

Sovereignty in Cyberspace on the Usurpation of Political Independence

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

“Sovereignty is a funny thing. It is allegedly the foundation of the Westphalian order, but its exact contours are frustratingly indeterminate.”¹

ABSTRACT

Sovereignty is a complex notion of international law, and not less disputed in the current digital era. The question raised by some States is whether sovereignty is a ‘mere’ principle of international law in the virtual cyberspace or a principle and a binding rule as it is in other physical domains. Though a growing number of States have provided legal opinions regarding this topic, many are reticent in doing so. But, international co-operation in cyberspace is challenging if the rules of the game, including the notion of State sovereignty, are not clear. The issue is not semantic; if sovereignty is not a binding rule, cyberspace activities below a coercive intervention cannot be labelled an international wrongful act.

This article argues that sovereignty – which is based on territorial integrity and political independence - is a binding rule and a principle of international law in cyberspace. Sovereignty in cyberspace will however not be based on territorial integrity but on political independence. The method used to substantiate the argument is to compare the actual 1965 usurpation – or taking over - of State functions in (then) Southern Rhodesia to a fictitious present-day case of election interference via cyberspace. In the case of a fictitious remotely executed cyber activity, territorial integrity will most likely not be violated since no physical or functional damage occurs. However, a cyber operation executed from abroad can and will violate the inherently governmental functions of the State, such as taxation, law enforcement or elections. Clarity regarding the exact threshold when inherently governmental functions are violated will require further State

** Peter Pijpers PhD is associate professor Cyber Operations at the Netherlands Defense Academy and researcher at the Amsterdam Center of International Law, Bart van den Bosch PhD is a former associate professor Military Law at the Netherlands Defense Academy. The authors would like to thank Prof Dr Marten Zwanenburg and Prof Dr Nicholas Tsagourias and the reviewers for their comments on earlier drafts of the article. Corresponding address: b.m.j.pijpers@uva.nl

¹ Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. LAW REV. 1579 (2017).

practice. However, questioning ‘when’ sovereignty is breached affirms the existence of a binding rule of sovereignty in cyberspace.

INTRODUCTION

On 11 November 1965, the government of Rhodesia issued a unilateral declaration of announcing its independence as a sovereign State. Until November 11th, (Southern) Rhodesia on paper was a colony of the British Empire but contrary to this status it held a unique position as it became a self-governing colony since 1923, constitutionally not different from a dominion.²

The unilateral declaration followed a protracted dispute between the British and Rhodesian governments over the terms of independence. The United Kingdom (UK) adhered to the condition, that colonies needed to have a government representing the majority of the population to gain independence, which contradicted the practice of the white minority governing Southern Rhodesia.

The following day the Security Council of the United Nations (UN) adopted Resolution 216³ condemning the unilateral declaration, and on 20 November Resolution 217 condemning the ‘usurpation of power by a racist settler minority in Southern Rhodesia’⁴ and ‘*Calls upon* all States not to recognize this illegal authority and not to entertain any diplomatic or other relations with it’.⁵

While sovereignty in general has been a complex legal notion, the UN Security Council resolution 217 clearly stated that the usurpation of power had no legal validity in the case of Southern Rhodesia and through this denial accepting its existence.

Sovereignty is not less undisputed in the current digital age.⁶ A prominent topic in contemporary legal discourse relates to the question whether sovereignty is a legally binding rule in cyberspace or ‘merely’ a principle.⁷ Though sovereignty has been a rule of international law, the

² A dominion was a self-governing nation of the British Empire. When the British Empire transformed into the commonwealth of Nations, the dominions became independent States.

³ Security Council resolution 216, S/RES/216 (12 November 1965).

⁴ Security Council resolution 217, S/RES/217 (20 November 1965). under 3.

⁵ Security Council resolution 217, S/RES/217 (20 November 1965). under 6.

