwa perkembangan literatur mengenai kedaulatan digital masih didominasi oleh narasi yang menempatkan posisi sentral pada negara di bidang politik-keamanan. Artikel ini mendukung pendekatan-pendakatan yang menyorot hadirnya hierarki dalam dimensi digital pada tingkat global dan transformasi aktor demi mendorong eksplorasi yang lebih jauh terhadap kedaulatan digital. Artikel ini tidak hanya dimaksudkan untuk menghasilkan kesimpulan yang tertutup terhadap debat yang berlangsung mengenai kedaulatan digital, namun dapat dipandang sebagai tulisan pengantar utnuk mendorong terciptanya pertanyaan-pertanyaan lanjutan dan mendukung potensi pengembangan agenda riset dari topik ini.

Kata kunci:
Kedaulatan Digital; Tata Kelola Internet Global; Aktor Negara; Politik Internet; Kedaulatan Internet; Kedaulatan Data; Hierarki Global; Transformasi Aktor

Abstract

The idea of digital sovereignty in the last twenty years increasingly reifies into chiefly policy making debates as the reaction of China's determined activism on internet governance, Snowden's case, and increasingly big internet corporations' unchecked endeavors. International actors' growing concerns on security, economy, data protection, and socio-political issues invoke new discourses on digital sovereignty since it bears global political consequences by nature. This stimulates recent intellectual debate in academic literature on how digital sovereignty affects (or be affected by) international politics. This article critically examines the development of digital sovereignty literatures. This article classifies literature taxonomically on four major themes: the conceptual development of digital sovereignty; actors in digital sovereignty; digital sovereignty and global internet governance; and categorical issues on digital sovereignty. This article argues that the development of literature on digital sovereignty is still largely dominated by state-centered and security-politics narrative. This article calls for global digital hierarchy and actor transformation approaches in order to spur future exploration on digital sovereignty. Instead of drawing closed-ended conclusion of the ongoing debate of digital sovereignty, this article positions itself as an intermediary text to drive more questions and call for broader potential development of the topic's research agenda.

Keywords:
Digital Sovereignty, Internet Global Governance, State Actors, Internet Politics, Internet Sovereignty, Data Sovereignty, Global Hierarchy, Actor Transformation

INTRODUCTION

The debate about sovereignty has long been central in International Relations as it structures the core character of state actors. Since Westphalia Treaty in 1648, the concept of sovereignty has been shaped, refuted, and evolved over historical conjunctures. The concept of sovereignty has also largely been discussed by International Relations and Political Science scholars ranging from Realism, Liberalism, Constructivism, to Critical Theory camp. Overtime, the discussion is also influenced by empirical process of international politics such as the rise of nation-states, decolonization, and the emergence of regionalism like European Union—unprecedented polity that to some extent pooling national sovereignty into regional institution. The emergence of non-state actors also drives new debates on to what extent state actors can exercise its sovereignty (Faisal, 2008; Juned *et al*, 2013). Even lately, the development of technology also prompts sovereignty's conceptual development into question (Anggoro, 2004). By the end of 1990s and early 2000s, the debate of whether state's sovereignty is eroded by internet prevailed as one of the most discussed ideas in international politics. In the last twenty years, the development already shifted that the question is no longer merely about the threat of technology to statehood. Rather, it goes to the questions like is there any sovereignty in cyberspace? How digital world should be governed? Who rules the internet? How to protect individuals' and private companies' rights in internet? How to reconcile between security and human rights consideration in cyberspace?

One of the most remarkable and recent developments of aforementioned intellectual and policy debates lies on digital sovereignty—the idea of to what extent actor can control, govern, exercise, and use digital information and communication. Although many scholars and stakeholders have been delving into definition(s) of digital sovereignty even since 1996, the conceptual development is factually still ongoing. For political scientists and IR scholars, debates on digital sovereignty turn into an interesting topic due to its complex nature. Cyberspace, in which digital information is situated, is located in non-physical territory, yet it has potentiality to affect physical domain, and *vice versa*. This hits the important debate on statehood and its political consequences. The idea of digital sovereignty itself raises questions on the prerequisites of nation-state: territory (since it has no physical territory), people (who to govern in cyberspace), and government (how to govern cyberspace). It, thus, offers theoretical importance to explore in political science and IR debates. In addition to that, the inevitably prominent role of non-state actors, including business actors, activists, and individuals, stimulates digital sovereignty

topic into novel questions that might drive new exploration in political science and IR. This is not to mention that digital sovereignty, by definition, brings intersectionality of various issues, such as security, politics, economy, social, culture, legal, and human rights. Also, the idea of digital sovereignty is considerably dynamic in regards to empirical development from related stakeholders.

There has been plenty of research and studies about digital sovereignty interdisciplinary conducted by various scholars. Mostly they focus on a case by case of digital sovereignty empirical progression. Yet, there are only a few to use helicopter view on the development of literature itself. It is of importance to survey and critically engage on the development of literature to know what has been done, what is the literature gap, and what to research in the future. There is an exceptional and impressive research using literature survey and discourse analysis conducted by Couture and Toupin (2019). They map digital sovereignty's literature and discourses into five perspectives category in which the narrative of digital sovereignty is used. Couture and Toupin's contribution is pivotal to advance the topic's discussion. Building on that, I think it is in utmost significance to propel the discussion by mapping and analyzing literature based on deeper analytical questions to broaden understanding of digital sovereignty. This prompts me to delve into reading on digital sovereignty literature to bring novel comprehension and come out with research question I will use in this article: How does the development of academic literature on Digital Sovereignty progress? This short-straight forward question will be followed by additional research questions to shed light on digital sovereignty's issues: How is the conceptual development of digital sovereignty? Which actor(s) is mostly discussed and why? What kind of pattern occurred between the interaction of digital sovereignty's discourse and internet governance? What kind of issue(s) is profoundly discussed? These four additional questions are useful to map out and analyze the development of digital sovereignty's literature beyond merely conceptual categories. These four questions also arise from my preliminary reading of the literature on digital sovereignty that needs better explanation to unfold.

