The 'Virtual Eichmann': on sovereignty in cyberspace

Pijpers, B.M.J.; van den Bosch, B.G.L.C.

DOI
10.2139/ssrn.3746843
Publication date
2021
Document Version
Final published version

The 'Virtual Eichmann': on sovereignty in cyberspace

Peter B.M.J. Pijpers & Bart G.L.C. van den Bosch **

We are not, therefore, defending our own interest alone.
We are not defending the physical person of Adolf Eichmann.
We are defending a right which we - the victims of the violation- cannot abandon
without becoming the accomplices of those who committed the violation
and assuming responsibility for the consequences that would ensue.[1]

"Sovereignty is a funny thing. It is allegedly the foundation of the
Westphalian order, but its exact contours are frustratingly indeterminate."[2]

** Peter Pijpers MSc. LL.M. and Dr Bart van den Bosch LL.M. are associate professors Cyber Operations resp. Military Law at the Netherlands Defence Academy. The authors would like to thank Prof Dr Marten Zwanenburg for his comments on earlier drafts of the article. Corresponding address: b.m.j.pijpers@uva.nl

[1] The Argentinian representative during the United Nations Security Council, 'S/PV. 865-68' (1960). 7 bullet 35.

[2] Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?' (2017) 95 Texas Law Review 1579.

Abstract

Sovereignty is a complex notion of international law, and not less disputed in the current digital era. The main question raised by some States is whether sovereignty is a 'mere' principle of international law in the virtual cyberspace or a binding rule as it is in other physical domains. Though a growing number of States provide a legal opinion regarding this topic, many remain reticent in doing so. But, international co-operation in cyberspace is challenging if the core premises, including the notion of State sovereignty, are not settled. The question is therefore not semantic; the consequences can be substantial, not least since cyberspace activities below a coercive intervention cannot be considered an international wrongful act if sovereignty is not a primary rule of law.

This article argues that the sovereignty of States, based on territorial integrity and political independence, is a primary rule of law in cyberspace. The breaches of sovereignty in cyberspace will however not follow the avenue of a violation of the territorial integrity but are based on a violation of the political independence. The method used to substantiate the argument is to compare the 1960s abduction of Eichmann to a present-day 'deletion of a virtual Eichmann'. In the 1960s abduction of Eichmann both territorial integrity and political independence - related to inherently governmental functions - were violated. In a fictitious remote cyber activity to delete a hackers-group, the 'virtual Eichmann', it is difficult to determine a violation of territorial integrity when no physical or functional damage occurs. However, the inherently governmental functions of the State can and will be violated when a remote cyber operation is executed aimed at State functions such as taxation, law enforcement or elections, not least since these functions are less territorial in nature. Clarity regarding the exact threshold when inherently governmental functions are violated will require further State practice, but questioning 'when' the breach happens alludes to the existence of sovereignty as a primary rule of law in cyberspace.

1. Introduction

In 1960 Otto Adolf Eichmann was secretly removed from Argentina (where he had lived after the end of WWII) by Israeli secret service agents and taken to Jerusalem. Under the specific provisions of the Israeli Nazi Collaborators (Punishment) Law, Eichmann was tried before the Jerusalem District Court, charged with crimes against the Jewish people, crimes against humanity, and war crimes.

The Eichmann abduction has been extensively documented and researched from numerous angles; political, human,[3] ethical and legal.[4] The legal discourse primarily dealt with the question whether the Israeli court had jurisdiction to prosecute Eichmann, based on principles and rules of both Israeli and international (criminal) law.

An adjacent legal issue was whether Eichmann's abduction had violated the sovereignty of Argentina? Argentina thought it did and filed a complaint with the UN arguing that it 'held the Government of Israel (..) responsible for the secret and unlawful transfer of Adolf Eichmann to the territory of Israel'.[5] And subsequently, the Israeli Government had violated the Argentinian territory and its sovereign rights.[6]

Though the violation of sovereignty was apparent in the 1960s Eichmann abduction in which the UN,[7] Argentina and even Israel acknowledged the violation of sovereignty, a binding rule of customary international law, this does not take away the fact that sovereignty is and has been a complex legal notion. And sovereignty is not less undisputed in the current digital age.[8]

A prominent topic in contemporary legal discourse relates to the question whether sovereignty is a legally binding rule in cyberspace or 'merely' a principle.[9] Though sovereignty has been a rule of international law, the emergence of cyberspace has triggered States and scholars to reconsider its status and not all are persuaded that sovereignty as a rule of law is applicable to cyberspace.[10] Reasons used to underscore the argument that sovereignty is a principle and not a rule of law in cyberspace is the lack of State practice on the matter, and the deviant characteristics of cyberspace, especially its (non-physical) virtual dimension.

Cyberspace, in the context of this article, contains a physical and a virtual component. The physical elements, such as the computer, routers or network cables are connected to a

---

[3] See e.g.: Hannah Arendt, *Eichmann in Jerusalem: A Report on the Banality of Evil* (Penguin 1976). But also Bettina Stangneth, *Eichmann Vor Jerusalem: Das Unbehelligte Leben Eines Massenmorders* (Rowohlt Verlag 2014).

[4] Vanni E Treves, 'Jurisdictional Aspects of the Eichmann Case'.; Nicholas N Kittrie, 'A Post Mortem of the Eichmann Case. The Lessons for International Law' (1964) 55 The Journal of Criminal Law, Criminology, and Police Science 16.; Hans W Baade, 'The Eichmann Trial: Some Legal Aspects' (1961) 1961 Duke Law Journal 400.

[5] United Nations Security Council (n 1). Para 5, 2.

[6] Treves (n 4). 558-559.

[7] Resolution 138 (1960) Question relating to the case of Adolf Eichmann 1960.

[8] See Michael N Schmitt, 'Taming the Lawless Void: Tracking the Evolution of International Law' (2020) 3 Texas National Security Review.; Michael N Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19 Chicago Journal of International Law.

[9] Michael N Schmitt, 'France's Major Statement on International Law and Cyber: An Assessment' [2019] Just Security. under 'sovereignty'; Przemysław Roguski, 'Application of International Law to Cyber Operations : A Comparative Analysis of States ' Views' (2020). 3-4; Duncan B Hollis, 'Improving Transparency International Law and State Cyber Operations (OAS - Fourth Report)', vol 19 (2020). 18.

[10] Jeremy Wright, 'Cyber and International Law in the 21st Century'.

territory, [11] while the virtual aspects, which are both the data, (software, code, 0s & 1s), and the virtual persona (reflections of persons and organisation in cyberspace e.g. Twitter accounts) are 'deterritorialised'.[12] That said, the physical and virtual components are not intrinsically linked. Technology such as blockchain stores data, not on a central mainframe, but in a distributed and decentralised manner in which transactions are based on, and will require peer-level consent. There is no connection between the blockchain software and a computer, hence no direct link to the territory of a State via the physical location of the ICT infrastructure. [13]

The discourse whether sovereignty is a principle or a rule in cyberspace, is not semantic as it can have genuine legal consequences. An internationally wrongful act, in the sense of Article 2 of the International Law Commission's Articles on State Responsibility,[14] is based on two conditions: first, the violation needs to be attributable to a State under international law, and second an international rule of that State needs to be breached.[15] If sovereignty is labelled as a principle and not as a primary rule of law, violation of sovereignty will not constitute an internationally wrongful act and redress cannot be invoked. In other words: an activity in cyberspace that infringes the sovereignty of another State can, in this case, not be considered unlawful.