⁶ See Michael N. Schmitt, *Taming the Lawless Void: Tracking the Evolution of International Law*, 3 TEXAS NATL. SECUR. REV. 32 (2020).; Michael N. Schmitt, “*Virtual*” *Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHIC. J. INT. LAW (2018).

⁷ Michael N. Schmitt, *France’s Major Statement on International Law and Cyber: An Assessment*, JUST SECUR. (2019). under ‘sovereignty’; PRZEMYSŁAW ROGUSKI, *Application of International Law to Cyber Operations : A Comparative Analysis of States’ Views*, THE HAGUE PROGRAM FOR CYBER NORMS POLICY (2020). 3-4; DUNCAN B. HOLLIS, *Improving*

emergence of cyberspace has triggered States and scholars to reconsider that status and not all are persuaded that sovereignty is a rule of law in cyberspace.⁸ 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, and the specific 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 element (such as the computer, routers or network cables) is connected to a territory,⁹ while the virtual aspects, which are both the data, (software, code, 0s & 1s), and the virtual persona (reflections of persons and organization in cyberspace e.g. X (Twitter) accounts) are non-tangible and therefore ‘deterritorialised’.¹⁰ The physical and virtual components are not intrinsically linked. Technologies such as blockchain do not store data on a central mainframe, but in a distributed and decentralized manner in which transactions are based on peer-level consent. Since blockchain software is not connected to a single mainframe (or computer), there is no direct link between the software (the virtual dimension) and the physical location of the ICT infrastructure, hence to the territory of a State.¹¹

The discourse whether sovereignty is a principle or a rule *and* a principle in cyberspace, is not semantic. Article 38(1) of the Statute of the International Court of Justice (ICJ) makes a difference between international conventions, international customary law and the general

Transparency International Law and State Cyber Operations (OAS - Fourth Report), 19 (2020). 18. The discourse on sovereignty as mentioned here is set in a dichotomic setting and does not take away that sovereignty as a principle can still have legal consequences. See: Nicholas Tsagourias, *Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace*, 9 EUR. SOC. INT. LAW REFLECTIONS SER. (2020).

⁸ Jeremy Wright, *Cyber and International Law in the 21st Century*, CHATHAM HOUSE (2018).

⁹ MICHAEL N. SCHMITT, *TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS* (2nd ed. ed. 2017). Rule 1, 15-18.

¹⁰ Jackson Adams & Mohamad Albakajai, *Cyberspace: A New Threat to the Sovereignty of the State*, 4 MANAG. STUD. 256 (2016).; Nicholas Tsagourias, *The Legal Status of Cyberspace: Sovereignty Redux?*, in RESEACH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE (Nicholas Tsagourias & Russell Buchan eds., 2nd ed. 2021). 13-14.

¹¹ See also the discussion in SCHMITT, *supra* note 9. 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.

principles of law.¹² Principles can be viewed as normative propositions while rules (laid down in treaties or extant in customary international law) are international obligations. Principles of international (humanitarian) law include proportionality, humanity and necessity, though some standards are a principle and a rule of customary international law, such as the prohibition of the use of force, which are even recognized in treaties.¹³

The legal consequences are crucial in this discourse. The consequences of violating an international obligation such as sovereignty depends on whether that obligation has been framed as a treaty regulation, an article of customary international law or a legal principle. Whenever a State argues that sovereignty is a principle and not a rule it means the State declares that the breaching the standard has no legal consequences. The latter can be problematic since 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: the violation needs to be attributable to a State under international law but, first and foremost, an international rule (or obligation) 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 cannot be considered unlawful and will not constitute an internationally wrongful act and redress cannot be invoked.

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 usurpation of state functions in the 1965 Rhodesia case, with a fictitious case of cyber-related usurpation.¹⁶ Would a 'digital usurpation' still be a violation of sovereignty? Or will the

¹² United Nations, *Statute of the International Court of Justice Article 38(1)*, 93. Apart from the judicial decisions and the teachings of the most highly qualified publicists which can be applied as subsidiary means.