In this article, I critically engage with literature on Digital Sovereignty topics by positioning this article as an intermediary text to drive more questions and call for broader potential development of the topic's research agenda, rather than drawing closed-ended conclusion on the ongoing debates. I utilize critical literature review approach by using similar intensive literature review methods deployed by Ramadhan (2018) and Ramadhanie (2017). Both embark on their literature review methods by selecting and

sorting out literature deemed importance, pointing out consensus-debate, and synthesizing into their reflection based on findings. However, this article also uses Kertzer and Tingley (2018) methods on examining the current state of selected fields. Kertzer and Tingley use data-driven snapshot of the contemporary state-of-the-art of selected topic using author-generated classifications of manuscript to characterize various approaches and substantive questions. Building on that, Kertzer and Tingley focus their attention on selected questions to see the trajectories of topics. Slightly different with Kertzer and Tingley, here I do not use *International Studies Quarterly*-based manuscripts. Instead, I use more inclusive basis on what texts I fetch as sources based on the text prominence itself. I also sort literature based on their citation numbers and diversity of analysis. I also specify manuscripts used in this article examination are -academic monograph, edited volume, journal article, or other academic peer-reviewed writings. The selected questions for mapping out literature on digital sovereignty are already mentioned in the previous paragraph. The four questions above drive the mapping of literature into four taxonomic categories: a) Conceptual Development of Digital Sovereignty; b) Actors in Digital Sovereignty; c) Digital Sovereignty and Global Internet Governance; and d) Categorical Issues on Digital Sovereignty. There are thirty manuscripts that I analyze and here the literature mapping is as follows.

Table 1. Literature Mapping on Digital Sovereignty

No.	Taxonomic Category	Literature
1.	Conceptual Development of Digital Sovereignty	Wu, 1997; Posch, 2006; Gourley, 2014; Couture & Toupin, 2019.
2.	Actors in Digital Sovereignty	Posch, 2006; Lewis, 2010; Franklin, 2010, 2015; Kumar, 2010; Choucri, 2012; Deibert & Crete-Nishihata, 2012; Irion, 2012; Mueller, 2012; Pohlmann, et. al., 2014; Antonova, 2013; Liaropoulos, 2013, 2017; DeNardis, 2014; Gourley, 2014; Polatin-Reuben & Wright, 2014; Bukharin, 2016; Carr, 2016; Duarte, 2017; Gueham, 2017;; Schlager, et.al., 2017; Stewart, 2017; Yagodin, 2017; Zeng, et.al., 2017; Budnitsky & Jia, 2018; McKune & Ahmed, 2018; Woods, 2018; Couture &

		Topin, 2019.
3.	Digital Sovereignty and Global Internet Governance	Lewis, 2010; Choucri, 2012; Deibert & Crete-Nishihata, 2012; Mueller, 2012; Antonova, 2013; Liaropoulos, 2013; DeNardis, 2014; Polatin-Reuben & Wright, 2014; Franklin, 2015; Gueham, 2017; Yagodin, 2017; Zeng, et.al., 2017; Budnitsky & Jia, 2018; McKune & Ahmed, 2018.
4.	Categorical Issues on Digital Sovereignty	**Security-Politics:** Wu, 1997; Posch, 2006; Kumar, 2010; Lewis, 2010; Choucri, 2012; Deibert & Crete-Nishihata, 2012; Irion, 2012; Mueller, 2012; Pohlmann, et.al., 2014; Liaropoulos, 2013, 2017; DeNardis, 2014; Gourley, 2014; Polatin-Reuben & Wright, 2014; Franklin, 2015; Bukharin, 2016; Carr, 2016; Slack, 2016; Schlager, et al, 2017; Yagodin, 2017; Zeng, et.al., 2017; Budnitsky & Jia, 2018; McKune & Ahmed, 2018; Couture & Toupin, 2019; **Economy:** Posch, 2006; Franklin, 2015; Bukharin, 2016; Gueham, 2017; **Social & Civil Rights:** Posch, 2006; Franklin, 2010; Duarte, 2017; Stewart, 2017; Couture & Toupin, 2019 **Normative:** Zeng, et.al., 2017; Slack, 2016; McKune & Ahmed, 2018; Woods, 2018;

This article will be divided into three parts: introduction, discussion, and conclusion. In the discussion, I examine those four categories of literature and add one reflective overview on how those four questions and mapping are captured analytically.

In the end of literature, I will draw conclusion, caveat of this research, and prospective future research agenda.

DISCUSSION

Conceptual Development of Digital Sovereignty

In this part, I would examine the construction of academic definition and conceptual basis on digital sovereignty. Digital sovereignty itself is often interchangeable or associated with cyber sovereignty, technological sovereignty, data sovereignty, or internet sovereignty. Such confusion arises, by and large, not because of academic debates. Rather it is caused by pervasive and reckless use of the term interchangeably in media and political discourse. The oldest academic conceptual basis of digital sovereignty in International Relations may be found in Timothy Wu's writing (1997). He uses cyberspace sovereignty to delineate the ability of state actors on two domains in cyberspace: content regulation and activity regulation (Wu, 1997, p. 649-650). Posch, later in 2006, comes up with digital sovereignty definition as "*(...) the ability to have full knowledge and control by the individual or by the society about who can access ones data and where ones data are transferred"* (Posch, 2006, p. 77). Gourley later influentially contributes to the academic conceptualization of cyber sovereignty using state-based approach as he believes that cyber domain must be taken as land, air, sea, and space domain based on sovereign territorial principles (Gourley, 2014, p. 277-278). He proposes the distinction between cyber domain and cyber space in which state can act accordingly. Cyber domain refers to physical and network aspects, whilst cyber space is the field upon which cyber domain operates. By then, there is a necessity to distinguish sovereignty *over* cyber space and sovereignty *in* cyber space (Gourley, 2014, p. 279 & 286). Gourley's definition brings detailed state-based explanation in which state actors may or may not exercise its sovereignty. His writing is one of the most influential academic manuscripts that his successors embark (or refute) on his conceptual basis.