Despite the lack of State practice regarding violations of sovereignty in cyberspace, the purpose of this article is to provide more granularity to the discourse on whether sovereignty is a rule or a principle of international law applicable in cyberspace. The method used is by comparing the sovereignty considerations surrounding the abduction of the physical Eichmann in 1960, with a fictitious case of removal or deletion of a 'virtual Eichmann'.[16] Would a 'digital deletion' still be a violation of sovereignty? Or will the characteristics of cyberspace force us to revisit this fundament of international law?

---

[11] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second ed, Cambridge University Press 2017). Rule 1, 15-18.

[12] Jackson Adams and Mohamad Albakajai, 'Cyberspace: A New Threat to the Sovereignty of the State' (2016) 4 Management Studies 256.

[13] See also the discussion in Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 11). Rule 1 (5), 12, Rule 2 (2-8) 13-15. Moreover, data via cyberspace is not sent in one piece but in packages that follow different routes to re-assemble in a later phase. And finally, the digital data is sent between States A, B and C is regulated via internationally agreed standards of digital services via UPU or ITU legislation making it difficult for any State to control the access and egress to its territory and the ICT (public or private) on it.

[14] United Nations General Assembly, 'Responsibility of States for Internationally Wrongful Acts - A/RES/56/83'.; James Crawford, *The International Law Commission's Articles on State Responsibility : Introduction, Text and Commentaries* (James (James Richard) Crawford ed, Cambridge University Press 2002). 81.

[15] Crawford, *The International Law Commission's Articles on State Responsibility : Introduction, Text and Commentaries* (n 14). 81. See also: *United States Diplomatic and Consular Staff in Tehran (USA v Iran), Judgement* [1980] ICJ Reports 3.; *Phosphates in Morocco - Preliminary Objections* (1938) Series A/B Collect Judgments, Orders Advis Opin. 28.

[16] The theme is inspired on the reference to the Eichmann incident in: Michael N Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 Texas Law Review 1639. 1659-1660, and discussion with Prof Dr T.D. Gill.

This article will first describe pre-cyberspace sovereignty based on case law, and assess the violation of sovereignty culminating in the 1960s Eichmann abduction (section 2). Then, in section 3, the appreciation of sovereignty will be transposed to a 2020s cyber-related case. After describing the discourse on sovereignty in cyberspace, an assessment is made of whether the deletion of a 'virtual Eichmann' can be seen as a violation of sovereignty. Thereby making use of the so-called Tallinn Manual, a seminal scholarly work on how existing international law applies to operations in cyberspace.[17] Before the conclusion (section 5), we will reflect on sovereignty in cyberspace (section 4).

A baseline for this article is that despite the growing number of international actors, sovereignty only applies in the relation between States.[18] This article is limited in several ways. First, the article does not delve into the substance of 1960s Eichmann case e.g. related to the extradition agreement between Argentina and Israel, the jurisdiction of Israel or the nationality of Eichmann. The only purpose of using the case is to make a cyber-related analogy with the violation of Argentinian sovereignty in the 1960s case. Second, the focus is on public international law between States, while internal law will not be taken into account. Furthermore, the article is limited to legal considerations and does not dwell on ethical or political issues. And finally, this article will not provide universal criteria for State behaviour regarding violating sovereignty but will make an appreciation of a specific situation.

2. Sovereignty in the pre-cyber era

In this section it is argued that sovereignty is a rule of customary international law as described in case law. Two elements of sovereignty can be distilled from customary international law: territorial integrity and political independence.[19] The Eichmann incident is tested against these two elements to assess whether sovereignty was violated and whether this was unlawful.

[17] The first edition of the Tallinn Manual was published in 2013. In 2017 a second edition was issued giving more prominence on operations in peacetime. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 11).
[18] ibid. rule 4(2) 17.
[19] See i.a. Quincy Wright, 'Subversive Intervention' (1960) 54 The American Journal of International Law 521. 522; Samuel KN Blay, 'Territorial Integrity and Political Independence' [2010] Max Planck Encyclopedia of International Law. A.1.

2.1 Sovereignty: territorial integrity and political independence

Sovereignty cannot easily be summarised.[20] It is a 'catch-all' term with a lengthy and troubled history.[21] Crawford argues that there is sovereignty between States and within States.[22] Notions that are highly intertwined as illustrated in the 1928 *Island de Palmas* Case in which Judge Huber stated that '(s)overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'[23]

Sovereignty among States refers to the legal equality of States. States are equal under international law, regardless of size or composition.[24] Sovereign equality is one of the cornerstones of the system of international law and is recognised in Article 2(1) of the UN Charter.

Sovereignty within States refers to the right to exercise the functions of the State, within a portion of the globe – often referred to as the two elements of Statecraft: territorial integrity and political independence.[25] Though sovereignty can and has been categorised in numerous ways, this article follows the notions of territorial integrity and political independence as also reflected in Article 2(4) of the UN Charter and several resolutions of the UN General Assembly.[26]

Territorial integrity is reflected in the exclusive authority and power a State has over its territory and those residing upon it to the exclusion of any other State, as Judge Huber stated, and entails both public and private entities. Territorial integrity includes the inviolability of, and respect for the territorial boundaries and connected territorial sea and airspace.

---

[20] See i.a. James Crawford, 'Sovereignty as a Legal Value', *The Cambridge Companion to International Law* (2012). 117-119.

[21] James R Crawford, *Brownlie's Principles of Public International Law* (9th ed., Oxford University Press 2019). 432; for a concise overview of the origins of modern international law, see Gleider Hernandez, *International Law* (Oxford University Press 2019). Chapter 1, 3-29.

[22] Crawford, 'Sovereignty as a Legal Value' (n 20). 120-123.

[23] *Island of Palmas Case (The Netherlands v United States)* (1928) II Reports Int Arbitr Award 829. 838.

[24] Eric Jensen, 'Cyber Sovereignty: The Way Ahead' (2015) 50 Texas International Law Journal 275. 285 – an equal has no power over an equal.

[25] Blay (n 19). Under A; Robert Jennings and Arthur Watts, *Oppenheim's International Law*, vol I (9th ed., Longman 2008). 382. Others make a similar division, see: Crawford, 'Sovereignty as a Legal Value' (n 20). 131-132; Charter of the United Nations 1945. Art 2(4) "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."; see also current day scholars, Schmitt, 'Taming the Lawless Void: Tracking the Evolution of International Law' (n 8). 38.

