[ж] CONQUEST OVER CYBERSPACE: AN UNLIMITED SOVEREIGNTY?

(SİBER UZAY ÜZERİNDEKİ HAKİMİYET: SINIRSIZ BİR EGEMENLİK Mİ?)

Jacques Kabano [*] [**]

ÖZ

Egemenlik, tanım gereği, devletin üstün gücünün sınır ötesi durumlarda, kendi toprakları içinde ve dışında kullanılmasıdır. Egemenlik kelimesi, Orta Çağ'dan beri her şeyin üzerinde olan hükümdarın - kral, prens veya imparator- gücüne atıfta bulunmak için kullanılmıştır. Ancak 1950'ler ile 1980'ler arasında siber uzay olarak adlandırılan yeni bir tür alan ortaya çıkmıştır. Bu sanal alan, diğer tüm alanlardan daha fazla karakteristik özelliğe sahipti. Zamanla, devletlerin ortaya çıkan bu yeni alanı kontrolleri altına almaları ise zorunlu hale gelmiştir.

Politik anlamda, sahip olduğu olanaklar göz önüne alındığında bu sanal egemenliğin ele geçirilmesi doğru bir harekettir. Hukuki açıdan bakıldığında, insanların toplumdaki yaşamlarını düzenleyen kuralların işleyişlerini ve içeriğini inceleyen sosyal bir bilim olan hukuk, toplumdaki herbirbireyi birbirine bağlayan ve onlara gerçek bir evrensel topluluk hüviyeti kazandıran bu "ağlar ağına" kayıtsız kalamayacaktır. Birleşmiş Milletler Şartı'nda yer alan egemen eşitlik ilkesi, modern uluslararası ilişkileri düzenleyen temel bir kuraldır ve devletlerarası münasebetlerin tüm alanlarında geçerlidir. Bu ilkenin, temel ilke olarak siber uzaya da uygulanması gerekmektedir çünkü siber uzay artık bu tür ilişkiler için pratik bir yerdir. Ancak, bu tür bir uygulanabilirliğin sağlanması için siber uzay, henüz sahip olmadığı net bir uluslararası hukuk konusu niteliğine sahip olmalıdır. Siber uzayda zaman ve mesafe gibi belirleyici faktörlerin olmaması, çoklu siber saldırı vakalarını ve siber savaş ihtimalini güçlendirmektedir. Bu alanın müphem karakteri, kabul edilebilir eşikleri geleneksel askeri operasyonlardan daha düşük olan doğrudan eylem biçimlerinden dönüşe izin vermektedir. Muhtelif aktörler arasındaki güç

[ж] Eserin Dergimize geliş tarihi: 09.10.2020. İlk hakem raporu tarihi: 01.12.2020. İkinci hakem raporu tarihi: 11.01.2021; Onaylanma tarihi: 14.01.2021.

[*] Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Doktora Öğrencisi

[**] Yazarın ORCID belirleyicisi: 0000-0002-0248-9204.

Esere Atıf Şekli: Jacques Kabano, "*Conquest Over Cyberspace: An Unlimited Sovereignty*?", YÜHFD, C.XVIII, 2021/1, s.117-139.

farklılıklarını azaltarak hatta klasik eylemlere ek olarak, asimetrik veya hibrit saldırıdan masrafsız bir dönüşe imkan verirken, failinin siber isnatlardan kaçınmak için kimliklerini gizlemesine izin verir. Bir devlet siber bölgesini ne kadar koruyabilir? Bu alan üzerinde devletin yetkisinin kapsamına ilişkin herhangi bir sınırlama var mıdır?

Bu çalışmada, sanal egemenliğe karşı klasik yaklaşımdaki egemenliği, bu tür egemenliklere ilişkin bilimsel tartışmaları ve uluslararası hukukun mevcut kurallarının siber uzaya kıyasen uygulanabilmesinin yanında bu tür egemenliklere ilişkin bilimsel tartışmalar ışığında sanal egemenlik ve klasik yaklaşımdaki egemenlik kavramlarının karşılaştırılması yapılacaktır.

***Anahtar Kelimeler**: Siber Uzay, Siber Saldırı, Egemenliğin Sınırlandırılması, Klasik Egemenlik, Sanal Egemenlik*

ABSTRACT

Sovereignty, by definition, is the exercise of the supreme power of the state inside and outside its territory, in case of extraterritoriality. The word 'sovereignty' since the Middle Ages, was used to refer to the power of the sovereign, who was overall; the king, prince, or emperor. However, between the 1950s and 1980s, a new kind of space dubbed cyberspace emerged. This virtual territory engaged more personalities than any other space. Over time, it became imperative for States to include this newly gained space under their control.

Conquering this virtual sovereignty given its potentials, politically speaking, equals the right move. From a legal perspective, Law as a social science that studies the mechanisms and contents of the rules through which humans regulate their lives in a community, cannot be alien to this 'network of networks' that connects each sub-community and brings them together in a genuine universal community. The sovereign equality as a principle under the Charter of the United Nations is an ultimate rule governing modern international relations and valid in all spaces of interstate exchanges. It is imperative for this principle and its essence to be applied to cyberspace because cyberspace is now the right place for diplomacies. However, to achieve this kind of applicability, cyberspace needs to have a clear international law position, which it does not have by the time. The absence of determining factors such as time and distance within cyberspace strengthens the multiple occurrences of cyber-attacks and the possibility of cyber warfare. Its opacity allows the return of direct modes of action whose acceptance thresholds are lower than conventional military operations. It allows an inexpensive return of the asymmetric or hybrid offensive, by

reducing the power differences between different players, or even in addition to conventional military actions, while allowing its author to hide their identities to avoid cyber attributions. How far would states go to protect their cyber territory? Are there any limitations to this conquest? In this paper, a comparison between sovereignty in the traditional approach and virtual sovereignty, scholarly discussions on these types of sovereignties, as well as the analogy to apply existing rules of international law to cyberspace, will be established.