However, I recognize that indeed there are more definitions and conceptualisations of digital sovereignty developed outside of academic publication. Many publications and utterances from think-tank, policy makers, bloggers, or even netizens splatter the idea of digital sovereignty. Determined and, presumably, the most authoritative efforts done by Couture & Toupin shed light on how this idea has been constructed and developed. Both employ discourse analysis to survey the conceptual construction of digital sovereignty. They discovered that idea of technological

sovereignty as proto-definition of digital sovereignty can be found in Science Council of Canada as early as 1967 by referring the term as a means to develop and control the technological capability to support national sovereignty. The term "digital sovereignty" itself, according to Couture & Toupin started to emerge in 2012 by French Businessman Pierre Bellange who mentions digital sovereignty as "(...) the control of our present and of our destiny as they manifest and orient themselves through the use of technologies and computer networks" (Couture & Toupin, 2019). Both also emphasize three persistent elements in that concept: nationalism, capacity, and freedom.

Here, we see that state-centric bias remains entailing problem to digital sovereignty definition. Indeed, by nature, sovereignty itself always lies as nation-state's core pillar. However, I see that digital realm offers different variation of sovereignty interlocutors in which it is not only massively influenced by state, but also strengthened by the dynamics of non-state actors, including but not limited to, private companies, civil society, non-governmental organizations, and even individuals. Based on the aforementioned discussion, I understand and posit digital sovereignty, particularly in this article, as the idea of to what extent actors can control, govern, exercise, transfer, and use digital information, communication, and infrastructure.

Couture & Toupin's finding also shows that the conceptualization of digital sovereignty is located chiefly outside of academic community, not even by political scientists or IR scholars. This problematic academic conceptualization of digital sovereignty emerges as a result of the lack of academic publication to rigorously constitute and establish a stable definition of digital sovereignty. In contrast, outside of academic peer-review publication, the development of digital sovereignty definition progressively advances.[1] By and large, these advanced conceptualizations of digital sovereignty outside of academic publication are driven as reactions to empirical processes, such as recent China's active promotion on internet sovereignty, Snowden and Wikileaks's case, or big companies unchecked behavior such as Google, Amazon, Facebook, and Apple (GAFA).

There is still a wide literature gap for capturing advanced conceptual developments in non-academic publication to academic publication. I call for more ideas developed in academic publication involving interdisciplinary approach, but still putting political science and IR as the core, to grasp a better understanding on digital sovereignty theoretically. I argue that the conceptualization shall be inclusive and stable enough to absorb fast changing nature of digital dynamics. It shall allow non-state centered

definition as growing non-state actors involvement in digital realm increasingly rises into prominence. The discussion regarding interaction between actors to digital sovereignty and actor to actor will be unfolded in the following discussion.

Actors in Digital Sovereignty

Historiographically, the internet attracts an interesting reading—as it was discovered by a state actor for military purpose, it has been immensely developed and benefited by non-state actors involvement. Consequently, cyber space has unprecedentedly advanced and shifted power relations between (state and non-state actors which call for novel explanation. One of the core issues lies on digital sovereignty. The idea of sovereignty in the digital realm has always been contested, especially by non-state actors *vis-a-vis* state actors. This is diametrically opposite with traditional notions of sovereignty allowing state actor's monopoly of territory and power principle against individual. Digital sovereignty also stimulates new *realpolitik* battlefield for state actors to pursue their interests and gain their influence at the expense of other state actors. This part will discuss competing international actors in their relations to digital sovereignty in selected literatures.

From 30 manuscripts analyzed in this research, the domination and hegemonic roles of state actors in the narrative of digital sovereignty blatantly appear in 22 literatures.[2] Those indeed come into different gradation and saturation of to what extent state actors should exercise its control to digital realm. Several proponents of state's digital sovereignty strongly call for increasing state's commitment and involvement in cyber space (Gourley, 2014; Bukharin, 2016; Carr, 2016). However, many others are positioned in moderate balance of state and non-state actors' politics in digital sovereignty (Choucri, 2017; Posch, 2016; Gueham, 2017; Liaropoulos, 2013, 2017). In more details, most of the writings are also still predominated by US-European cases. This is considerably understandable since the idea of digital sovereignty is increasingly gaining traction, especially in Europe with European Union posing General Data Protection Rights and several other digital sovereignty initiatives. However, US and European Union have diverging standpoint as the former believes in relatively more freedom in internet facilitating private companies to expand and encourage innovation, while the latter has begun campaigning on data protection issues, human rights concerns, and digital business ecosystem sustainability. EU also intends to reassure its detachment from digital dependence to other foreign entities and manage delicate balance with big companies like

GAFA (Gueham, 2017). But, both still agree on the basic tenets of internet to support freedom, democracy and human rights, at least in rhetoric. The Discussion on US and European Union has also been influenced by NSA controversy, Snowden and Wikileaks' cases—in which those forced policymakers to contemplate and reformulate on digital sovereignty's domain, authority, and scope.