[26] United Nations General Assembly, 'Declaration on Principles of International Law Concerning Friendly Relations and Co - Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)' (1970).; United Nations General Assembly, 'Definition of Aggression - Resolution 3314 (XXIX)' (1974).; Oliver Dörr and Albrecht Randelzhofer, 'Purposes and Principles, Article 2 (4)' in Bruno Simma and others (eds), *The Charter of the United Nations: A Commentary*, vol I (3rd edn, Oxford University Press 2014). 215-217. See Article also 2(4) of the Charter of the United Nations.; United Nations Information Organization (UNIO), 'United Nations Conference on International Organization (UNCIO)- Volume VI'. 334-335; Crawford, *Brownlie's Principles of Public International Law* (n 21). 200.

Political independence enables a State to 'freely pursue a path to economic, social and cultural development of its choice,[27] conducive to executing the 'functions of the State',[28] or the 'inherently governmental functions',[29] i.e. collection of taxation, conduct of elections, law enforcement or the conduct of diplomacy.[30] Political independence also means that States can engage with, and enter into relations with other sovereign States on an equal footing.

2.2 Sovereignty as a rule

Without dwelling on the history of sovereignty,[31] in modern times sovereignty has been a binding rule of international law. This in effect means that sovereignty is not only a principle of customary international law from which many legal rights and obligations derive, including the prohibition of intervention, jurisdiction and the obligation of due diligence; but sovereignty is also a rule in itself,[32] and a violation thereof, if the violation is attributable to another State, can constitute an internationally wrongful act with an obligation to provide redress as a consequence.[33]

The UN Charter safeguards several aspects of sovereignty: the sovereign equality of States is referred to in Articles 2(1) and 78; and the territorial integrity and political independence in Article 2(4).[34] Also the regional Organisation of American States refers to sovereignty, territorial integrity and independence in the first article of its charter.[35] Likewise the Helsinki Final Act speaks about juridical equality, territorial integrity and freedom and political independence as attributes inherent to sovereignty.[36]

---

[27] Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace', *Peacetime Regime for State Activities in Cyberspace* (2013). 191.
[28] *Island of Palmas Case (The Netherlands v United States)* (n 23). 838.
[29] Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (n 8). 45; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 11). 21-22.
[30] Marko Milanovic and Michael N Schmitt, 'Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic' (2020) 11 Journal of National Security Law & Policy 247. 7-10.
[31] Hernandez (n 21). 5-26.
[32] In the 1986 Nicaragua Case the ICJ did not consider a violation of sovereignty and of non-intervention based on the principle of sovereignty, it argued and confirmed that violation of sovereignty was a separate breach aside from the use of force and intervention. *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (1986) Judgement ICJ Reports 14. Paras 212-213, 111.
[33] James Crawford, 'Articles on Responsibilty of States for Internationally Wrongful Acts' 385. 211ff.
[34] Charter of the United Nations.
[35] Charter of the Organization of American States 1948. Article 1.
[36] Helsinki Final Act 1975 1. Article 1. Mindful that the Helsinki Final Act is a political rather than a legal convention, see Terry D Gill, 'Non-Intervention in the Cyber Context', *Peacetime Regime for State Activities in Cyberspace* (2013). 220.

Though regional or thematic treaties mention aspects of sovereignty,[37] the legal basis for sovereignty as a rule is found in customary international law, most prominently reflected in judicial decisions and considerations of inter alia the International Court of Justice (ICJ).[38]

Case law on sovereignty is extensive. The judgment of the Permanent Court of International Justice in the 1927 *Lotus* Case, in essence on a dispute concerning jurisdiction between France and Turkey, considers that, if there are no permissive rules, a State 'may not exercise its power in any form in the territory of another State' alluding to the territorial integrity but also the political independence of a State.[39] The most prominent articulation of sovereignty, as stated above, is given by Judge Huber in the 1928 *Island of Palmas* arbitral award,[40] a view that was reiterated by Judge Alvares in an individual opinion to the ICJ judgment in the *Corfu Channel* case.[41]

The 1949 *Corfu Channel* Case (United Kingdom vs Albania) is important for two reasons. First of all, the ICJ states in its judgment in this case, that '(b)etween independent States, respect for territorial sovereignty is an essential foundation of international relations'.[42] And second, the ICJ queries whether the sovereignty of Albania was violated by the United Kingdom. Irrespective of the assessment of the ICJ, the fact that the ICJ contemplates the violation of sovereignty gives prominence to the fact that respect for sovereignty is a binding obligation. This is underlined by the United Kingdom (UK), invoking exemptions to the obligation to respect the sovereignty of other States. Invoking exemptions does not weaken but underlines the rule of sovereignty.

Also after the 1960s, in which the Eichmann incident took place, sovereignty was violated on numerous occasions and was brought to the ICJ or a similar court or arbitrary tribunal.[43] In the 1974 *Nuclear Tests* Case (Australia vs France), Australia claims that the fall-out of French nuclear testing had landed on Australian soil, in effect violating the sovereignty of Australia and hence breaching international law. France acknowledges the fall-out and does not dispute its French origin but claims that deposits are negligible and constitute no danger to the health of the population.[44] Though the ICJ decided not to pursue litigation, the case denotes the existence of territorial integrity of a State which violation entails the breach of a binding rule.[45]

---

[37] United Nations Convention on the Law of the Sea 1982.
[38] Schmitt and Vihul (n 16). 1650ff.
[39] *The Case of the SS Lotus (France v Turkey) - Judgment* (1927) Series A Collect Judgments 1. 18.
[40] *Island of Palmas Case (The Netherlands v United States)* (n 23). 838.
[41] *Corfu Channel (UK v Alb), 1949 ICJ (Opinion of Judge Alvarez)* 43.
[42] *Corfu Channel Case (merits) - Judgment of 9 April 1949*. 35.
[43] Besides the examples mentioned here see also e.g. *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of A Road in Costa Rica Along the San Juan River - Judgment of 16 December 2015*. 740ff., para 229.
[44] *Nuclear Tests (Austl v Fr) - Judgement* [1974] ICJ Reports 253.
[45] ibid. para 18, 258.

The 1986 ICJ judgment in the *Nicaragua* Case refers to territorial integrity and sovereignty numerous times,[46] highlighting that a violation thereof constitutes a breach of an obligation under customary international law. Though the violation of sovereignty is often a consequence of a breach of the prohibition of intervention or of the use of force, sovereignty is also breached as a stand-alone legal rule in the case of the laying of mines in the Nicaraguan territorial waters,[47] and related to unauthorised overflights.[48]

In the 1990 *Rainbow Warrior* Arbitration it was held that France violated the territorial integrity of New Zealand,[49] by sinking the Greenpeace ship Rainbow Warrior in Auckland harbour, executed by agents of the French intelligence service.

The obligation to respect the sovereignty of States as a rule in customary law is also echoed in numerous declarations of the UN. The 1970 United Nations General Assembly declaration on Friendly Relations emphasises the importance of sovereign equality of States.[50] The sovereign equality entails not only the judicial equality of States but also highlights the inviolability of territorial integrity and political independence of the State and its right to freely choose and develop its political, social, economic and cultural systems. The latter was already stated in the 1965 Declaration on the Inadmissibility of Intervention in the Domestic Affairs,[51] and is confirmed in the 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States.