Keywords: *Cyberspace; Cyber-attack; Limitation of Sovereignty, Classic Sovereignty; Virtual Sovereignty*

***

INTRODUCTION

We are confronted at the beginning of the 21st century with the legacy that the last century left us, setting the trend in technology and facing an imminent change in the social, cultural, and economic paradigm. In the current context where multi-polarization, economic globalization, cultural diversification, and computerization are gaining in-depth, and where the global governance system is undergoing profound changes, humanity is entering a new era of the information revolution. Digital platforms offer a new square of exchanges that strengthens the free and direct expression of citizens. They compete with traditional intermediary organizations: unions, political parties, and various associations. This square is called cyberspace. Cyberspace can be defined *as "a global and interconnected network of information, communication infrastructures, including the Internet, telecommunications networks, computer systems, and the information located there*."[1]

There are so many factors to limit the sovereignty of States; such as limitations of State sovereignty in the economic sphere through liberalization-privatization and multinational corporations and international economic organizations, limitations brought by ratified conventions and treaties, and other factors such as globalization where socio-economic cultural exchanges between citizens of different countries are inevitable. However, this paper will focus on those limitations that involve States directly and hit their sovereignties, either directly imposed on them or self-assumed responsibilities. For that reason, it will only discuss limitations by unilateral international obligation where States limit the extent of their sovereignty with a unilateral commitment which at the end becomes binding

[1] N. Melzer, Cyberwarfare and international Law, *UNIDIR*, 2011, p. 4

and no chance to revoke, by limitation not to use force and settle their disputes peacefully, and finally by limitations imposed to them of not to interfere into other States' internal matters. After establishing a comparison between traditional and virtual sovereignty, then an analysis of these limitations in the framework of cyberspace will follow.

A. CLASSIC APPROACH ON SOVEREIGNTY

The State is not subordinate to any other entity and is subject only to its own will. The State exercises its supreme authority over a given population and a territory.[2] Sovereignty, therefore, means independence, the ability not to have the will of others imposed on them (principle of non-intervention), and freedom of internal organization. External sovereignty is based on the principle of equality between States, whatever their effective power, resources, or demography, and therefore regardless of de facto inequalities.[3] This equality also means that States are not subject to any higher authority even outside of it. States are theoretically subordinate to only standards which they have defined or to which they have consented.[4] In this sense, international relations are thus characterized by horizontal relations between independent political groups.[5] The concept of sovereignty was forged, to sum up, this singular power which is posed as the distinctive sign of the State, an abstract entity erected as the depositary of social identity and the source of all authority: it means that the State has supreme power of domination, that is to say of an irresistible and unconditional power which not only imposes itself on the subjugated, without them being able to escape from it but also escapes any bond of subordination, to any relationship of dependence.

This affirmation of the sovereign power of the State does manifest itself internally: the legal order of the State gradually imposes its supremacy, by replacing, or at least by superimposing itself, on the pre-existing legal orders

[2] A. Franceschet, "Sovereignty and Freedom: Immanuel Kant's Liberal Internationalist 'Legacy.'" Review of International Studies 27, no. 2 (2001): 209–28. doi:10.1017/S0260210500002096

[3] Y.S. Hakyemez, Mutlak Monarşilerden Günümüze Egemenlik Kavramı: doğuşu, gelişimi kavramsal çevresi ve dönüşümü, Seçkin Yayıncılık, Ankara, 2004, p. 66-68.

[4] J. Robert, Marxist-Leninist Doctrine and The Soviet Theory of Sovereignty. In: The Soviet Concept of Limited Sovereignty from Lenin to Gorbachev. Palgrave Macmillan, London, 1990, p. 211.

[5] E. KURUBAŞ, "Uluslararası İlişkiler Düşüncesi ve Dünya Politikasında Değişimi Anlamak", Kırıkkale Üniversitesi Sosyal Bilimler Dergisi, Cilt 2 Sayı 1 (2012), p.16-19. https://dergipark.org.tr/tr/download/article-file/181031 accessed 16 September 2020

and by becoming the sole legal framework of reference for the whole community; as Kelsen pointed out, the State tends to become "the total legal order,"[6] which integrates and brings together all others. It also manifests itself externally. Classic international law is built on the idea of State sovereignty, sovereignty which does not mean here a supreme power as in the internal order, but the absence of any link of subordination:[7] the sovereign State does not recognize any authority superior to its own and any limitation of that authority can only come from its consent; international society thus appears to be a fundamentally "anarchic" society, made up of equally sovereign entities and within which there is no power of command.

This classic theory of sovereignty and the theory of State[8] itself has been the subject of strong criticism in legal doctrine, without eradicating the underlying conception of law.

The most systematic criticism is undoubtedly that of Duguit, who rejected the very idea of sovereignty and beyond the very concept of the State. According to him, the State is in reality only an abstract entity placed behind the physical person of the rulers to legitimize the use of coercion; the legal norm is therefore not the expression of sovereign power, but only the manifestation of the power of domination held, in fact, by the rulers.[9] However, insofar as he admits the privilege of the precondition and affirms that obedience is due to any act emanating from the rulers, the commands of power are presumed to conform to objective and legitimate law, Duguit indeed surreptitiously reintroduced the idea of public sovereign power.[10]

Kelsen also challenged the classic theory of sovereignty insofar as it conceives of the State as a mystical entity which, hidden behind the law, would order its creation and give it binding force: in reality, it is the legal order itself which regulates the conditions of production of legal norms and makes the State exist as a "*legal person*" to whom these acts will be imputed, which means that "*the law regulates its creation*"; the State is thus, in the end, " *the national legal orders find the reason for their validity in the international legal order, which at the same time defines their spheres of*

[6] H. Kelsen, The Pure Theory of Law and Analytical Jurisprudence, Harvard Law Review, Vol. 55, No. 1 (Nov. 1941), pp.44-70. Available at https://www.jstor.org/stable/1334739?seq=1 accessed 9 December 2020.

[7] O. Beaud, *La puissance de l'État*, PUF, Coll. Léviathan, 1994, p.16

[8] For more about State theory, especially discussions and criticisms, see: O. Uygun, Devlet Teorisi, On Iki Levha Yayincilik, İstanbul, 2015, pp.189-286

[9] L. Duguit, *Traité de droit constitutionnel,* 3rd Ed., vol.5, Fontemoing, 1927-1930, p.67,79.

[10] Duguit, p. 79.

validity, the international legal order must be superior to each national order."[11]

However, a further step is required. The relationship established between State formation and legal monism is undoubtedly schematic: despite its totalizing claims and its quest for exclusivity, the State legal order has never succeeded in reducing to itself and condensing all legal phenomena; it has always been caught in the rear and bypassed by norms forming in other places and partly escaping its mediation. And these breaches, which lie below, on the fringes and beyond the State, are widening in contemporary society. State law is dominated by an increasingly dense set of norms, which contribute to further limit the sovereignty of States.