Increasingly, there is also expanding trend to analyze emerging countries, particularly China and Russia to analyze their digital sovereignty activism (Mueller, 2012; Polatin-Reuben & Wright, 2014; Bukharin, 2016; Zeng, et.al., 2017; McKune & Ahmed, 2018; Budnitsky & Jia, 2018). Especially studies on China, it is chiefly empirically stimulated by organized efforts by the East Asian country to promote digital sovereignty through four important pillars: non-interference for internal affairs; data sovereignty; security concerns; and commerce. China exerts its digital sovereignty campaign in domestic level by establishing well-known China Great Firewall separating their internet ecosystem to the rest of the world, whilst actively promotes its internet and digital firms abroad (Mueller, 2012). In similar but not identical vein, Russia also tries to promote internet sovereignty in pursuit of protecting political status quo/stability and securing payment gateway. Both countries also try to engage in public-private partnership with its domestic telecommunication and internet firms, such as Baidu and Yandex, to exercise its digital sovereignty domestically. Lately, both countries pursue the same objective in advancing digital sovereignty in global internet governance (Budnitsky & Jia, 2018). It is indeed clashing with US-European norms and understanding of digital sovereignty and internet norms. These conflictual relations will be discussed later in another part of this article.

In contrast, far less attention has been given to non-state actors. Only eight literatures emphasize non-state actors on their analysis tables.[3] Each of literature varies in their depiction of which non-state actor plays on what sort of digital sovereignty it exerts. Some emphasize the crucial role of civil society, indigenous people, and individuals (Franklin, 2010; Antonova; 2013; Franklin, 2010, 2015; Duarte, 2017; Couture & Toupin, 2019). Some others explain business firms and epistemic communities essential involvement in digital sovereignty (Schlager, et al, 2017; Kumar, 2010). Yet, they adjoint in the same consensus that non-state actors are inevitably active agents in refining ideas of digital sovereignty. The ingrained anarchic character of digital realm facilitates non-state actors to transform their own capability and gain relative power in order to drag ideas of digital sovereignty to their interests. Another consensus arise from

those literature groups is that there is a pertaining precarious and anguished tension between non-state actors to state actors and non-state actors to another non-state actors. One recurring topic in that tension is a tug of war of regulate-deregulate advocacies which vary according to each actor's different path causes. Nevertheless, the discussion based on non-state actors remains largely scarce. There is huge disparity between discussion in stakeholders level and academic level regarding to non-state actors involvement in digital sovereignty. I deem it is paramount to explore research on especially, but not limited to, big internet companies in relation to the idea of digital sovereignty. Many reports have been published in think-tank publications, policy recommendations, and blogs. Little of those reap into academic discussion with theoretical debates. Examination on indigenous people, hacktivists, and political buzzer may also offer interesting perspective on digital sovereignty in the future research. Also, I call for Global South research in examining countries in ASEAN, Africa, and Latin America as their general economic overview lately benefits from the development of technology and startups.

Digital Sovereignty and Global Internet Governance

The precarious and uncomfortable interaction between international actors on digital sovereignty largely takes place in global internet governance. DeNardis defines internet governance as 'the design and administration of the technologies necessary to keep the Internet operational and the enactment of substantive policy around these technologies' (DeNardis, 2014: 6). By definition, it invites discursive contest among related actors pursuing their interests manifested in policy, operational, or regulations. All the parties discussed in previous part of this article push their diverging agenda and policy preferences and consequently put them in power struggles.

There are fourteen prominent literatures in the field explaining the internet governance in relation to digital sovereignty.[4] Scholars in those literatures profoundly discuss global internet governance politics, in which state and non-state actors are inextricably caught in the battle of interests. Most of political struggles take place over Domain Name System (DNS) and Internet Corporation for Assigned Names and Numbers (ICANN), whilst in addition another power struggles also occur in the International Telecommunication Union (ITU) and Internet Governance Forum (IGF). Those institutions are functionally important in bringing actors together in agreement on internet operational and cyber space norms. Those institutions crucially have technical capabilities and responsibilities to manage Internet Protocol space allocations, DNS, and operate

related infrastructures (Liaropoulos, 2017). A number of authors devout to closely analyze power struggle within those institutions, such as Deibert & Crete-Nishihata (2012), Liaropoulos (2017), Mueller (2012), and Budnitsky & Jia (2018). By and large, recurring theme in those literatures is the power struggles between state actors, particularly North American-European led bloc versus Russia and China led bloc. Mueller (2012) and Deibert & Crete Nishihata (2012) analyze how North American-European led bloc is diametrically opposite in propagating norms against Russia and China. North American-European bloc generally believe in non-state centered digital sovereignty by bringing economic and civil rights consideration, whilst Russia and China forcefully propagate state-centered digital sovereignty with security concern and non-interference principles. Deibert & Crete-Nishihata (2012) see this pattern, in turn, would shift the initial norms of digital sovereignty and cyberspace governance, which benefit and were largely crafted by non-state actors, to more state-centered notion—even European Union recently shifted into that trajectory.