2.3 Sovereignty during the Eichmann incident

The removal of Eichmann from Argentina in 1960 was a violation of both the territorial integrity and political independence. The territory of Argentina was violated after agents of the Israeli secret service gained unauthorised access to the country. The political independence, or execution of the functions of the State,[52] was violated because in apprehending Eichmann, Israel took over the Argentinean State function of the execution of

---

[46] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (n 32). Para 212, when referring to the laying of mines, 111.
[47] ibid. 111, para 213. The prohibited use of force regarding the laying of mines is discussed, 118, para 227.
[48] ibid. 128, para 251.
[49] *Rainbow Warrior (New Zealand v France)* (1990) 20 215.
[50] United Nations General Assembly, 'Declaration on Principles of International Law Concerning Friendly Relations and Co - Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)' (n 26). Under 'the principle of sovereign equality of States'.
[51] United Nations General Assembly, 'Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty - Resolution 2131 (XX)' (1965). Bullet 5: "Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State."
[52] *Island of Palmas Case (The Netherlands v United States)* (n 23). 898.

the law, more specifically law enforcement. This activity can be labelled as a usurpation due to the unauthorised and non-consensual execution of law enforcement by Israel.[53]

The violation was unlawful since there was no legal justification for the breach of sovereignty. The Israeli action was not endorsed by a UN Security Council resolution, it was not a form of self-defence, countermeasure nor could Israel invoke circumstances precluding wrongfulness.[54] Israel tried to preclude unlawfulness by arguing that Eichmann was illegally in Argentina and had consented to the deportation, but Argentina argued that though this may or may not be true, it does not provide justification for violating Argentinean sovereignty. [55]

3. Sovereignty in Cyberspace - the 'Virtual Eichmann'

Sovereignty as a binding legal rule has a firm foundation in international law. Respect for sovereignty is a primary rule of law, and the breach of which constitutes a violation of international law. Sovereignty is based on territorial integrity and political independence, both of which were violated when removing Eichmann from Argentinean soil in 1960.

This section starts with describing the discourse regarding sovereignty in cyberspace, after which a case will be laid out making a digital analogy with the physical abduction of Eichmann in 1960. This case will be tested against territorial integrity and political independence, to assess whether sovereignty is a legal rule in cyberspace or not.

3.1 The 'sovereignty in cyberspace'-discourse

Respect for sovereignty is a well-recognised norm of international law,[56] with the subsequent obligation not to violate the sovereignty of another State. This would also account for sovereignty in cyberspace. During the two iterations of the Tallinn Manual this was confirmed - or rather not disputed. The position taking during the Tallinn Manual process is that 'sovereignty constitutes both an international law principle from which various rules derive (such as the prohibitions on coercive intervention and the use of force) and a primary rule in its own right capable of being violated.'[57]

---

[53] Michael N Schmitt, 'Grey Zones in the International Law of Cyberspace' (2017) 42 The Yale Journal of International Law 1. 6-7 (note 30).
[54] As currently depicted in Chapter V of the United Nations, 'Responsibility of States for Internationally Wrongful Acts' (2001) II Yearbook of the International Law Commission vol II (Part Two).
[55] United Nations Security Council (n 1). Bullets 26 & 28. See also: Treves (n 4). 558-559; Kittrie (n 4). 16-17.
[56] See e.g. Charter of the United Nations.; Helsinki Final Act.
[57] Schmitt, 'France's Major Statement on International Law and Cyber: An Assessment' (n 9). 2.

But sovereignty in cyberspace appeared not to be undisputed. Since mid 2016 a discussion between several States and legal scholars is ongoing in which some challenge the concept of sovereignty as a rule in cyberspace.[58] The fact that many States refrain from providing their legal opinion on the issue, is not helpful for the argument,[59] but does not mean that they reject sovereignty as a rule.

The idea that sovereignty is a principle but not a rule in cyberspace, is the current UK position.[60] In 2016 UK Attorney General Wright stated that the emergence of cyberspace has posed questions regarding the applicability of international law.[61] On the one hand Wright argues that the prohibition of intervention, and of the threat or use of force against States, are applicable in cyberspace and that violations thereof constitute an internationally wrongful act after which redress is possible, following the rationale that international law applies to cyberspace. But, on the other hand, Wright is 'not persuaded' to 'extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention.'[62]

Several scholars hold similar views. Corn and Tayler argue that there are sufficient proscriptions against unlawful uses of force and interventions in treaty law and customary international law, but 'below these thresholds, there is insufficient evidence of either state practice or *opinio juris* to support assertions that the principle of sovereignty operates as an independent rule of customary international law that regulates states' actions in cyberspace.'[63] Furthermore, Corn mentions that based on the law and State practice, 'sovereignty serves as a principle of international law that guides state interactions, but is not itself a binding rule that dictates results under international law'.[64] Others argue that the prohibition of the use of force, and intervention apply to cyberspace,[65] but '(p)recisely when a non-consensual cyber operation violates the sovereignty of another State'[66] is still undefined and would require more State practice and *opinio iuris*. A final scholarly, but also State view is that for the ICT

[58] See e.g. Michael N Schmitt, 'The Defense Department's Measured Take on International Law in Cyberspace' [2020] Just Security.; Michael N Schmitt and Liis Vihul, 'Sovereignty in Cyberspace: Lex Lata Vel Non?' (2017) 111 AJIL Unbound 213.; Przemysław Roguski, 'Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace* (2020). 67-69.
[59] Barrie Sander, 'The Sound of Silence : International Law and the Governance of Peacetime Cyber Operations' 1.
[60] But the UK is not the only country, also e.g. Chile argues that sovereignty is a principle and not a stand-alone rule. See: Hollis (n 9). 18-20.
[61] Wright (n 10).
[62] ibid. (2018), hereafter "UK Wright Speech".
[63] Gary P Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 AJIL Unbound 207. 208.
[64] ibid. 208.
[65] See Schmitt, 'The Defense Department's Measured Take on International Law in Cyberspace' (n 58).; Robert Chesney, 'The Pentagon's General Counsel on the Law of Military Operations in Cyberspace' [2020] Lawfare 1. Under 4 c-d; Paul C Ney, 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference'. Under B. International law.
[66] Brian Egan, 'International Law and Stability in Cyberspace' (2017) 35 International Tax & Business Lawyer 169.

infrastructure (hence the physical part of cyberspace) sovereignty as a rule applies, this is not necessarily the case for the virtual dimension of cyberspace.[67]

Though many States remain silent on whether sovereignty is a rule or a principle in cyberspace,[68] a growing number of States, including Australia,[69] New Zealand,[70] Estonia,[71] France [72] and the Netherlands, [73] has given their legal opinion on the applicability of international law in cyberspace including reference to sovereignty.[74] For France sovereignty is a rule also in cyberspace,[75] stating that it will protect its sovereignty over the information systems located on its territory and implements the means necessary to protect this sovereignty,[76] and reserves the right to respond to any cyber-attack of which it has been the victim.[77] France argues that a violation of sovereignty is not only related to rules regarding the prohibition of intervention or use of force, but also related to territorial integrity and the jurisdiction over its territory and the persons and objects within that territory. Cyber operations executed by another State on French digital infrastructure will violate sovereignty and international law.[78] The Netherlands also states that sovereignty is an independently binding rule of international law and its violation constitutes an internationally wrongful act,[79]