No doubt international law is at first glance perfectly compatible with the principle of sovereignty since it was built on the foundation of this principle. It implies that the State cannot be obliged without its permission: on the other hand, nothing prevents it from entering into the agreements it deems useful with other States, as well as from respecting certain rules relating to custom or jus cogens; as the *International Permanent Court of Justice* ruled in its first judgment of August 17, 1923, "*the right of entering into international engagements is an attribute of State sovereignty*".[12] International law is therefore not, like domestic law, the expression of supreme power, but the product of the meeting of sovereign wills: it is an "*inter-state*" law, created from the agreement of States.

This approach is, however, too simple: beyond their sovereignty in principle, States are required to enter into the agreements necessary for their development and to forge links of interdependence that they cannot break unilaterally; an international order has indeed been formed from a set of conventional and unconventional sources, and this order weighs as a constraint on States. Supra-state law takes on even greater importance from the moment when, as in Europe, regional groups have been built above States: this construction results in the existence of a specific and superior legal order to that of States;[13] the extreme density of community law, which

[11] H. Kelsen, 1941, p. 70

[12] S.S. "WIMBLEDON" Judgment of 17 August 1923 (Series A, No. 1), First Annual Report of the Permanent Court of International Justice (1 January 1922 – 15 June 1925), Series E, No. 1, pp. 163-168. Available at https://legal.un.org/PCIJsummaries/documents/english/5_e.pdf accessed 5 October 2020.

[13] Summaries of EU Legislation, Precedence of European Law, 1 January 2010. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14548 accessed 5 October 2020.

has become more and more invasive, as evidenced by the proliferation of regulations and directives, which States are forced to apply under penalty of sanctions, shows that this regulatory space is tending to become constantly expanding to the detriment of the State legal space.

Applied to law, the concept of sovereignty traditionally has two inseparable faces, referring to one another as if by mirror effect:[14] as an order of constraint, the law implies the existence of a supreme order of which it is supposed to derive any legality; and the existence of this order is the guarantee of the normative power of law. However, the law could no more be locked in the folds of a supreme and totalizing order than it could be reduced to the sole constraint: vector of institutionalization, the law is found at very different levels of the social structure; and the coordination of social activities can be carried out in various ways, more or less constrained.

B. VIRTUAL SOVEREIGNTY

In theory, the legal structure can easily adapt to technological changes and it is up to the jurisprudence to carry out the necessary adjustments to make the system viable in the context of conflicts and specific transactions. The interpretation of the rules of international law within the framework of cyberspace presupposes above all that these rules are applicable. Although there is no convention or rules specifically relating to cyberspace, this does not mean that cyberspace is a zone of "lawlessness", in which there is a legal vacuum and where no applicable rules exist.

The United Nations Intergovernmental Group of Experts (GGE), established by a resolution of the General Assembly in 2003[15], has been tasked with examining the risks that arise or could arise from cyberspace and possible cooperative measures to deal with them. In this report, the group notably declared that: "*international law and, in particular, the United Nations Charter applies to the use of ICTs by States. This affirmation is essential to maintaining peace and security and promoting an open, secure, stable, accessible and peaceful ICT environment".*[16]

Article 2 (1) of the *Charter of the United Nations* thus States that "*the organization is founded on the principle of the sovereign equality of all its*

[14] J. Chevallier, *Souveraineté Et Droit*, In D. M. Desgrées du Loû, *Les évolutions de la souveraineté,* Montchrestien, Coll. Grands Colloques, 2006, pp. 203-219. Available at: https://hal.archives-ouvertes.fr/hal-01728232/document accessed 5 October 2020

[15] A/RES/58/32.

[16] UN GGE Report 2013 (A/68/98*), §19 (adopted by the GA: UN Resolution A/RES/68/243 on the UN GGE Report 2013)

Members". Tallinn manual editors consider that States also exercise their sovereignty in cyberspace, at least over their cyberinfrastructures.[17] In this sense, the bigger the cyberinfrastructures, the bigger the cyberspace. Cyberspace, while providing enormous prospects for humanity, also postures various new problems and contests. Safety and stability in cyberspace are now a matter of global concern that involves the sovereignty, security, and development interests of different countries. The Internet suffers from problems that become more and more severe, such as unbalanced development, imperfect rules, and irrational order.

Along with the law, power constitutes the other factor regulating international relations. The power of the State can be measured against the level of freedom of action it has; it corresponds as much to its ability to coerce as to its ability to influence the behaviors of other actors. The power of a State therefore determines its ability to guide the course of international relations. Today, the control of information and the networks that it uses, as well as that of artificial intelligence, are becoming essential components of the power of States, both to influence the various actors and to legitimize their action. In the same logic, the NGOs, transnational firms, IOs, and civil society can also benefit from the use of information technologies to spread their fundamental ideologies.

It is useful to make a distinction between the governance "of" the Internet as a technical system (the rules applicable to the logical layer: protocols, naming systems, addressing, etc.) and, on the other hand, governance "on" the Internet, i.e., the rules applicable to what Internet users do in cyberspace (issues of privacy, freedom of expression, security, etc.). Overall, the system of governance "of" the Internet, which is based on an effective ecosystem of organizations, including ICANN[18], works quite well. There are certainly always improvements to be made and specific questions remain, notably on the status of ICANN, which is a US multi-stakeholder group. However, the technical governance system that supports Internet activities has managed to allow the network to grow from a few hundred

[17] Tallinn Manual – Rule 1 – Sovereignty: « *A State may exercise control over cyberinfrastructure and activities*
within its sovereign territory ». This means that a State regulates the use and access to infrastructure located on its territory as it wishes. (M. N. Schmitt (ed.)., Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations, (Michael N. Schmitt ed., 2d ed. 2017)

[18] *The Internet Corporation for Assigned Names and Numbers (ICANN*) is the organization that coordinates the Internet address and domain name system (www.icann.org).

users to three billion without major technical problems.[19]The reason for this growth goes side by side with the evolution of technology itself. As the technology evolved new versions of applications, new technical solutions like antiviruses, and new features in telecommunication devices have been added to markets so that users can have more choices available to their needs and their financial situations.