The case of non-state actors involvement in digital sovereignty and internet governance is also interrogated by selected literature. Business sector, particularly internet companies, take integral position in internet governance since there is shifting historic control over public interest areas from state to private sector (DeNaris, 2014, 1). Deliberate attempts by private companies to prevent state actors' aggressive intention taking control of cyberspace draw new complexities in internet governance. They are also as active as, if not more, state actors in reshaping global agenda on internet governance. Big companies, in particular, have abundant resources, technical capabilities, and know-how in digital space far faster and better than most state actors. They are involved in cyberpolitics either by demonstrating new innovation that affects internet governance or do the state actors' usual business in politics, like negotiating, lobbying, or shaping discourse. Private companies generally agree that less regulation is better regulation in internet governance. Yet, they still need some amount of regulation to keep the business and commerce going fairly, for instance the copyright and protection of critical infrastructure issues. Franklin (2015) and Antonova (2013) premise the importance of civil society and individuals in internet governance as both assess recent state and business-centered internet governance potentially affect individuals and communities whose voices are not heard substantively. Topics such as civil liberties and human rights are perpetuated by global civil society in internet governance to protect citizen's rights. Some others prompt cyber space as global commons to be protected and not owned by

any sovereign entity. There is also a call for constructing internet social contract, so that digital realm would be engaged in consensual boundaries by various actors. Whilst, Choucri (2012, p. 223) states that global civil society poses a role in new realignment of cyber politics, including in global internet governance. Cyberspace, according to Choucri (2012, p. 223), is not only enablers of power for global civil society, but it has become critical drivers to their interest. All of these complexities are relational. Liaropoulos (2017) determine these relational patterns of global internet governance and digital sovereignty as Multilateral Governance and Multi-Stakeholderism. This means that decision making processes and norm setting dynamics are multifaceted in involving various actors and issues. The complexities of relational pattern in digital sovereignty and internet global governance are proven to be drawn by the existing variation of involved actors. The other complexities also rest on the issues on which actors' disputes are debated and resolved. Discussion about issues in digital sovereignty will be interrogated in the next paragraphs.

Categorical Issues in Digital Sovereignty

The issues discussed in digital sovereignty literature are indeed cross-cutting given its self-nature, comprising of politics, social, economy, and normative. However, I believe that this cross-sectional issues on digital sovereignty can be analysed based on literatures emphasize on specific issues in silo and categorical boxes that presumably capture realities on the ground before delving the interaction between issue. From selected literatures, I found four major themes discussed in digital sovereignty: security-politics, economy, social and civil rights, and normative-legal. This might seem arbitrary in locating and dislocating literature into several categorical issues boxes as some of them might be intersectional and cross-cutting in their analysis. Hence, I render these categorical boxes by examining what is the most highlighted issue in each manuscript and still accommodate those texts, if any, into different categories.

The most discussed issue in digital sovereignty texts rests on security-politics. This category of security-politics specifies on texts concentrating to national and international security as well as national and international politics. Almost all of the texts refer to security-political analysis and implications in relation to digital sovereignty.[5] I see examinations on those literatures unfold into three consensuses. First, there is major consensus that digital sovereignty has been becoming crucial discourse and interest for state actors in the wake of Edward Snowden and NSA's case, cybercrime, terrorism, and

data protection. These four cases have been regularly situated as background and context in which state actors refer to securitize digital sovereignty. Second, there is varying capabilities of each actor in exercising their power to drag the idea of digital sovereignty to their own interests. Power and capabilities among actors are diffused, proven by some business private firms might having greater resources and activism in digital sovereignty compared to some state actors. Third, geopolitical rivalry remains to be the driving seat of state actors political behavior. Recurring contentious relations in digital sovereignty between Western bloc against Russia-China bloc self-evidently demonstrate that geo-political rivalry is also well-translated into techno-political rivalry.

Another group of literatures are far less than the discussion in security-politics categorical issue. I notice only four manuscripts highlighting the economic consequences of digital sovereignty (Posch, 2006; Franklin, 2015; Bukharin, 2016; Gueham 2017). In economic category, there is a converging avenue of arguments that digital sovereignty discussion cannot be detached from profit-taking and market orientation considerations. Digital sovereignty innately has economic and commercial elements in which those who successfully shift the agenda to their own interest, by logic, would earn most or lose least. The same scarcity also goes to normative and legal categorical issues as there are four notable literatures captured in this grouping (Zeng, et.al., 2017; Slack, 2016; McKune & Ahmed, 2018; Woods, 2018). The consensus lies on the problem of jurisdictions of enacting regulations and law in which until now the debate is still ongoing—mostly taking place empirically in parliaments, courts and policy-making discussions rather than academically. Slightly different literature state of art occurs in social and civil rights. Even though I take into account five notable manuscripts (Posch, 2006; Franklin, 2010; Duarte, 2017; Stewart, 2017; Couture & Toupin, 2019), those texts are strongly weighted with important contribution. By and large, they call for civil liberties protection for individuals and marginalized communities and invoke more non state actors' engagement in the digital sovereignty debates. They also critically interrogate hegemonic discourse and governance of digital sovereignty that entail state-centric and business-dominated notions.

I see that by analyzing development of literatures through categorical issues incite novel overview about academic discussion disparity. Hegemonic discourses on digital sovereignty cover profoundly on politics and security perspective, compared to three other categorical standpoints. This shall be a ringing alarm for scholars to deliberately investigate into those largely lacking perspectives in order to advance digital

sovereignty's ideas exploration. More ideas can be explored through interaction between those categorical issues which potentially offer unprecedented analysis.

Reflection: Actor Transformation and Global Hierarchy in Digital Sovereignty?

Based on debates and discussions above, I would like to synthesize those ideas in a broader picture and highlighting prospective literature gap for future research in this part. These four-fold discussions above present helicopter view on literature discussing digital sovereignty which are characterized by heavily fragmented and scattered trajectories of debates but pooling into categorical cores such as conceptual development, actors' dynamics, governance, and issues taken. The conceptual development of digital sovereignty remains to be open-ended discourse but chiefly concentrated on the idea of to what extent actor can control, govern, exercise, transfer, and use digital information, communication, and infrastructure. The conceptualization of digital sovereignty must accommodate every actor and issue involved in digital realm and is stable enough to adjust with technological developments present or in the future. Actors and issues engaged in digital sovereignty discourse increasingly multiply and diffuse. Even though it is still dominated by state actors and, to a lesser extent, business firms to pursue security-political and economic advantage, more actors and issues increasingly multiply and diffuse. Adding to that argument, the dynamic interplay in internet global governance demonstrates acute conflicting relations upon which actors and issues are immensely contesting. As a result, politics in digital sovereignty presumably would experience deepening and widening contention in the upcoming future.