¹³ These sources of law do not completely overlap see e.g. Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports (1986). Bullet 181.

¹⁴ United Nations General Assembly, *Responsibility of States for Internationally Wrongful Acts - A/RES/56/83* (2002).; JAMES CRAWFORD, *THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY : INTRODUCTION, TEXT AND COMMENTARIES* (James (James Richard) Crawford ed., 2002). 81.

¹⁵ CRAWFORD, *supra* note 14. 81. See also: United States Diplomatic and Consular Staff in Tehran (USA v Iran), Judgment, ICJ Reports 3 (1980).; PCIJ, *Phosphates in Morocco - Preliminary Objections*, Series A/B Collect. Judgments, Orders Advis. Opin. (1938). 28.

¹⁶ The theme is inspired by examples given in: Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. LAW REV. 1639 (2017). 1659-1660, and discussions with Prof Dr T.D. Gill. Schmitt & Vihul specifically refer to the virtual versions of the 1960 Eichmann incident, the 1978 Soviet Spacecraft Cosmos 954 and the 2014 Russian occupation of the Crimean Peninsula.

characteristics of cyberspace force us to revisit this fundament of international law?

This article will first describe pre-cyberspace sovereignty based on case law and will assess the violation of sovereignty in the 1965 Rhodesian case study (section I). Then, in section II, the appreciation of sovereignty will be transposed to a 2020s cyber-related case of taking-over power via election interference (the virtual usurpation case). After describing the discourse on sovereignty in cyberspace, an assessment is made on whether inherently governmental functions can be virtually usurped and 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 IV), we will reflect on sovereignty in cyberspace (section III).

A baseline for this article is that despite the growing number of international actors, the legal notion of sovereignty only applies in the relation between States.¹⁸ Furthermore, this article is limited in several ways. First, the article does not analyze the Rhodesian process of decolonization. The only purpose of using the 1965 Rhodesian case study is to be able to make an analogy in cyberspace of the usurpation of political independence – as also alluded in the UN Security Council resolution – without referring to a violation of territorial integrity. Second, the focus is on public international law between States, while internal law will not be taken into account. And finally, this article will not provide universal criteria for State behavior regarding violating sovereignty but will make an appreciation of a specific situation.

I. 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 1965 Rhodesian case study 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, *supra* note 9.

¹⁸ *Id.* rule 4(2) 17; Tsagourias, *supra* note 10. 12.

¹⁹ See i.a. Quincy Wright, *Subversive Intervention*, 54 AM. J. INT. LAW 521 (1960). 522; Samuel K N Blay, *Territorial Integrity and Political Independence*, MAX PLANCK ENCYCL. INT. LAW (2010). A.1.

A. *Sovereignty: territorial integrity and political independence*

Sovereignty cannot easily be summarized.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 results in 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 recognized 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. Though sovereignty can and has been categorized in numerous ways,²⁵ 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

²⁰ See i.a. James Crawford, *Sovereignty as a Legal Value*, in THE CAMBRIDGE COMPANION TO INTERNATIONAL LAW 117 (2012). 117-119.

²¹ JAMES R CRAWFORD, BROWNLIE’S PRINCIPLES OF PUBLIC INTERNATIONAL LAW (9th ed. ed. 2019). 432; for a concise overview of the origins of modern international law, see GLEIDER HERNANDEZ, INTERNATIONAL LAW (2019). Chapter 1, 3-29.

²² Crawford, *supra* note 20. 120-123.

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

²⁴ Eric Jensen, *Cyber Sovereignty: The Way Ahead*, 50 TEX. INT. LAW J. 275 (2015). 285; Arthur Watts, *Sovereignty*, ENCYCLOPEDIA PRINCETONIENSIS (2019).