On the other hand, there is a problem concerning governance "on" the Internet (or in cyberspace): there are no instruments, nor even the spaces for dialogue so that the various actors concerned by the activities on the Internet can discuss their ways of cooperation among themselves. Certainly, national governments exist and their laws must apply, but cyberspace is fundamentally cross-border and there are no tools to deal with normative tensions such as settling questions regarding privacy, freedom of expression, and the fight against cybercrimes. Conferences or intergovernmental organizations fail to deal seriously with these issues because governments do not agree with each other. Today there is a pile of national laws seeking to reaffirm national sovereignty or sovereignties, at the risk of encroaching on the sovereignty of other countries. The revealing element in this regard was the paroxysm of the extraterritorial extension of the sovereignty of a country, the *United States*, represented by the activities of the *National Security Agency* (*NSA*).[20]

The fact that internet service mega-companies[21] from some countries like the US and China are used by countries and *de facto* they apply the law of those countries outside of them, is completely contrary to the very principles of sovereignty and non-interference. For all many actors, the application of surveillance through operators based in the United States is in fact, a violation of sovereignty.[22]

[19] Interview with Bertrand de La Chapelle on Sovereignty in the cyberspace. He was a member of the board of directors of ICANN from 2010 to 2013. F. Douzet*: Souveraineté et jurisdiction dans le cyberespace*, *Hérodote*, n° 152-153, La Découverte, 2014. https://www.cairn.info/revue-herodote-2014-1-page-174.htm accessed 4 October 2020.

[20] D. Kedmey, Report: NSA Authorized to Spy on 193 Countries, 1 July 2014. https://time.com/2945037/nsa-surveillance-193-countries/ accessed 6 October 2020.

[21] A. Bloomenthal, World's Top 10 Internet Companies, 18 September 2020, https://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp accessed 5 October 2020.

[22] F. Douzet, 2014

The United States, European countries, European Union[23], Japan, and several other OECD countries have not changed their general position on how internet governance should work, they are in favor of multi-stakeholder mechanisms that bring together governments, civil societies, and the private sectors. On the other hand, China and Russia, but also Saudi Arabia and a few others, rightly reaffirm what has been the reality for a very long time: "*Public policy matters are the exclusive domain of States, and therefore, if international regimes are to be defined, it is up to governments alone to decide governance on the Internet.*"[24] Many countries have not taken a position, so do not have a clear idea of what they want.

C. COMPARISON OF CLASSIC APPROACH ON SOVEREIGNTY AND VIRTUAL SOVEREIGNTY IN TERMS OF THEIR LIMITATIONS

Whether in practice or doctrine, the notion of sovereignty stands as the most debatable topic in the history of public international law.[25] Since the emergence of the first "independent human groups, endowed with a supreme authority which could be individual or collective"[26], the term "sovereignty" has known "*a long and eventful history during which it took on meanings, connotations, and ideas of different tones depending on the context and the objectives of those who employed it* ".[27]

National sovereignty is opposed to the notion of popular sovereignty, which in turn involves mechanisms of direct democracy, such as citizens' assemblies, imperative terms, or referendums. The notion of national

[23] **Communication from The Commission to The European Parliament, The Council, The European Economic, and Social Committee and The Committee of The Regions Internet Policy and Governance Europe's Role in Shaping the Future of Internet Governance (Text with EEA Relevance) /* COM/2014/072 Final,** https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014DC0072&from=DA **accessed 9 December 2020.**

[24] E. Saakashvili, "The global rise of Internet sovereignty", Authoritarian Tech, 21 March 2019. Available https://www.codastory.com/authoritarian-tech/global-rise-internet-sovereignty/ accessed 6 October 2020.

[25] H. Steinberger, Sovereignty, in Encyclopaedia of Public International Law by R. Bernhardt, Elsevier, vol. 4, 2000, p. 500.

[26] TRUYOL and SERRA, Sovereignty, in Fundamental Legal Vocabulary of Law, APD, t. 35, 1990, p. 313. These are according to these authors, the first examples of human societies established under a supreme authority such as, for example, the Egyptian, Greek, or the Roman States.

[27] W. M. Reisman, "Sovereignty and Human Rights in Contemporary International Law", American Journal of International Law 84, no. 4 (1990): 866–76. doi:10.2307/2202838

sovereignty legitimizes a political body with real autonomy in decision-making. In the reflection on sovereignty, the Nation-State holds a central place, since it is also a founding element that serves as a basis for legal and political reflection on the power of the State and therefore on sovereignty. Historically speaking, this supports the absolutism of sovereignty by giving a unitary character to its holder. Sovereignty, in its original sense, is defined as indivisible, supreme, absolute, and inalienable power.[28] As it has been mentioned in the introduction of this paper, sovereignty with absolute nature (national sovereignty) has always met different challenges in the international arena. In comparison with Virtual sovereignty, the following section will analyse whether or not virtual sovereignty has a legal back up.

1. A Sovereignty Limited by Unilateral International Legal Order

The subject of the objectivity of the obligations resulting from unilateral acts of States, especially since the jurisprudence of the International Court of Justice in the cases of nuclear tests, opposing New Zealand[29] and Australia[30] to France, inspired much interest among the internationalists.

As to the question of their legal effects as a source of subjective rights and obligations, an affirmative answer is possible insofar as unilateral acts of States can be a source of subjective obligations.[31] If the unilateral act of the State implies commitments towards other subjects of international law, it would have the obligation to respect its commitments and its obligations which may always be imposed on it within the limits admitted by international law.[32] While the obligations that unilateral acts create are subjective, their existence is objective. Indeed, the fact that these obligations result from unilateral acts does not imply that they have a subjective existence, dependent only on the will of the State which is at the origin of the unilateral commitment. Indeed, the State which commits unilaterally can no longer take back its commitments in the same unilateral manner.[33]It

---

[28] Id

[29] Nuclear Tests (N.Z. v. Fr.), 1973 I.C.J. 457 (Dec. 20) online: http://www.worldcourts.com/icj/eng/decisions/1974.12.20_nuclear_tests2.htm accessed 6 September 2020.

[30] Nuclear Tests (Australia v. France), Judgement, I.C.J. Reports 1974, p. 253., online: https://www.icj-cij.org/files/case-related/58/058-19741220-JUD-01-00-EN.pdf accessed 6 September 2020.

[31] Blake, 1999 Inter-Am.Ct.H.R., (ser C.) No. 48., p.5 (Jan. 22, 1999)

[32] ABI-SAAB (G.), *La souveraineté permanente sur les ressources naturelles*, in *Droit international, Bilan et perspectives*, M. Bedjaoui (Ed.), t. II, Pedone, 1991, pp. 639-661.