[67] This is the position of Ecuador, but also Chile and the US are inclined to this view. See: Hollis (n 9). Para 51, 19.
[68] In the sense that there are not overt activities nor is there official documentation on the cyber activities of the state. See also: Harriet Moynihan, 'The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention' (2019).p. 9; Hollis (n 9). 2-3.
[69] Australian Government Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (2017).
[70] New Zealand Ministry of Foreign Affairs & Trade, 'The Application of International Law to State Activity in Cyberspace' (2020).
[71] Kristi Sits, 'President of Estonia : International Law Applies Also in Cyber Space', *CyCon 2019* (2019).
[72] Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace' (2019).; See also Michael N Schmitt, 'France Speaks Out on IHL and Cyber Operations : Part I' [2019] EJIL 1.; Przemysław Roguski, 'France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I' [2019] OpinioJuris 1.
[73] Ministry of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace 2019.; See also: Michael N Schmitt, 'The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis' [2019] Just Security.
[74] The discussion is not confined to Europe and the US, also in the Organisation of American States silence is broken. Bolivia, Guatemala and Guyana argue that sovereignty is a stand-alone rule that can be breached in cyberspace. Other are less outspoken and some suggest it only a principle. See: Duncan B Hollis, Ben Vila and Daniela Rakhlina-Powsner, 'Elaborating International Law for Cyberspace' [2020] Directions Cyber Digital Europe.; Hollis (n 9). Para 52, 19.
[75] Schmitt, 'France's Major Statement on International Law and Cyber: An Assessment' (n 9).
[76] SGDSN, 'Revue Stratégique de Cyberdéfense'. 82.
[77] Ministère des Armées (n 72). 6.
[78] ibid. 7
[79] Ministry of Foreign Affairs, Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace 2019 1. 2.

related to the territorial integrity and the inherently governmental functions of a state.[80] A position also adopted by Austria, the Czech Republic, Finland and Switzerland.[81]

Other States are less outspoken or remain 'on the fence'.[82] The US view is murkier[83] and though several statements have been issued,[84] no *opinio iuris* is given. Australia concurs that for cyber activities below the threshold of the use of force, general principles of international law, the principle of due diligence and the customary international law on State responsibility apply.[85] Estonia, similar to Australia circumvents wording on the appreciation of sovereignty in cyberspace, but affirms that international law applies to cyberspace, and that States must refrain from the threat of or use of force against the territorial integrity and political independence of other States.[86] Also China states that 'the principle of sovereignty enshrined in the UN Charter covers all aspects of state-to-state relations, which also includes cyberspace.'[87] A view echoing the Joint Statement by China and the Russia Federation on cooperation in Information Space Development in which they strongly support the principle of national sovereignty within the UN framework.[88] This statement confirms an earlier declaration of six members of the Shanghai Cooperation Organisation, sent to the UN Secretary General in January 2015.[89] The language used is neutral and restates the text of the UN Charter when referring to sovereignty. Hence, not confirming but certainly not denying the existence of the rule of sovereignty in cyberspace.

Though sovereignty has been a binding legal rule of customary international law, the dawn of cyberspace commenced a discourse on whether this also applies to cyberspace. Public international law can of course change based on diverging State behaviour over time, imputed by the characteristics of cyberspace which are different from the traditional

---

[80] The Netherlands follows the rationale of the Tallinn Manual. See also: Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 11). Rule 4, 20.

[81] Swiss Ministry of Foreign Affairs, 'Position Paper on Switzerland's Participation in the UN OEWG and UNGGE' (2020).; Czech Republic Ministery of Foreign Affairs, 'Comments Submitted by the Czech Republic in Reaction to the Initial "Pre-Draft" Report of the OEWG' (2020).; Michael N Schmitt, 'Finland Sets Out Key Positions on International Cyber Law' [2020] Just Security.; Austrian Ministry of Foreign Affairs, 'Pre-Draft Report of the OEWG - ICT' (2020).

[82] Including Israel, see: Michael N Schmitt, 'Israel's Cautious Perspective on International Law in Cyberspace: Part I (Methodology and General International Law)' [2020] Just Security.

[83] Hollis (n 9). 20.

[84] Ney (n 65).; Egan (n 66).

[85] Australian Government Department of Foreign Affairs and Trade (n 69). Annex A, p. 91; Australian Government Department of Foreign Affairs and Trade, '2019 International Law Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace'.

[86] Sits (n 71). First and fifth bullet.

[87] Ministery of foreign affairs of the people's republic of China, 'International Strategy of Cooperation on Cyberspace'. Chapter II para 2.

[88] 'Joint Statement Between the People's Republic of China and the Russian Federation on Cooperation in Information Space Development' (2016).

[89] United Nations General Assembly, 'A/69/723 Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General' (2015) 00392 UN Doc. A/69/723. 4.

domains. However, arguing that international law, and more specifically the notion of sovereignty, needs to change due to the dawn of cyberspace appears to be a reversed and flawed rationale. Not least since the lack of State practice also applies to cases related to intervention and the use of force in cyberspace,[90] which clearly constitute rules of international law.[91] But, based on *opinio iuris*, the latter two are applicable in cyberspace while sovereignty (strangely enough) is not. The authors take note of the discussion but argue, in line with the Tallinn Manual scholars[92] and the *opinio iuris* of some States, that sovereignty is both a principle and a binding legal rule in cyberspace which will be underlined with a fictitious case of the deletion of a 'virtual Eichmann'.

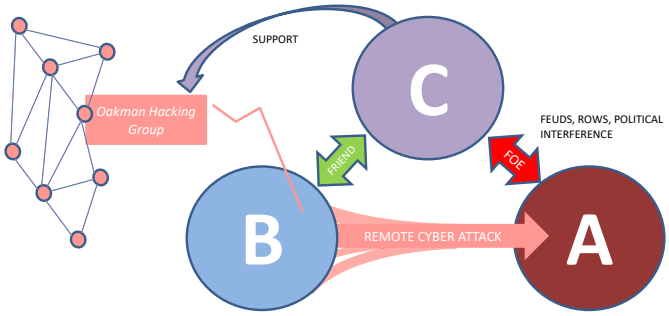
3.2 The 'virtual Eichmann'-case

Sovereignty in the 1960 Eichmann abduction was violated since both the territorial integrity and the political independence of Argentina were breached unlawfully.[93] But can the rules and principles of sovereignty, which have a sound foundation in the notion of territory, be applied in a similar way to cyberspace? Or does the changing context require additional interpretation on the object and purpose of the existing legal rules?[94]

To test the binding legal rule of sovereignty a fictitious case is presented in which a virtual entity, the so-called Oakman Hacking Agency, instead of a real person will be 'removed' from cyberspace.