²⁵ Blay, *supra* note 19. Under A; I ROBERT JENNINGS & ARTHUR WATTS, OPPENHEIM’S INTERNATIONAL LAW (9th ed. 2008). 382. Others make a similar division, see: Crawford, *supra* note 20. 131-132; United Nations, *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, *supra* note 6. 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 & Albrecht Randelzhofer, *Purposes and Principles, Article 2 (4), I in THE CHARTER OF THE UNITED NATIONS: A COMMENTARY* (Bruno Simma et al. eds., 3rd ed. 2014). 215-217. See Article also 2(4) of the United Nations, *supra* note 25.; United Nations Information Organization (UNIO), *United Nations Conference on International Organization (UNCIO)- Volume VI* (1945). 334-335; CRAWFORD, *supra* note 21. 200.

Territorial integrity includes the inviolability of, and respect for the territorial boundaries, the connected territorial sea and airspace above it.²⁷ The State has exclusive authority and power 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.

Political independence enables a State to ‘freely pursue a path to economic, social and cultural development of its choice’,²⁸ conducive to executing the ‘functions of the State’,²⁹ or the ‘inherently governmental functions’,³⁰ i.e. collection of taxation, conduct of elections, law enforcement or the conduct of diplomacy.³¹ Political independence also means that States can engage with, and enter into relations with other sovereign States on an equal footing.

B. Sovereignty as a rule

Without dwelling on the history of sovereignty,³² in modern times sovereignty has been a binding rule of international law. This in effect means that sovereignty is not only a principle of 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,³³ 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.³⁴

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).³⁵ Also the regional Organization of American States refers to sovereignty, territorial

²⁷ Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 U.S. NAV. WAR COLL. INT. LAW STUD. 123 (2013). 128-131.

²⁸ Benedikt Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, in PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE (2013). 191.

²⁹ PCA, *supra* note 23. 838.

³⁰ Schmitt, *supra* note 6. 45; SCHMITT, *supra* note 9. 21-22.

³¹ Marko Milanovic & Michael N. Schmitt, *Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic*, 11 J. NATL. SECUR. LAW POLICY 247 (2020). 7-10.

³² HERNANDEZ, *supra* note 21. 5-26.

³³ 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, *supra* note 13. Paras 212-213, 111.

³⁴ James Crawford, *Articles on Responsibility of States for Internationally Wrongful Acts*, UNITED NATIONS AUDIOV. LIBR. INT. LAW (2012). 211ff.

³⁵ United Nations, *supra* note 25.

integrity and independence in the first article of its charter.³⁶ Likewise the Helsinki Final Act speaks about juridical equality, territorial integrity and freedom and political independence as attributes inherent to sovereignty.³⁷

Though regional or thematic treaties mention aspects of sovereignty,³⁸ 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 ICJ.³⁹

Case law on sovereignty is extensive. The judgment of the Permanent Court of International Justice in the 1927 *Lotus* Case, 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.⁴⁰ The most prominent articulation of sovereignty, as stated above, is given by Judge Huber in the 1928 *Island of Palmas* arbitral award,⁴¹ a view that was reiterated by Judge Alvarez in an individual opinion to the ICJ judgment in the *Corfu Channel* Case.⁴²

The 1949 *Corfu Channel* Case (United Kingdom vs Albania) is important for two reasons. First of all, the ICJ judgment states that ‘(b)etween independent States, respect for territorial sovereignty is an essential foundation of international relations’.⁴³ And second, the ICJ queries whether the sovereignty of Albania was violated by the UK. 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 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 mid-1960s, in which the Rhodesian declaration of independence was issued, sovereignty was violated on numerous occasions and was brought to the ICJ or a similar courts or arbitrary tribunals.⁴⁴ In the

³⁶ OAS, *Charter of the Organization of American States*, (1948). Article 1.

³⁷ CSCE, *Helsinki Final Act*, 1 (1975). 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*, in PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 217 (2013). 220.

³⁸ United Nations Convention on the Law of the Sea, (1982).

³⁹ Schmitt and Vihul, *supra* note 16. 1650ff.