Given that actors and issues' multiplexity, digital sovereignty invites more detailed and specific explanations especially (power) relational account among actors and issues. However, at the same time, it also necessitates generalization and parsimonious explanation in understanding political and relational pattern between actors and issues. Here I see that the whole complexities mentioned above can be parsimoniously reflected by understanding actor transformation and global hierarchy as consequences of politics in digital sovereignty. I regard actor transformation as the process of actor acquiring capabilities, constituting their interests, reacting to external environment & issues, adjusting with other actor's behavior, and experiencing conjunctures upon which the actor has set of expected behavior. This idea is inspired by Hameiri & Jones' state transformation analytical framework (Hameiri & Jones, 2015). However, here I widen up

transformation not exclusively belong to state actors (as proposed by Hameiri & Jones) and reflect more on the case discussed in this paper.

By looking in detail at those transformations of each actor, we would have better lenses in understanding its behavior in digital sovereignty. Particularly, the two most important elements are power and interests. Investigating actor's transformation in their relations digital sovereignty would discover not only an actor's expected behavior, but also the distribution of power, capabilities, and resources among actors. Employing this approach in the future presumably would discover why one actor is gaining more influence better than another actor in digital sovereignty. In turn, it also allows readers and scholars to see reflexive interaction in digital sovereignty caused primarily by actor's power, interest, history, and perception to another actor and external environment. This reflexive interaction can be found in the several discussions on digital governance taking place in ICANN, DNS, or ITU.

Actor transformation in digital sovereignty might answer on question why some state actors are left behind in digital sovereignty by another state actors or even non-state actors. As every actor experience different technological path dependence, so it goes to their variation of power and interest in digital sovereignty. Consequently, the physical power pertinent in an actor outside of digital realm might not necessarily translate into their power and interest in digital space. Thus, these lead to structural overview of power distribution and interest diversity among actors in digital sovereignty.

Building on the aforementioned argument, I reflect that current digital sovereignty and its relational consequences among actors creating global hierarchy in digital space. Instead of resting every interaction in governance analytical tools, I assume that global digital hierarchy is produced since every actor possesses hierarchical power. This idea is also inspired by Ayse Zarakol's writing about Hierarchies in World Politics (2017). When an actor is contesting with another actor in certain interaction or governance, global digital hierarchy is erected autonomously. It is caused by recurring power relations when one exercises its power to another actor. Nevertheless, due to intrinsic digital nature, I presume the global digital hierarchy is relatively more fluid compared to global political hierarchy outside of the digital realm. Global digital hierarchy is also presumably characterized by non-linear power distribution. Instead, it has fragmented distribution of power, and thus its hierarchy, due to each actor's functionality and limits.

In my reflection, global digital hierarchy does not only establish among *actors*. It might also establish based on categorical *issues* due to actors' interest diversity. One issue

might be prioritized and discussed more frequently than others in which it creates hierarchical priority. We can examine global digital issues hierarchy by checking which topic experiencing more discursive practice and performativity not only in academic publications but also in the media and policy making debates. It is also essential to regularly observe competing narratives in global internet governance. Yet again, global digital issues hierarchy might be more fluid and unstable compared to actor-based hierarchy. I predict it is caused by the rapid growth of technological development that always brings new externalities.

Here, I try to contemplate my reflection by using Global Hierarchy and Actor Transformation lenses to capture the whole complexities in more parsimonious fashion and mediate more opportunity in analyzing digital sovereignty. It is also my reflective engagement with numerous texts discussed in this article. Based on discussion in previous parts, I see that there is a lack of weighted theoretical engagement in current available texts. Some texts already underpin political science and IR approaches in understanding digital sovereignty by employing a range of mainstream lenses from realism to constructivism. However, there has not been yet any substantive novelty that significantly contribute to the theoretical development, either for the conceptualization of digital sovereignty itself or broader related topics such as sovereignty, territoriality, and international (or transnational) politics. The only literature I deem standing out in terms of theoretization is Choucri's writing (2012) that demonstrate most comprehensive assessment on past, current, and future cyberpolitics trajectories, together with its theoretical contribution. The rest of literature mostly still touch deeply into empirical interplay whilst put aside potential significant theoretical deduction.

This is not to mention that in the current discussion about digital sovereignty I still notice massive disparity and unexplored research fields. The lack of substantive conceptual development in digital sovereignty must be addressed by future research and studies in adapting with current fast-changing empirical dynamics on digital sovereignty. I invite more scholars to look at recent European Union initiatives and Global South progress on digital sovereignty. More research shall be conducted beyond state-centered narratives, especially for civil societies, business firms, and individuals. In categorical issues, I believe more ideas can be explored in increasingly widening issues related to digital sovereignty beyond security-politics interplay. Scholars also need to address quantity disparity of academic texts and non-academic texts on digital sovereignty. Empirical processes on digital sovereignty appear to be more rapid rather than scholars'

analyses and knowledge production. This disparity cannot be sustained. There shall be broader engagement and research by scholars on the topic.

CONCLUSION

The discussion on digital sovereignty above is aimed to answer the main research question on how does the development of academic literature on Digital Sovereignty progress. I found that the development of academic literature on digital sovereignty is still largely dominated by state-centered narrative and security politics issues. The conceptualization of digital sovereignty still needs more constructive efforts to overcome current weaknesses. I also notice massive disparity between state-emphasized to non-state actors-emphasized analysis on digital sovereignty which becomes literature gap to be addressed for future research agenda. In a similar vein, disparity is also prevalent among categorical issues in which security-politics narrative prevails far than social and civil rights, economy, and normative perspective.