[33] P. DAILLIER, M. FORTEAU and A. PELLET, *Droit international public*, LGDJ, 8th Ed., 2009, pp. 406-413

effectively follows the logic given by the Court that the requirement to comply with a unilateral commitment is no longer an individual choice which the State can also decide unilaterally; it becomes an obligation for it to execute.

Thus, no less than any other international obligation, obligations arising from unilateral acts of States are also binding on their creator in an objective manner.[34] This commitment becomes a burden that the State cannot revoke unilaterally in its so-called State sovereignty. By losing the power to revoke what it has independently initiated, its sovereignty is restricted.

What about virtual sovereignty, can State's unilateral acts in cyberspace become a reason to restrict its virtual sovereignty? The answer is yes and this is why: According to the commentary of article 12 of the *Draft Articles on Responsibility of States for Internationally Wrongful Acts* responsibilities *may arise for a State by a treaty and by a rule of customary international law or by a treaty and a unilateral act*.[35] The *International Law Commission*'s commentary 3 on this draft's article 12, stressed that whatever the origin of these unilateral acts so long as they have been initiated by a competent authority of the State and generate a result that breaches international law, these acts will constitute obligations to be carried out by that State regardless of whether these actions were unilateral or not. Since the origin is ruled out, the cyber origin can come in. These will include cyber operations that might be launched by a State. However, as it is known in the case of international obligation, for a State to be liable for any action; attributing those actions to a specific State is very crucial.

Here comes the very first difference between classic sovereignty and virtual sovereignty. It is very problematic to attribute cyber operations to States because, for dark operations, actors will often hide their identities from any track. In addition to this, States might pay individual hackers to do their dirty works and stay clean. Examples of this, Estonia[36] in 2007 and all

[34] L. Bal, *Le mythe de la souveraineté en droit international : la souveraineté des Etats à l'épreuve des mutations de l'ordre juridique international*, Droit, Université de Strasbourg, 2012. Available online at: https://tel.archives-ouvertes.fr/tel-00721073/document accessed 4 October 2020.

[35] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries 2001, session (A/56/10), https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf accessed 4 October 2020

[36] R. Ottis, Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia,

cyber operations against Ukraine[37] on a very satisfying line of patterns, Russia was behind them but up to this time, a 100% attribution of these cyber operations to the Russian government has never been established.

Another aspect of sovereignty in cyberspace is the ability of actors (mostly the State in this case) to neutralize the physical infrastructures that allow it to function. According to the Tallinn Manual handbook on the application of international law on cyber operations, experts concluded that at least a State has sovereignty over cyberinfrastructures available in their legal spaces. Within the logic of this text cutting the Internet in a given territory (through the interruption of data transfers by international optical fibers) may be a gesture of sovereignty by a State actor whose territory in which those infrastructures reside, these actions may have repercussions on other actors since such infrastructures are shared between the States. Is it therefore the exercise of State sovereignty, an attack, or an act calling into question the stability of the international system?

Depending on which side you are supporting, this would mean different things to different sides. Although this is in a State's unilateral capacity to exercise such sovereignty, the real deal here is the degree of damage such an act may cause to other States. Besides, this would undermine the principle of cooperation between States as always publicized by the United Nations. For the actor of this action, this is a pure exercise of sovereignty over its infrastructure, for the rest, this is an attack and instability of the international system. The end of this debate is not granted.

2. A Sovereignty Limited by Prohibition to Use Force

For a long time, international law recognized in States a competence to engage in wars. The legal theologians of the School of Salamanca [38]of the 16th and 17th centuries, Francisco Vitoria, Luis de Molina, Francisco Suarez, were interested in the conditions of the legality of the war; they developed the doctrine of *ius ad bellum*. They took up Thomas Aquinas' theory of "just war"[39] under which three conditions should be completed; 1) *it must be*

https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformation WarfarePerspective.pdf accessed 18 September 2020

[37] T. Maurer, Cyber Proxies, and the Crisis in Ukraine, New America, 2018. https://www.ccdcoe.org/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf accessed 18 September 2020

[38] J. B. Scott, *The Spanish origin of international law: Francisco de Vitoria and his law of nations*, Oxford: Clarendon Press, 1934, p.288

[39] R. Cox, "Historical Just War Theory up to Thomas Aquinas", Saint Andrew, 2015, pp. 1-26. Available:

decided by the authority of a prince, that is to say by a sovereign authority, 2) *it must have a just cause*, in the sense that it must either be the consequence of an injury or breach of international responsibility, 3) *it must have a good intention*; it must therefore aim for the common good. However, a few centuries after Aquinas, relations between States met substantial changes through history and the concept of "war" became the last resort thing to do after all negotiations have failed. And with the end of the second world war, the countries united in a new international organization, the UN, and banned the use of force to resolve disputes.

The principle of the ban on the use of force is a centerpiece in the structure of the collective security system set up in 1945. Numerous resolutions[40] of the *United Nations General Assembly* have recalled the existence of this principle which, according to the *International Court of Justice*, constitutes a "*cornerstone of the Charter of the United Nations*"[41]. In 1986, the ICJ even found that it had acquired customary value.[42] The principle of the prohibition of the use of force therefore has the dual status of a conventional norm and a customary norm. Finally, given its importance, this norm is often cited as an example of a jus cogens rule[43], in other words as an overriding principle, a rule that cannot be derogated from.[44]

https://researchrepository.standrews.ac.uk/bitstream/handle/10023/11776/Ch05_Cox_Historical_Just_War_Theory_up_to_Aquinas.pdf?sequence=1 accessed 7 October 2020.

[40] The principle of the prohibition of the use of force has been reaffirmed by many United Nations General Assembly resolutions: 2625 (XXV) of 24 October 1970, 2660 (XXV) of 7 December 1970, 3314 (XXIX) of 14 December 1974, A / RES / 31/9 of 8 November 1976, A / RES / 33/72 of 14 December 1978, A / RES / 42/22 of 18 November 1987.

[41] Armed Activities on the Territory of the Congo (the Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 59 section 148. Online: https://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf accessed 6 September 2020.

[42] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. the United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 92. Section 193. Online: https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf accessed 6 September 2020.

[43] In principle when a rule has reached the status of jus cogens it accepts no derogations, meaning that no treaty and no consent is allowed to violate this rule. However, when it comes to the use of force (art. 42, 51 of the UN Charter and art. 101, 105, and 110 of the UNCLOS for example allow the use of force to a certain extent. Read more: Helmersen, Sondre Torp. "The Prohibition of the Use of Force as Jus Cogens: Explaining Apparent Derogations." Netherlands International Law Review 61, no. 2 (2014): 167–93.