⁴⁰ PCIJ, *The Case of the S.S. Lotus (France v. Turkey)* - Judgment, Series A Collect. Judgments 1 (1927). 18.

⁴¹ PCA, *supra* note 23. 838.

⁴² *Corfu Channel (U.K v. Alb.)*, 1949 I.C.J. (Opinion of Judge Alvarez), ICJ Reports 43 (1949).

⁴³ *Corfu Channel Case (merits)* - Judgment of 9 April 1949, ICJ Reports (1949). 35.

⁴⁴ 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*

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.⁴⁵ Though the ICJ decided not to pursue litigation, the case not only denotes the existence of territorial integrity of a State but also underscore that a violation thereof breaches a binding rule.⁴⁶

The 1986 ICJ judgment in the *Nicaragua Case* refers to territorial integrity and sovereignty numerous times,⁴⁷ 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,⁴⁸ and related to unauthorized overflights.⁴⁹

In the 1986 *Rainbow Warrior Arbitration* it was held that France violated the territorial integrity of New Zealand,⁵⁰ by sinking the Greenpeace ship *Rainbow Warrior* in Auckland harbor, executed by agents of the French intelligence service.

The obligation to respect the sovereignty of States as a rule of customary law is also echoed in numerous declarations of the UN. The 1970 United Nations General Assembly declaration on Friendly Relations emphasizes the importance of sovereign equality of States.⁵¹ 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,⁵²

Costa Rica Along the San Juan River - Judgment of 16 December 2015, ICJ Reports (2015). 740ff., para 229.

⁴⁵ *Nuclear Tests (Austl. v. Fr.) - Judgment*, ICJ Reports 253 (1974).

⁴⁶ *Id.* para 18, 258.

⁴⁷ *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, *supra* note 13. Para 212, when referring to the laying of mines, 111.

⁴⁸ *Id.* 111, para 213. The prohibited use of force regarding the laying of mines is discussed, 118, para 227.

⁴⁹ *Id.* 128, para 251.

⁵⁰ Reports of International Arbitral Awards, *Case Concerning the Differences between New Zealand and France Arising from the Rainbow Warrior Affair*, XIX UNITED NATIONS PUBL. 199 (1986). 209.

⁵¹ UNITED NATIONS GENERAL ASSEMBLY, *supra* note 26. Under ‘the principle of sovereign equality of States’.

⁵² UNITED NATIONS GENERAL ASSEMBLY, *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence*

and is confirmed in the 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States.

C. Sovereignty in the Rhodesian Case Study

The 1965 declaration of independence by the then-government of Southern Rhodesia was not necessarily a breach of territorial integrity, in the sense that those disseminating the declaration were legal inhabitants of the British Empire, a sovereign State of which Rhodesia was an integral part. The incident was, however, a violation of political independence of the UK since Southern Rhodesia was part of the British realm.

The political independence was violated because by declaring themselves independent the then incumbent government of Southern Rhodesia took over the UK State functions including the appointment of State officials, national security, engage in diplomatic relations and law enforcement. This activity can be labelled as a usurpation due to the unauthorized and non-consensual nature of taking over executive power from the UK.⁵³ The violation of UK sovereignty was unlawful as underlined by the UN Security Council resolutions.

II. SOVEREIGNTY IN CYBERSPACE

This section starts with describing the on-going discourse regarding sovereignty in cyberspace, after which a case will be laid out making a digital analogy to the usurpation of State functions as described in the 1965 Rhodesian unilateral declaration of independence. This virtual case will be tested against territorial integrity and political independence, to assess whether sovereignty is a legal rule in cyberspace or not.

A. The 'sovereignty in cyberspace'-discourse

Sovereignty as a binding legal rule has a firm foundation in international law.⁵⁴ The obligation to respect sovereignty is a primary rule of law, and the breach of which constitutes a violation of international law. 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

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."

⁵³ Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT. LAW 1 (2017). 6-7 (note 30).

⁵⁴ See e.g. United Nations, *supra* note 25.