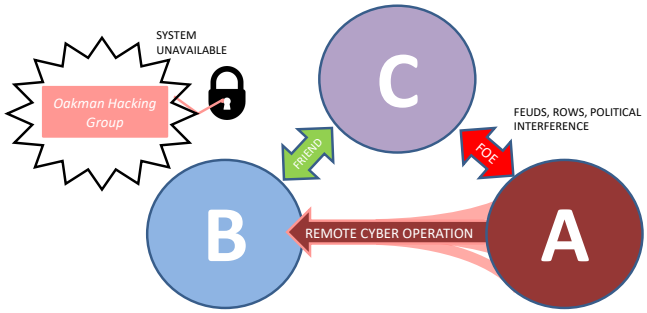
[90] Dale Stephens, 'Influence Operations & International Law' (2020) 19 Journal of Information Warfare 1. 6.
[91] Steven Wheatley, 'Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about "Coercion"' (2020) 30 Duke Journal of Comparative and International Law. 11.
[92] See e.g. Schmitt and Vihul (n 16). 1649; *Corfu Channel Case (merits) - Judgment of 9 April 1949* (n 42). 35; *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (n 32). Para 202, 106 202 & para 213, 111. In the latter, the Court quotes the Corfu Judgment in stating that '"Between independent States, respect for territorial sovereignty is an essential foundation of international relations", and international law requires political integrity also to be respected.'
[93] United Nations Security Council (n 1). Bullet 47, 10.
[94] Article 31 of the Vienna Convention on the Law of Treaties 1969.

'Oakman Hacking Group' has executed several remote cyber operations against State A. Oakman is a group of loosely affiliated hackers that log in from all over the world, using multiple ICT infrastructures and servers in as many States. Oakman, as a firm registered in State B, has in the past allegedly been supported by State C. State B is aligned with State C based on common economic and security interests. State A and State C have had issues in the past including feuds over borders, economic rows and mutual political interferences.



Several members of Oakman have been indicted based on State's A penal legislation, for remote cyber intrusions, inflicting damage to materiel in State A, causing the loss of functionality of State supported ICT infrastructure during elections and undermining the free electoral process of State A by intense disinformation campaigns. Apart from extradition requests, State A has put political pressure on State C to stop supporting Oakman, and invoking a due diligence request to State B. State B has informally acknowledged the existence of Oakman and its activities on the soil of State B, but fails to see the harm inflicted to State A. State A even filed a complaint under art 33 UN Charter to the UN Security Council which in turn issued a generic statement calling upon States not to interfere in other States with cyber means and to act responsibly when aware that agents on their territory pursue activities that could harm other States.

After long deliberation and international inactivity, State A has, under the aegis of a countermeasure due to failed due diligence, executed a remote operation in cyberspace and has put Oakman's network in State B out of order using a multitude of malware, taking the entire encrypted network including virtual persona hostage. Though there is no physical or functional damage nor injuries, Oakman was rendered incapable of operating, de facto removing it from cyberspace.



3.3 Sovereignty in the 'virtual Eichmann'-case

The sovereignty in the 'virtual Eichmann'-case will be assessed based on the violations of territorial integrity and political independence.

Territorial integrity is based on the territory of the State. Cyber activities of agents of State A present *in* State B would, similar to the Eichmann incident, constitute a breach of territorial integrity if these agents are active in State B without permission. A remote cyber operation however, does not physically cross the borders of State B, hence the question is whether the authority of State B regarding access and egress of its territory was tampered with.

The notion of territoriality is challenging in cyberspace. The essence of activities in cyberspace are within the virtual dimension i.e. the data and the virtual persona which are not connected to the territory of a State. Assessing whether the act of installing dormant malware in software that could be used on a foreign ICT infrastructure, constitutes a violation of territorial integrity might prove difficult. The eventual effect in the form of physical or functional damage to the cyberspace infrastructure or affiliated systems and operators is a more tangible violation of territorial integrity.

The challenges also give rise to the discourse regarding the effect-based versus the act-based doctrine.[95] The act-based doctrine is depicted in what Roguski calls the 'penetration-based' approach. This approach, which is reflected in the legal opinion of France,[96] argues that every penetration of ICT infrastructure located within the State's territory violates its sovereignty. Following this rationale for activities in cyberspace, States would be in a 'constant state of violation' of sovereignty.[97]

Given the practical predicaments of an act-based approach to cyberspace, an alternative could be found in the delineation of thresholds that must be reached before sovereignty is violated, including a minimum bar. The *de minimis* threshold stipulates that though sovereignty has to be respected, a minimum threshold needs to be crossed before a violation occurs.[98] The *de minimis*, but also the thresholds on display in the Tallinn Manual are an

[95] Roguski, 'France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I' (n 72). Roguski, 'Application of International Law to Cyber Operations : A Comparative Analysis of States ' Views' (n 9).; Moynihan (n 68). 21-24.
[96] The French legal opinion has both elements of the act-based and the effect-based approach, see: Ministre de 'Europe et de Affairs Etrangeres, 'Stratégie Internationale de La France Pour Le Numérique —'.
[97] Moynihan (n 68). 20.
[98] ibid. 48.

elaboration of the effect-based doctrine.[99] This doctrine, as also considered in the 1974 *Nuclear Tests* Case, looks at the impact of an action.

The experts of the Tallinn Manual confirm that a 'State must not conduct cyber operations that violate the sovereignty of another State',[100] and have introduced several thresholds on when remote cyber operations violate territorial integrity.

The first level is physical damage, destruction or injuries. If one of these is the effect of a remote cyber operation, as was the case during the Stuxnet attack,[101] a breach of territorial integrity can be agreed upon. In the Oakman case, the network of Oakman was taken hostage and rendered ineffective by State A. Neither during the remote cyber-attack nor in its effect, were persons hurt or was infrastructure damaged or destroyed.

The second level is functional damage, or the loss of functionality of cyber infrastructure. This means that the infrastructure is rendered permanently out of service. Though the Tallinn Manual-experts agreed that this could constitute a violation of sovereignty, no exact threshold could be agreed upon due to the lack of legal opinions of States.[102] This threshold is not reached in the Oakman case: The network is temporary rendered out of service but it was not destroyed or manipulated. If Oakman ceases its acts, or State B will prosecute the Oakman Hacker group, State A could 'release' the network without further ado.

The third threshold caps all activities resulting in effects below physical or functional damage, such as the deletion of data, slowing down the system, a temporary loss of functionality e.g. by a DDoS attack, and partially coalesces with the earlier mentioned considerations regarding the *de minimis* approach. The experts could not agree if and when these effects would constitute a violation of sovereignty.[103] Also, in the Oakman case, the direct effect will be that the malign hacker group can no longer execute activities. From a penetration approach point of view this would entail an infringement in the network of a private entity which falls under the State's territorial authority. But taking the effect-based view it is questionable if the *de minimis* threshold is crossed by rendering the Oakman network temporarily out of service with the option to reverse the action by lifting the hostage taking. Moreover, the threshold is only crossed related to those physical network structures that are located in State B.

Much focus is on territorial integrity while the violation in the Oakman case can also be judged against the criteria of political independence, related to the inherently governmental functions. The Tallinn Manual offers two thresholds for violation of political independence.

---

[99] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 11). Rule 4. 17ff.
[100] ibid. Rule 4, 17.
[101] Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict and Security Law 212. 219- 221.
[102] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 11). Rule 4 (13) 20-21.
[103] ibid. Rule 4 (14) 21.