[44] Id.

With the creation of the United Nation, the power of a sovereign authority to wage wars except in specific cases determined by its Charter was revoked. Article 2(4) of the *Charter* proclaims the general character of the principle of the ban on the use of force: "*Members of the Organization shall refrain, in their international relations, from resorting to threats or the use of force, either against the territorial integrity or political independence of any State or in any other manner incompatible with the purposes of the United Nations*". This article refers not to war but to force. The concept of force used by Article 2 (4) is not defined in the Charter and to date, there is no unanimous interpretation of what is meant by the concept of "force" in the international community.

The dictionary offers different definitions of the word "force". It can be the use of "p*ower, violence, compulsion, or constraint exerted upon or against a person or thing. Power dynamically considered that is, in motion or action; constraining power, compulsion; strength directed to an end*".[45]

In the context of international law, the same tension is felt over the interpretation to be given to the term "force". Relatively broad, it can encompass both forces by arms and also economic force or other coercive measures. Since the scope of the term "force" cannot be defined with certainty, one must observe how the term is used in the treaty and take into account its object and purpose.

Depending on the way you wish to interpret article 2(4) of the Charter, two ideas may be entertained. According to a verbatim interpretation of the terms of article 2 (4), one may argue that the drafters of the *Charter* intentionally chose not to speak of "armed" force in article 2 (4) to prohibit the use of force on a broader scope. If the drafters had meant only to refer to the use of military force, Article 2 (4) would have included the adjective "armed". For the second opinion supported by authors like Schmitt,[46] the interpretation of this article must follow the guidelines and the spirit of the *UN Charter*'s preamble, which explicitly refers to the prohibition of armed force.

According to the first reasoning on the meaning of the force, as stipulated in the UN Charter, any action of one State that threatens the sovereignty of

[45] WEST's Encyclopedia of American Law, the definition of "Force" https://legal-dictionary.thefreedictionary.com/Force accessed 7 October 2020.

[46] M. N. Schmitt, Computer network attacks and the use of force in international law: Thoughts on a normative framework, *Columbia Journal of Transnational Law, Vol. 37*, 1999, p. 21-26. https://apps.dtic.mil/dtic/tr/fulltext/u2/a471993.pdf accessed 7 October 2020.

another sovereign State can be considered as a force. Cyber-attacks are operations that can put the sovereignty of a country in danger. Since the qualification "use of force" is independent of the type of weapons employed, cyber operations should, in theory, be able to constitute a use of force. Nevertheless, it is not possible to conclude that a cyber-attack always constitutes a use of force, since these can be carried out by means and on a scale that varies. It is therefore a case of analysing cyber-attacks individually.[47]

What conditions should be examined to define whether a cyber-attack constitutes a use of force? There are different theories about this. The so-called "instrument-based" approach is concerned with the methods used to conduct an attack. A cyber act becomes the use of force if the act in question exhibits the corporeal features conventionally related to an armed operation.[48] A second theory is concerned with the target of the operation (strict liability approach). When it targets critical national infrastructure, the operation is tantamount to the use of force.[49] Finally, the third method takes into account the consequences of the attack as a whole (consequence-based approach) and seeks to analyze whether the effects of the operation are serious enough to qualify it as a use of force.[50]

The sovereignty of a State over its cyberspace infrastructures does not allow it to use such infrastructures to violates the rights of other States especially undermining their sovereignties. Not all operations reach the use of force threshold as provided in article 2 (4). An effective legal framework for qualifying cyber use of force operations should consider the seriousness of the consequences of an attack for State sovereignty and international peace and security. It would also take into account the reversible or non-reversible effects of a cyberattack as well as the target of an attack, without applying the target-based approach which ignores the consequences. A cyber-attack would thus be qualified as the use of force when it aims to

[47] CSIS, Significant Cyber Incidents Since 2006, Center for Strategic and International Studies (CSIS) | Washington, D.C. https://csis-website-prod.s3.amazonaws.com/s3fs-public/201002_Significant_Cyber_Events_List.pdf retrieved 7 October 2020

[48] M. Benatar, Use of Cyberforce: Need for Legal Justification? Goettingen *Journal of International Law* 1, 3, 2009, p. 388.

[49] D. B. Hollis, "why states need an informational law for information operations", *Lewis & Clark Law Review, Vol. 11,* p. 1041. https://law.lclark.edu/live/files/9551-lcb114art7hollis.pdf accessed 6 October 2020.

[50] Tallinn Manual, Rule 11 – Definition of use of force: "*A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force*".

cause large-scale and irreversible physical damage by attacking the computer systems and networks on which a society depends for its proper functioning. A-State is, therefore, prohibited to use force either by classic armed force or by cyber operations that may be qualified as use of force. In both cases, its sovereignty is restricted.

3. A Sovereignty Limited by Prohibition to Interfere in Other States' Internal Matters

The principle of sovereignty began to take root in the relations between States with the Treaties of Westphalia which reshaped the map of Europe in 1648.[51] Sovereignty is exercised over a given territory and, on this territory, only the internal actors in it can exercise the attributes of public power. The rule is that of non-intervention of external actors in the activities of a sovereign State.

Any reason that may allow other States to meddle with internal matters of a State is a typical violation of the principle of sovereignty. Historical examples show that interventions mostly military have been used in the territory of other States with or without their prior authorizations.[52]The legitimacy of these interventions is not our focus in this paper. The *raison d'être* of this concern is that in international law, the principles of sovereignty and non-intervention have always conflicted. The existence of one excludes the presence of another.

As discussed above, not all cyber-attacks constitute the use of force, let alone armed aggression. However, these acts are not necessarily in conformity with international law. These attacks may fall into a category other than the use of force, namely that of intervention prohibited by international law. Few authors have focused on the principle of non-intervention applied to cyberattacks, compared to the principle of prohibiting the use of force.[53] Generally, the principle is quickly evoked as constituting a category for cyber-attacks not equivalent to the use of force, without further reflection on what the principle of non-intervention encompasses and how it finds to be applied in the cyber background.

---

[51] D. Hassan, The Rise of the Territorial State and The Treaty of Westphalia, Yearbook of New Zealand Jurisprudence Vol. 9, pp. 62-70, 2006.
https://opus.lib.uts.edu.au/bitstream/10453/3289/1/2006006060.pdf accessed 7 September 2020.