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.’⁵⁵

But sovereignty in cyberspace appeared not to be undisputed. Since mid-2016 a discussion between several States and legal scholars has been ongoing, in which some challenge the concept of sovereignty as a rule in cyberspace.⁵⁶ The fact that many States refrain from providing their legal opinion on the issue is not helpful for the argument but does not mean that they reject sovereignty as a rule.⁵⁷

The idea that sovereignty is a principle but not a rule in cyberspace, is the current UK position.⁵⁸ In 2016 UK Attorney General Wright stated that the emergence of cyberspace has posed questions regarding the applicability of international law.⁵⁹ 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.’⁶⁰

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.’⁶¹ 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’.⁶² Others argue that the prohibition of the

⁵⁵ Schmitt, *supra* note 7. 2.

⁵⁶ See e.g. Michael N. Schmitt, *The Defense Department’s Measured Take on International Law in Cyberspace*, JUST SECUR. (2020).; Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, 111 AJIL UNBOUND 213 (2017).; Przemysław Roguski, *Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach*, in GOVERNING CYBERSPACE 65 (Dennis Broeders & Bibi van den Berg eds., 2020). 67-69.

⁵⁷ Barrie Sander, *The Sound of Silence : International Law and the Governance of Peacetime Cyber Operations*, 1 (2019).

⁵⁸ 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, *supra* note 7. 18-20.

⁵⁹ Wright, *supra* note 8.

⁶⁰ *Id.* (2018), hereafter “UK Wright Speech”.

⁶¹ Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207 (2017). 208.

⁶² *Id.* 208.

use of force, and intervention are applicable to cyberspace,⁶³ but ‘(p)recisely when a non-consensual cyber operation violates the sovereignty of another State’⁶⁴ is still undefined and would require more State practice and *opinio iuris*. A final scholarly, but also State view is that for the ICT infrastructure (hence the physical part of cyberspace) sovereignty as a rule applies, this is not necessarily the case for the virtual dimension of cyberspace.⁶⁵

Though many States remain silent on whether sovereignty is a rule (and a principle) or a principle (without legal consequences) in cyberspace,⁶⁶ a growing number of States, including Australia,⁶⁷ New Zealand,⁶⁸ Estonia,⁶⁹ France,⁷⁰ the Netherlands,⁷¹ Germany,⁷² and Canada⁷³ have given their legal opinion on the applicability of international law in cyberspace including reference to sovereignty.⁷⁴ For France sovereignty is a

⁶³ See Schmitt, *supra* note 56.; Robert Chesney, *The Pentagon’s General Counsel on the Law of Military Operations in Cyberspace*, LAWFARE 1 (2020). Under 4 c-d; Paul C. Ney, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, (2020). Under B. International law.

⁶⁴ Brian Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT. LAW (2016).

⁶⁵ This is the position of Ecuador, but also Chile and the US are inclined to this view. See: HOLLIS, *supra* note 7. Para 51, 19.

⁶⁶ 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, *supra* note 7. 2-3.

⁶⁷ AUSTRALIAN GOVERNMENT DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, AUSTRALIA’S INTERNATIONAL CYBER ENGAGEMENT STRATEGY (2017).

⁶⁸ NEW ZEALAND MINISTRY OF FOREIGN AFFAIRS & TRADE, *The Application of International Law to State Activity in Cyberspace*, (2020).

⁶⁹ Kristi Sits, *President of Estonia : International Law Applies Also in Cyber Space*, in CYCON 2019 1 (2019).

⁷⁰ MINISTÈRE DES ARMÉES, *Droit International Appliqué Aux Opérations Dans Le Cyberspace*, (2019).; See also Michael N. Schmitt, *France Speaks Out on IHL and Cyber Operations : Part I*, EJIL 1 (2019).; Przemysław Roguski, *France’s Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I*, OPINIOJURIS 1 (2019).

⁷¹ 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*, JUST SECUR. (2019).