First the interference with the inherently governmental functions and second, usurpation thereof.[104]

Where the domain of the territorial integrity is concerned with the sovereignty domain of the territory of the State and the population living there, the domain of political independence is related to the functions of the State, or the inherently governmental functions i.e. conducting elections, collecting taxes, law enforcement and conducting diplomacy. An interference in these inherently governmental functions could be a long-term DDoS attack on the governmental website filing digital tax returns.

In the Oakman case, State A not only interfered with the governmental task of law enforcement but even took over this function, hence usurping an inherently governmental functions of State B,[105] similar to the 1960s Eichmann incident.

4. Reflections

In the 1960s Eichmann incident the sovereignty of Argentina was violated because Israeli agents were on Argentinean soil without permission – breaching the territorial integrity – and performed law enforcement activities which are the prerogative of the State - breaching the political independence.

The emergence of cyberspace provided many challenges including how to apply public international law to this emerging domain. Moreover, while cyberspace contains a physical element which is connected to the territory of a State, it also entails a boundless and ubiquitous virtual dimension. The latter is an inconvenient fit with the notion of territory.

The virtual dimension of cyberspace in which effects can be tangible and visible (but an initial act of intrusion seldom is) gives prominence to the discourse on whether sovereignty applies to this virtual dimension as a binding legal rule.

In the Oakman case, a fictitious scenario, the challenges of applying sovereignty as a rule of international law in cyberspace come to the fore. It is fair to state that violation of territorial integrity is difficult to substantiate, especially if an act-based doctrine is followed. The penetration approach argues that any incursion into the cyber infrastructure of another State would account to a violation of sovereignty. The danger of this approach is that sovereignty will be interpreted subjectively from the position offended State, while international law must

[104] ibid. Rule 4 (15-19) 21-23; Schmitt and Vihul (n 16). 1660.
[105] Schmitt and Vihul (n 16). 1660.

be applied objectively.[106] Following this line of argument, with a focus on territorial integrity as the core element of sovereignty, the rationale of the UK Wright Speech,[107] and the reticence of many States to be more outspoken on the matter, is understandable.

However, in the Oakman case, sovereignty was violated, not based on a violation of the territorial integrity but based on the usurpation and/or interference of the inherently governmental functions of the State. Sovereignty in the virtual dimension of cyberspace, based on territoriality integrity is challenging since the territorial link does not necessarily exist. The notion of political independence is not directly linked to the physical territory of the State but to the more metaphysical inherently governmental functions. Therefore, political independence is a more persuasive basis to argue that sovereignty is a rule in cyberspace.

5. Conclusions

Sovereignty is based on the notions of territorial integrity and political independence. Violation of territorial integrity is traditionally related to physical incursions into the territory of the State.[108] Hence, a large part of the discourse of sovereignty in cyberspace focuses on the territorial aspect of sovereignty and less on its political independence.

It is challenging to align remote cyber activities (that do not physically cross borders and engage in the non-tangible virtual dimension of cyberspace) with the concept of territoriality. Especially if activities in cyberspace do not manifest physical damage or injury to either persons, objects or cyberinfrastructure.

It can be fair to conclude that violations of territorial integrity, caused by remote cyber operations, are difficult to substantiate if there is no physical or functional damage, which unfortunately is the case with most remote cyber-related activities.

But these difficulties do not render the rule of sovereignty in cyberspace obsolete. Interference with the political independence of another State is not necessarily dependent on the notion of territory similarly to the violation of territorial integrity. Therefore, activities in

---

[106] Moynihan (n 68). 20.

[107] Wright (n 10). Wright argues that: "Some have sought to argue for the existence of a cyber specific rule of a "violation of territorial sovereignty" in relation to interference in the computer networks of another state without its consent. Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law."

[108] Phil Spector, 'In Defense of Sovereignty, in the Wake of Tallinn 2.0' (2017) 111 AJIL Unbound 219. 222.

cyberspace can infringe or usurp the inherently governmental functions in a way similar to infringements in other (physical) domains.

Relying on territorial integrity to effectuate sovereignty as a rule of international law in cyberspace, might prove to be a dead-end street for remote cyber operations in the virtual dimension. Not least since a breach thereof is difficult to prove. The notion of political independence on the other hand is applicable in cyberspace as it is in physical realm, and is therefore a relevant indication that sovereignty is still a rule of international law.

In the Oakman case, sovereignty was violated. It was unlikely that territorial integrity was violated, not least since the notion of territorial integrity is not easily transferable to the virtual characteristics of cyberspace. The inherently governmental functions of the State were usurped or interfered with, resulting in a violation of political independence. The latter is therefore a more plausible option to claim that sovereignty is a binding rule in cyberspace.

The main conclusion of this article is that sovereignty is a binding rule of customary international law in cyberspace,[109] as it is in other (physical) domains. States enjoy sovereignty over cyber infrastructure, persons and cyber activities on their territory, and based on their political independence.[110] In the view of the authors, the question related to sovereignty in cyberspace should therefore not be 'if' there is a rule of international law, but rather when the rule of sovereignty in cyberspace is violated.[111]

Bibliography

Arendt H, *Eichmann in Jerusalem : A Report on the Banality of Evil* (Penguin 1976)

Australian Government Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (2017)

——, '2019 International Law Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace'

Austrian Ministry of Foreign Affairs, 'Pre-Draft Report of the OEWG - ICT' (2020)

[109] See Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 11). 11-13. But also the UN GGE reports, e.g. the United Nations GGE 2015 Report, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174', vol 12404 (2015)..

[110] Schmitt and Vihul (n 16). 1647.

[111] Moynihan (n 68). 17-18. Which is in line with Egan's referral to the 'de minimus' activities, and Corn's argument that 'whether and precisely when non-consensual cyber operations below the threshold of a prohibited intervention violate international law is a question that must be resolved through the practice and opinio juris of states'. See: Egan (n 66).; Corn and Taylor (n 63). 210-211. Michael N Schmitt, 'International Cyber Norms: Reflections on the Path Ahead' [2018] Militair Rechtelijk Tijdschrift. 17.