[52] M.N.S. Sellers, Intervention under International Law, 29 Md. J. Int'l L.1., 2014, p. 6-11. Available at: http://digitalcommons.law.umaryland.edu/mjil/vol29/iss1/3 accessed 7 October 2020.

[53] *Id.*

A typical example of a cyberattack that may be characterized as an intervention prohibited by international law is operations targeting the computer systems of New Zealand's Stock Exchange Market in 2020[54], the operations happened for four days and one of them forced the State to halt its stock exchange from 11.30 am to 3 pm. Although the officials did not attribute these operations to any State besides mentioning "overseas hackers", the failure to stop them raised the attention of the government to rethink its security systems. The same thing happened to its neighboring country, Australia[55]. These events have to be considered as interventions, in particular, because they have been carried out without causing loss of human life or the destruction of property in a direct way, which could not necessarily be avoided by a kinetic operation with the same goal. It does not constitute the use of force or military aggression, since its effects are confined to the economic domain. On the other hand, it would be an intervention prohibited by international law, since undermining the economic and financial system of the victim State constitutes interference in its internal affairs. Another practical example as mentioned earlier in this paper would be to apply the law of another country only because the internet line used, is from that country.

In the classic approach of sovereignty, a State may face a violation of its sovereignty because a specific State (States) has/have interfered in its internal matters, therefore breaching its supreme authority and integrity. In virtual sovereignty, the principle of non-intervention makes it possible to qualify cyber-attacks that do not reach the threshold for the use of force as illegal acts under international law. However, given the lack of clarity attached to the principle of non-intervention, mainly, the attribution problems, it remains difficult to apply in cyberspace. Currently, for lack of being able to qualify an operation carried out by a non-state group, or quite simply for lack of being able to attribute an operation to a State, the principle cannot apply and does not open up a response to the victim State.

[54] Reuters Staff, New Zealand bourse resumes trade after cyber-attacks, government activates security systems, Technology News, 28 August 2020. https://www.reuters.com/article/uk-nzx-cyber/new-zealand-bourse-crashes-for-fourth-day-after-cyberattacks-idUSKBN25O03Q accessed 10 September 2020.

[55] Id.

CONCLUSION

Whether classic or virtual sovereignty, the concept of a nation, a State, or a republic whatever denomination it may be given, is built on the principle of sovereignty. As discussed in this paper, cyberspace and cyber-attacks do not escape the application of international law. However, cyberspace responses to cyberattacks remain limited, in particular by the problem of identifying and attributing cyberattacks. In this paper, it has been mentioned that the principle of sovereignty has many exceptions and only three of them were discussed. After an established comparison, it can be concluded that like other fields of operations (land, air, sea, outer space) cyberspace operations are unique, and based on this uniqueness applying international law by analogy to such operations is not only confusing but also unhelpful. The territories of the digital world hold the most valuable and profitable deposits of the contemporary economy. Of course, the raw materials of the material economy continue to flourish, but they are not sustainable and their lifespan is getting shorter every day. On the contrary, the resources of the intangible economy continue to grow faster than before. The globalization of the internet does not allow strictly national solutions to flourish, nor regional solutions. As it can be observed, the failure to take this into account, at an international level allows the global nature of the Internet to generate disorders and to preserve the fundamental inequality between States which is the characteristic of the current situation.

The current distribution of IT resources breaks the principle of State sovereignty. Indeed, the territories of the digital world are almost totally dominated by a few giant firms of the star-spangled banner. Faced with the unprecedented danger that this unprecedented domination may represent for the sovereignty of other States, the community of nations, founded on the search for balance, should propose a new international organization with the mission of easing tensions and co-regulation of the resources of the digital world. There is a necessity for a whole new treaty regarding cyberspace which would provide common definitions according to cyber perspectives and common guidelines to be applied to certain cyber operations, especially those with enormous serious damages. An international organ like a court specifically dealing with cyber operations would also be a viable mechanism to develop legal scholarship and doctrine on cyber matters. Technology evolves quickly and always comes with new challenges; the law should not wait for a disaster to happen to be ready for the rapid change of technology.

BIBLIOGRAPHY

ABI-**S**AAB (G.), *La souveraineté permanente sur les ressources naturelles,* in Droit international, Bilan et perspectives, M. Bedjaoui (Ed.), t. II, Pedone, 1991, pp. 639-661.

Armed Activities on the Territory of the Congo (the Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 59 section 148. Online: https://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf accessed 6 September 2020.

BAL, Lider**,** Le *mythe de la souveraineté en droit international : la souveraineté des Etats à l'épreuve des mutations de l'ordre juridique international*, Droit, Université de Strasbourg, 2012. Available online at: https://tel.archives-ouvertes.fr/tel-00721073/document accessed 4 October 2020.

BEAUD, Olivier, *La puissance de l'État*, PUF, Coll. Leviathan, 1994

BENATAR, Marco, "Use of cyber force: the need for legal justification?", Goettingen Journal of International Law, 1, 3, 2009, pp: 379-395.

BLAKE V. GUATEMALA, 1999 Inter-Am.Ct.H.R., (ser C.) No. 48., p.5 (Jan. 22, 1999)

BLOOMENTHAL, Andrew World's Top 10 Internet Companies, 18 September 2020, https://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp accessed 5 October 2020.

CHEVALLIER, Jacques, *Souveraineté Et Droit*, In : D. M. Desgrées du Loû, *Les évolutions de la souveraineté,* Montchrestien, Coll. Grands Colloques, 2006, pp. 203-219. Available at: https://hal.archives-ouvertes.fr/hal-01728232/document accessed 5 October 2020

COX, Rory, "Historical Just War Theory up to Thomas Aquinas", Saint Andrew, 2015, pp. 1-26. Available:https://researchrepository.standrews.ac.uk/bitstream/handle/10023/11776/Ch05_Cox_Historical_Just_War_Theory_up_to_Aquinas.pdf?sequence=1 accessed 7 October 2020.

CSIS, Significant Cyber Incidents Since 2006, Center for Strategic and International Studies (CSIS) | Washington, D.C. https://csis-website-prod.s3.amazonaws.com/s3fs-public/201002_Significant_Cyber_Events_List.pdf retrieved 7 October 2020

DAILLIER, Patrick ; FORTEAU, Mathias and PELLET, Allain, *Droit international public*, LGDJ, 8th Ed., 2009.

DOUZET, Frédérick, *«* Souveraineté et jurisdiction dans le cyberespace », Hérodote, n° 152-153, La Découverte, 2014. https://www.cairn.info/revue-herodote-2014-1-page-174.htm accessed 4 October 2020.