⁷² GERMAN MINISTRY OF FOREIGN AFFAIRS, *On the Applicability of International Law in Cyberspace*, (2021).

⁷³ GOVERNMENT OF CANADA, *International Law Applicable in Cyberspace*, (2022).

⁷⁴ The discussion is not confined to Europe and the US, also in the Organization of American States silence is broken. Bolivia, Guatemala and Guyana argue that sovereignty is a stand-alone rule that can be breached in cyberspace. Others are less outspoken and some suggest it only a principle. See: Duncan B Hollis, Ben Vila & Daniela Rakhlina-Powsner, *Elaborating International Law for Cyberspace*, DIR. CYBER DIGIT. EUR. (2020).; HOLLIS, *supra* note 7. Para 52, 19.

rule both in the physical world as well as in cyberspace,⁷⁵ stating that it will protect the sovereignty of the information systems located on its territory, is willing 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 the violation thereof constitutes an internationally wrongful act,⁷⁹ related to the territorial integrity and the inherently governmental functions of a State.⁸⁰ The German position paper on the application of international law to cyberspace echoes that sovereignty is both a principle and rule of international law,⁸¹ thereby providing an elaborate distinctive interpretations of political interdependence and territorial integrity related to different layers of cyberspace. Similar positions are reflected in the legal opinions of Austria, the Czech Republic, Finland and Switzerland.⁸²

Other States are less outspoken or remain ‘on the fence’.⁸³ The United States (U.S.) take a more nuanced⁸⁴ or murkier⁸⁵ stance, and though

⁷⁵ Schmitt, *supra* note 7.

⁷⁶ SGDSN, *Revue Stratégique de Cyberdéfense* (2018). 82.

⁷⁷ MINISTÈRE DES ARMÉES, *supra* note 70. 6.

⁷⁸ *Id.* 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*, 1 (2019). 2.

⁸⁰ The Netherlands follows the rationale of the Tallinn Manual. See also: SCHMITT, *supra* note 9. Rule 4, 20.

⁸¹ Michael N. Schmitt, *German Position on International Law in Cyberspace - Part I: General International Law*, JUST SECUR. (2021).; GERMAN MINISTRY OF FOREIGN AFFAIRS, *supra* note 72. pp. 2-4.

⁸² And also New Zealand considers this position. See: NEW ZEALAND MINISTRY OF FOREIGN AFFAIRS & TRADE, *supra* note 68. Swiss Ministry of Foreign Affairs, *Position Paper on Switzerland's Participation in the UN OEWG and UNGGE*, (2020).; Czech Republic Ministry 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*, JUST SECUR. (2020).; Austrian Ministry of Foreign Affairs, *Pre-Draft Report of the OEWG - ICT*, (2020).

⁸³ Including Israel, see: Roy Schondorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, EJIL 1 (2020).; Michael N. Schmitt, *Israel's Cautious Perspective on International Law in Cyberspace: Part I (Methodology and General International Law)*, JUST SECUR. (2020).

⁸⁴ Tsagourias, *supra* note 7.

several statements have been issued,⁸⁶ 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.⁸⁷ 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 or use of force against the territorial integrity and political independence of other States.⁸⁸

A different position is taken by States member of the Shanghai Cooperation Organization (SCO), including China and the Russian Federation. A Joint Statement by China and the Russia Federation on cooperation in Information Space Development supports the principle of national sovereignty within the UN framework,⁸⁹ and highlights that ‘the principle of sovereignty enshrined in the UN Charter covers all aspects of state-to-state relations, which also includes cyberspace.’⁹⁰ While the language appears neutral China argues that cyberspace sovereignty is a ‘natural extension of state sovereignty in cyberspace’,⁹¹ cyberspace is thus governed by domestic laws and no distinction is made between virtual and physical elements of cyberspace. Numerous authoritarian States highlight that sovereignty is not restricted to physical boundaries but argue that States also have digital sovereignty i.e. national control of all ICT aspects within the State borders.