In my reflection of discussion among texts, I see that there is a lack of weighted theoretical underpinning in most of the texts. As a result, little contribution is given to the grand debate in political science and International Relations. Thereby, I try to provoke more theoretical engagement by reflecting current digital sovereignty debates to two structural and interrelated approaches: actor transformation and global hierarchy. Actor transformation understanding would potentially shed light on how actors behave according to their power, interest, history, and perception. When an actor interacts with another actor, it autonomously establishes power relations that in turn creating distribution of power landscape and result to global digital hierarchies among actors. This global digital hierarchy emerges not only based on actors, but also to the issues related to digital sovereignty. These two interrelated approaches I propose are intended not necessarily to be strictly regarded as theoretical offer. Yet, it is more as a display that exploration on theorization of digital sovereignty has many to offer in the future.

Again, this article positions itself as intermediary text to drive readers to broader research exploration on digital sovereignty. The caveat of this research lies in its limited elaboration of each analysis, diversity of issues brought up, and narrow selection of the texts. It creates a sense that this research is shallow and superficial. In my defense, it is intentionally aimed to fulfill this article intention to be intermediary text on digital sovereignty. It is also the reason why I do not draw rigorous conclusion as I intend to point out and depict the current state-of-the-art literature on digital sovereignty. Last but

not least, digital sovereignty is still an unfinished business to explore and construct academically. It is an open-ended topic in which its empirical process evolves rapidly and demands more compelling academic analysis. And like every unfinished business, it needs stronger and wider efforts by political scientists and IR scholars to develop the topic even more and unleash the topic's potentiality.

BIBLIOGRAPHY

Anggoro, Kusnanto. (2004). "Kedaulatan, Teritorialitas, dan Keamanan Pasca-Westphalia", *Global: Jurnal Politik Internasional*, 6(2):1-14.

Antonova, Slavka. (2013). "Internet and the Emerging Global Community of Rights: The Human Rights Debate at the Internet Governance Forum", *Journal of Philosophy of International Law,* 4(1): 89-98.

Budnitsky, Stanislav & Jia, Lianrui. (2018). "Branding Internet Sovereignty: Digital Media and the Chinese-Russian Cyberalliance", *European Journal of Cultural Studies,* 21(5): 594-613.

Bukharin, Vladislav. (2016). "The Russian's Digital Sovereignty as a Technical Basis of Information Security", *MGIMO Review of International Relations,* 6(51).

Carr, Madeleine. (2016). *US Power and the Internet in International Relations: The Irony of the Information Age*. New York: Palgrave.

Choucri, Nazli. (2012). *Cyberpolitics in International Relations*. Cambridge: The MIT Press.

Couture, Stephane & Toupin, Sophie. (2019). "What Does the Notion of "Sovereignty" Mean When Referring to the Digital?", *New Media & Society,* 21(10):2305-2322.

Deibert, Ronald J. & Crete-Nishihata, Masashi. (2012). "Global Governance and the Spread of Cyberspace Controls", *Global Governance*, 18(3): 339-361.

DeNardis, Laura. (2014). *The Global War for Internet Governance*. New Haven & London: Yale University Press.

Duarte, Marisa Elena. (2017). *Network Sovereignty: Building the Internet across Indian Country*. Seattle: University of Washington Press.

Faisal, Moch. (2008). "Dari *Anarchic Cyber Space* menjadi *Transnational Public Sphere:* Membaca Relasi antara *Cyber-space* dan *Civil Society* di Era Post Modern (Studi Kasus: *Greenpeace Online Activist*", *Global: Jurnal Politik Internasional,* 9(2): 2008.

Franklin, M.I. (2010). "Digital Dilemmas: Transnational Politics in the Twenty-First Century", *The Brown Journal of World Affairs*, 16(2): 67-85.

Franklin, M.I. (2015). "(Global) Internet Governance and Its Civil Discontents", in Joanna Kulesza and Roy Balleste, eds. *Cybersecurity and Human Rights in the Age of Cyberveillance*. Maryland USA: Rowman & Littlefield Publishers.

Gourley, Stephen K. (2014). "Cyber Sovereignty", in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Ed. Panayotis A. Yannakogeorgos & Adam B. Lowther. Boca Raton: Taylor & Francis.

Gueham, Farid. (2017). *Digital Sovereignty - Steps Towards a New System of Internet Governance*. Paris: Fondapol.

Hameiri, Shahar & Jones, Lee. (2015). "Global Governance as State Transformation", *Political Studies*, pp. 2-15.

Irion, Kristina. (2012). "Government Cloud Computing and National Data Sovereignty", *Policy and Internet*, 4(3-4): 40-71.

Juned, Mansur, *et al*. (2013). "Kekuatan Politik Media Sosial: Uji Kasus pada Revolusi Mesir 2011", *Global: Jurnal Politik Internasional*, 15(1): 68-83.

Kertzer, Joshua D. & Tingley, Dustin. (2018). "Political Psychology in International Relations: Beyond the Paradigms", *Annual Review of Political Science*, 21:319-339.

Kumar, Sangeet. (2010). "Google Earth and the nation state:Sovereignty in the age of new media", *Global Media and Communication*, 6(2):154-176.

Lewis, James A. (2010). "Sovereignty and the Role of Government in Cyberspace", *Brown Journal of World Affairs*, 16(2): 55-65.

Liaropoulos, Andrew. (2013). "Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-stakeholderism, and Power Politics", *Journal of Information Warfare*, 15(4):14-27.

Liaropoulos, Andrew. (2017). "Cyberspace Governance and State Sovereignty", in *Democracy and an Open-Economy World Order*, ed. George Bitros & Nicholas Kyriazis. Cham: Springer.