DUGUIT, Léon, *Traité de droit constitutionnel,* 3rd Ed., vol.5, Fontemoing, 1927-1930.

FRANCESCHET, Antonio, "Sovereignty and Freedom: Immanuel Kant's Liberal Internationalist 'Legacy.'" Review of International Studies 27, no. 2 (2001): 209–28.

HAKYEMEZ, Yusuf Şevki, Mutlak Monarşilerden Günümüze Egemenlik Kavramı: doğuşu, gelişimi kavramsal çevresi ve dönüşümü, Seçkin Yayıncılık, Ankara, 2004

HASSAN, Daud, "The Rise of the Territorial State and The Treaty of Westphalia", Yearbook of New Zealand Jurisprudence Vol. 9, pp. 62-70, 2006. https://opus.lib.uts.edu.au/bitstream/10453/3289/1/2006006060.pdf accessed 7 September 2020.

HOLLIS, B. Duncan, "why States need an informational law for information operations", *Lewis & Clark Law Review, Vol. 11,* 2007, pp.1-39. https://law.lclark.edu/live/files/9551-lcb114art7hollis.pdf accessed 6 October 2020.

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries 2001, session (A/56/10), https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf accessed 4 October 2020

KEDMEY, Dan, Report: NSA Authorized to Spy on 193 Countries, 1 July 2014. https://time.com/2945037/nsa-surveillance-193-countries/ accessed 6 October 2020.

KELSEN, Hans, The Pure Theory of Law and Analytical Jurisprudence, Harvard Law Review, Vol. 55, No. 1 (Nov. 1941), pp:44-70. Available at http://www.jstor.org/stable/1334739 accessed 5 October 2020.

KURUBAŞ, Erol, "Uluslararası İlişkiler Düşüncesi ve Dünya Politikasında Değişimi Anlamak", Kırıkkale Üniversitesi Sosyal Bilimler Dergisi, Cilt 2 Sayı 1 (Ocak 2012), pp: 9-34

MAURER, Tim, Cyber Proxies, and the Crisis in Ukraine, New America, 2018. https://www.ccdcoe.org/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf accessed 18 September 2020

MELZER, Nils, "Cyberwarfare and international Law", *UNIDIR*, 2011.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. the United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 92. Section 193. Online: https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf accessed 6 September 2020

Nuclear Tests (Australia v. France), Judgement, I.C.J. Reports 1974, p. 253., online: https://www.icj-cij.org/files/case-related/58/058-19741220-JUD-01-00-EN.pdf 6 September 2020

Nuclear Tests (N.Z. v. Fr.), 1973 I.C.J. 457 (Dec. 20) online: http://www.worldcourts.com/icj/eng/decisions/1974.12.20_nuclear_tests 2.htm 6 September 2020

OTTIS, Rain, Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf 18 September 2020

REISMAN, Michael. W., Sovereignty and Human Rights in Contemporary International Law, American Journal of International Law 84, no. 4 (1990): 866–76.

REUTERS STAFF, New Zealand bourse resumes trade after cyber-attacks, government activates security systems, Technology News, 28 August 2020. https://www.reuters.com/article/uk-nzx-cyber/new-zealand-bourse-crashes-for-fourth-day-after-cyberattacks-idUSKBN25O03Q accessed 10 September 2020.

ROBERT, Jones, Marxist—Leninist Doctrine and The Soviet Theory of Sovereignty. In: The Soviet Concept of Limited Sovereignty from Lenin to Gorbachev, Palgrave Macmillan, London, 1990.

S.S. "WIMBLEDON" Judgment of 17 August 1923 (Series A, No. 1), First Annual Report of the Permanent Court of International Justice (1 January 1922 – 15 June 1925), Series E, No. 1, pp. 163-168. Available at https://legal.un.org/PCIJsummaries/documents/english/5_e.pdf accessed 5 October 2020.

SAAKASHVILI, Eduard, "The global rise of Internet sovereignty", Authoritarian Tech, 21 March 2019. Available https://www.codastory.com/authoritarian-tech/global-rise-internet-sovereignty/ accessed 6 October 2020.

SCHMITT, Michael N (ed.), Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations, 2017

SCHMITT, Michael N., "Computer network attacks and the use of force in international law: Thoughts on a normative framework", *Columbia*

Journal of Transnational Law, Vol. 37, 1999. https://apps.dtic.mil/dtic/tr/fulltext/u2/a471993.pdf accessed 7 October 2020.

SCOTT, J. Brown, The Spanish origin of international law: Francisco de Vitoria and his law of nations, Oxford: Clarendon Press, 1934.

SELLERS, Mortimer, N.S., Intervention under International Law, 29 Md. J. Int'l L.1., 2014, pp:1-11. Available at: http://digitalcommons.law.umaryland.edu/mjil/vol29/iss1/3 accessed 7 October 2020.

STEINBERGER, Helmut, Sovereignty, in Encyclopaedia of Public International Law by R. Bernhardt, Elsevier, vol. 4, 2000

Summaries of EU Legislation, Precedence of European Law, 1 January 2010. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14548 5 October 2020.

The European Economic and Social Committee and The Committee of The Regions Internet Policy and Governance Europe's Role in Shaping the Future of Internet Governance (Text with EEA Relevance) /* COM/2014/072 Final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014DC0072&from=DA accessed 9 December 2020.

TRUYOL and SERRA, Sovereignty, in Fundamental Legal Vocabulary of Law, APD, t. 35, 1990

UN GGE Report 2013 (A/68/98*), §19 (adopted by the GA: UN Resolution A/RES/68/243 on the UN GGE Report 2013)

UNGA RESOLUTION: 2660 (XXV) of 7 December 1970

UNGA RESOLUTION: 3314 (XXIX) of 14 December 1974

UNGA RESOLUTION: A / RES / 42/22 of 18 November 1987.

UNGA RESOLUTION: 2625 (XXV) of 24 October 1970

UNGA RESOLUTION: A / RES / 31/9 of 8 November 1976

UNGA RESOLUTION: A / RES / 33/72 of 14 December 1978

UNGA RESOLUTION: A/RES/58/32 of 8 December 2003

UYGUN, Oktay, Devlet Teorisi, On Iki Levha Yayincilik, İstanbul, 2017

WEST's Encyclopedia of American Law, the definition of "Force" https://legal-dictionary.thefreedictionary.com/Force accessed 7 October 2020.