Baade HW, 'The Eichmann Trial: Some Legal Aspects' (1961) 1961 Duke Law Journal 400

Blay SKN, 'Territorial Integrity and Political Independence' [2010] Max Planck Encyclopedia of International Law

Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict and Security Law 212

Chesney R, 'The Pentagon's General Counsel on the Law of Military Operations in Cyberspace' [2020] Lawfare 1

Corn GP and Taylor R, 'Sovereignty in the Age of Cyber' (2017) 111 AJIL Unbound 207

Crawford J, *The International Law Commission's Articles on State Responsibility : Introduction, Text and Commentaries* (James (James Richard) Crawford ed, Cambridge University Press 2002)

——, 'Articles on Responsibilty of States for Internationally Wrongful Acts' 385

——, 'Sovereignty as a Legal Value', *The Cambridge Companion to International Law* (2012)

Crawford JR, *Brownlie's Principles of Public International Law* (9th ed., Oxford University Press 2019)

Czech Republic Ministery of Foreign Affairs, 'Comments Submitted by the Czech Republic in Reaction to the Initial "Pre-Draft" Report of the OEWG' (2020)

Dörr O and Randelzhofer A, 'Purposes and Principles, Article 2 (4)' in Bruno Simma and others (eds), *The Charter of the United Nations: A Commentary*, vol I (3rd edn, Oxford University Press 2014)

Egan B, 'International Law and Stability in Cyberspace' (2017) 35 International Tax & Business Lawyer 169

Gill TD, 'Non-Intervention in the Cyber Context', *Peacetime Regime for State Activities in Cyberspace* (2013)

Hernandez G, *International Law* (Oxford University Press 2019)

Hollis DB, 'Improving Transparency International Law and State Cyber Operations (OAS - Fourth Report)', vol 19 (2020)

Hollis DB, Vila B and Rakhlina-Powsner D, 'Elaborating International Law for Cyberspace' [2020] Directions Cyber Digital Europe

Jackson Adams and Mohamad Albakajai, 'Cyberspace: A New Threat to the Sovereignty of the State' (2016) 4 Management Studies 256

Jennings R and Watts A, *Oppenheim's International Law*, vol I (9th ed., Longman 2008)

Jensen E, 'Cyber Sovereignty: The Way Ahead' (2015) 50 Texas International Law Journal 275

'Joint Statement Between the People's Republic of China and the Russian Federation on Cooperation in Information Space Development' (2016)

Kittrie NN, 'A Post Mortem of the Eichmann Case. The Lessons for International Law' (1964) 55 The Journal of Criminal Law, Criminology, and Police Science 16

Milanovic M and Schmitt MN, 'Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic' (2020) 11 Journal of National Security Law & Policy 247

Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace' (2019)

Ministery of foreign affairs of the people's republic of China, 'International Strategy of Cooperation on Cyberspace'

Ministre de 'Europe et de Affairs Etrangeres, 'Stratégie Internationale de La France Pour Le Numérique —'

Moynihan H, 'The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention' (2019)

New Zealand Ministry of Foreign Affairs & Trade, 'The Application of International Law to State Activity in Cyberspace' (2020)

Ney PC, 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference'

Ohlin JD, 'Did Russian Cyber Interference in the 2016 Election Violate International Law ?' (2017) 95 Texas Law Review 1579

Pirker B, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace', *Peacetime Regime for State Activities in Cyberspace* (2013)

Roguski P, 'France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I' [2019] OpinioJuris 1

——, 'Application of International Law to Cyber Operations : A Comparative Analysis of States ' Views' (2020)

——, 'Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace* (2020)

Sander B, 'The Sound of Silence : International Law and the Governance of Peacetime Cyber Operations' 1

Schmitt MN, 'Grey Zones in the International Law of Cyberspace' (2017) 42 The Yale Journal of International Law 1

——, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second ed, Cambridge University Press 2017)

——, 'International Cyber Norms: Reflections on the Path Ahead' [2018] Militair Rechtelijk Tijdschrift

——, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19 Chicago Journal of International Law

——, 'France's Major Statement on International Law and Cyber: An Assessment' [2019]

Just Security

——, 'France Speaks Out on IHL and Cyber Operations : Part I' [2019] EJIL 1

——, 'The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis' [2019] Just Security

——, 'Finland Sets Out Key Positions on International Cyber Law' [2020] Just Security

——, 'Israel's Cautious Perspective on International Law in Cyberspace: Part I (Methodology and General International Law)' [2020] Just Security

——, 'Taming the Lawless Void: Tracking the Evolution of International Law' (2020) 3 Texas National Security Review

——, 'The Defense Department's Measured Take on International Law in Cyberspace' [2020] Just Security

Schmitt MN and Vihul L, 'Respect for Sovereignty in Cyberspace' (2017) 95 Texas Law Review 1639

——, 'Sovereignty in Cyberspace: Lex Lata Vel Non?' (2017) 111 AJIL Unbound 213

SGDSN, 'Revue Stratégique de Cyberdéfense'

Sits K, 'President of Estonia : International Law Applies Also in Cyber Space', *CyCon 2019* (2019)

Spector P, 'In Defense of Sovereignty, in the Wake of Tallinn 2.0' (2017) 111 AJIL Unbound 219

Stangneth B, *Eichmann Vor Jerusalem: Das Unbehelligte Leben Eines Massenmorders* (Rowohlt Verlag 2014)

Stephens D, 'Influence Operations & International Law' (2020) 19 Journal of Information Warfare 1

Swiss Ministry of Foreign Affairs, 'Position Paper on Switzerland's Participation in the UN OEWG and UNGGE' (2020)

Treves VE, 'Jurisdictional Aspects of the Eichmann Case'

United Nations, 'Responsibility of States for Internationally Wrongful Acts' (2001) II Yearbook of the International Law Commission vol II (Part Two)

United Nations General Assembly, 'Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty - Resolution 2131 (XX)' (1965)

——, 'Declaration on Principles of International Law Concerning Friendly Relations and Co - Operation among States in Accordance with the Charter of the United Nations - Resolution 2625(XXV)' (1970)

——, 'Definition of Aggression - Resolution 3314 (XXIX)' (1974)

——, 'Responsibility of States for Internationally Wrongful Acts - A/RES/56/83'

——, 'A/69/723 Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General' (2015) 00392 UN Doc. A/69/723

United Nations GGE 2015 Report, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174', vol 12404 (2015)

United Nations Information Organization (UNIO), 'United Nations Conference on International Organization (UNCIO)- Volume VI'

United Nations Security Council, 'S/PV. 865-68' (1960)

Wheatley S, 'Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about "Coercion"' (2020) 30 Duke Journal of Comparative and International Law

Wright J, 'Cyber and International Law in the 21st Century'

Wright Q, 'Subversive Intervention' (1960) 54 The American Journal of International Law 521

Case Concerning Military and Paramilitary Activities in and against Nicaragua (1986) Judgement ICJ Reports 14

Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of A Road in Costa Rica Along the San Juan River - Judgment of 16 December 2015

Corfu Channel (UK v Alb), 1949 ICJ (Opinion of Judge Alvarez) 43

Corfu Channel Case (merits) - Judgment of 9 April 1949

Island of Palmas Case (The Netherlands v United States) (1928) II Reports Int Arbitr Award 829

Nuclear Tests (Austl v Fr) - Judgement [1974] ICJ Reports 253

Phosphates in Morocco - Preliminary Objections (1938) Series A/B Collect Judgments, Orders Advis Opin

Rainbow Warrior (New Zealand v France) (1990) 20 215

The Case of the SS Lotus (France v Turkey) - Judgment (1927) Series A Collect Judgments 1

United States Diplomatic and Consular Staff in Tehran (USA v Iran), Judgement [1980] ICJ Reports 3

Ministry of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace 2019

——, Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace 2019 1

Charter of the Organization of American States 1948

Charter of the United Nations 1945

Helsinki Final Act 1975 1

Resolution 138 (1960) Question relating to the case of Adolf Eichmann 1960

United Nations Convention on the Law of the Sea 1982

Vienna Convention on the Law of Treaties 1969