McKune, Sarah & Ahmed, Shazeda. (2018). "The Contestation and Shaping of Cyber Norms through China's Internet Sovereignty Agenda", *International Journal of Communication*, 12: 3835-3855.

Mueller, Milton L. (2012). "China and Global Internet Governance: A Tiger by the Tail", in *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, ed. Ronald Deibert, et.al., Cambridge & London: The MIT Press.

Ramadhan, Ghifari Athallah. (2018). "The Development of Concept of Territory in International Relations", *Global: Jurnal Politik Internasional*. 20(2):120-135.

Ramadhanie, Arshie. (2017). "Evolusi Konsep Keamanan Energi", *Global: Jurnal Politik Internasional*. 19(2):98-120.

Pohlmann, Norbert, et. al. (2014). "Secure Communication and Digital Sovereignty in Europe", *ISSE 2014 Securing Electronic Business Processes*, ed. Helmut Reimer, et. al. Springer.

Polatin-Reuben, Dana & Wright, Joss. (2014). "An Internet with BRICS Characteristic: Data Sovereignty and the Balkanisation of the Internet", Conference: 4th USENIX Workshop on Free and Open Communications on the Internet.

Posch, Reinhard. (2006). "Digital Sovereignty and IT-Security for a Prosperous Society", in *Informatics in the Future*. Vienna: Springer.

Schlager, Christian, et. al. (2017). "Enabling Cyber Sovereignty: with Knowledge, Not with National Products", *Digital Marketplaces Unleashed*, in ed. Claudia Linnhoff-Popien, et. al. Berlin: Springer.

Slack, Chelsey. (2016). "Wired yet Disconnected: The Governance of International Cyber Relations", *Global Policy*, 7(1): 69-78.

Stewart, Michelle. (2017). "Of Digital Selves and Digital Sovereignty: *Of the North*", *Film Quarterly*, 70(4): 23-38.

Woods, Andrew Keane. (2018). "Litigating Data Sovereignty", *Yale Law Journal*, 128(2):328-406.

Wu, Timothy. (1997). "Cyberspace Sovereignty--The Internet and the International System", *Harvard Journal of Law & Technology*, 10(3): 647-666.

Yagodin, Dmitry. (2017). "Governance and Digital Sovereignty: The Instrumental Role of Journalistic Consensus in Russia", in *Journalism and the NSA Revelations: Privacy, Security, and the Press*. Ed. Adrienne Russell, et. al. London & New York: IB Tauris.

Zarakol, Ayse. (2017). "Theorising Hierarchies: An Introduction". In *Hierarchies of World Politics*, ed. Zarakol, Ayse. Cambridge: Cambridge University Press.

Zeng, Jinghan, et.al. (2017). "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty", *Politics and Policy,* 45(3):432-464.

ACKNOWLEDGEMENT

This writing is profoundly inspired by Yann Tran and Jean-Baptiste Demaison's teaching on Cybersecurity Operational and Challenges in PSIA, Sciences Po. Several substantive and weighted discussions with Giulia Pasquali and John Jack Smith also endow this article progression and development. I also thank to Mette Frederiksen for her generous proof-reading. Chiefly, the meta-reading and meta-interpretation of this manuscript are celestially magnified by series of paramount constitutive dialogues with Mabda Haerunnisa Fajrilla Sidiq in early 2019.

NOTES:

[1] See more conceptualization of digital sovereignty in these websites EU Website https://euagenda.eu/publications/digital-sovereignty-steps-towards-a-new-system-of-internet-governance, European Council on Foreign Relations https://www.ecfr.eu/article/commentary_reality_bytes_europes_bid_for_digital_sovereignty, and Techopedia https://www.techopedia.com/definition/33887/digital-sovereignty

[2] State focused narrative can be seen in Wu, 1997; Posch, 2006; Lewis, 2010; Choucri, 2012; Deibert & Crete-Nishihata, 2012; Irion, 2012; Mueller, 2012; Pohlmann, et. al., 2014; Liaropoulos, 2013, 2017; DeNardis, 2014; Gourley, 2014; Polatin-Reuben & Wright, 2014; Bukharin, 2016; Carr, 2016; Slack, 2016; Gueham, 2017; Yagodin, 2017; Zeng, et.al., 2017; Budnitsky & Jia, 2018; McKune & Ahmed, 2018; Woods, 2018.

[3] On non state actor, there are eight prominent literatures discussing the importance of non-state actors, as follows, Couture & Toupin, 2019; Franklin, 2010; Kumar, 2010; Stewart, 2017; Schlager, et al, 2017; Antonova, 2013; Duarte, 2017.

[4] It includes Lewis, 2010; Choucri, 2012; Deibert & Crete-Nishihata, 2012; Mueller, 2012; Antonova, 2013; Liaropoulos, 2013; DeNardis, 2014; Polatin-Reuben & Wright, 2014; Franklin, 2015; Gueham, 2017; Yagodin, 2017; Zeng, et.al., 2017; Budnitsky & Jia, 2018; McKune & Ahmed, 2018.

[5] In political-security categorical issue, the texts are as follow, Wu, 1997; Posch, 2006; Kumar, 2010;

Lewis, 2010; Choucri, 2012; Deibert & Crete-Nishihata, 2012; Irion, 2012; Mueller, 2012; Pohlmann, et.al., 2014; Liaropoulos, 2013, 2017; DeNardis, 2014; Gourley, 2014; Polatin-Reuben & Wright, 2014; Franklin, 2015; Bukharin, 2016; Carr, 2016; Slack, 2016; Schlager, et al, 2017; Yagodin, 2017; Zeng, et.al., 2017; Budnitsky & Jia, 2018; McKune & Ahmed, 2018; Couture & Toupin, 2019.