The dawn of cyberspace commenced a discourse on whether sovereignty also applies to cyberspace. Public international law can change over time based on divergent State behavior, or the characteristics of new developments which differ from the time the law emerged. Peculiar to the discourse on the application of international law to cyberspace is that, without any substantial State practice, the legal opinion of States is that the prohibition of intervention and the (threat or) use of force applies to

⁸⁵ HOLLIS, *supra* note 7. 20.

⁸⁶ Ney, *supra* note 63.; Egan, *supra* note 64.

⁸⁷ AUSTRALIAN GOVERNMENT DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, *supra* note 67. Annex A, p. 91; Australian Government, *Australia’s Position on the Application of International Law to State Conduct in Cyberspace (Annex B)* (2020).

⁸⁸ Sits, *supra* note 69. First and fifth bullet.

⁸⁹ JOINT STATEMENT BETWEEN THE PEOPLE’S REPUBLIC OF CHINA AND THE RUSSIAN FEDERATION ON COOPERATION IN INFORMATION SPACE DEVELOPMENT, (2016).

⁹⁰ Ministry of foreign affairs of the people’s republic of China, *International Strategy of Cooperation on Cyberspace* (2017). Chapter II para 2.

⁹¹ Zhang Xinbao & Xu Ke, *A Study of Cyberspace Sovereignty*, 4 CHINA LEG. SCI. 33 (2016). p. 34.

cyberspace,⁹² which is not being extended to the legal standard of sovereignty.

The authors take note of the discussion but argue, in line with the Tallinn Manual scholars⁹³ and the *opinio iuris* of numerous States, that sovereignty has legal consequences and is therefore both a principle and a binding legal rule in cyberspace which will be underlined with a fictitious case of the next section.

B. The 'virtual usurpation'-case

Sovereignty in the 1965 Rhodesian case study was violated since the political independence of the UK was breached unlawfully.⁹⁴ But can the rule and principle of sovereignty, which has a sound foundation in the notion of territory,⁹⁵ 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?⁹⁶

To test the binding legal rule of sovereignty a fictitious case is presented in which a foreign State A tampers with the national presidential elections in State B, making use of cyberspace.

⁹² Dale Stephens, *Influence Operations & International Law*, 19 J. INF. WARF. 1 (2020). 6.

⁹³ See e.g. Schmitt and Vihul, *supra* note 16. 1649; Corfu Channel Case (merits) - Judgment of 9 April 1949, *supra* note 43. 35; Case Concerning Military and Paramilitary Activities in and against Nicaragua, *supra* note 13. 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.

⁹⁴ United Nations official documents, 865-68th meetings (22 June 1960), Bullet 47, 10.

⁹⁵ Nicholas Tsagourias, *The Legal Status of Cyberspace*, in RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 13 (2015). 17.

⁹⁶ Article 31 of the Vienna Convention on the Law of Treaties, (1969).

The African State B, located near the Zambezi river, is a State with a wealth of natural resources. Resources that attract foreign investors from the European Union (EU), China and the Russian Federation. State B is up for elections, and after preliminaries, there are two remaining candidates for the presidency of State B. One is pro-African, wanted to have a better but equal relationship with the EU and North America and seeks a more prominent role in the African Union. The other is averse of any relationship with the former colonial powers in Africa and wishes to tighten (trade) arrangements with State A which has close ties with China and Russia.

In the run-up to the elections the national electoral commission has been hacked and data of the candidates, including their financial and personnel data, has been pilfered. The lists of registered voters have been scanned and research provided evidence that malware has been planted in the software that counts the votes. An independent cyber-security firm has indication that a pro-Russian group, operating from State A, is behind the intrusion. Apart from these cyber activities an intense information and influence campaign exists especially in favor of the anti-colonial candidate and libeling the pro-EU candidate. The campaign is mainly directed towards minorities in State B, that perceived to be disregarded during the previous pro-EU presidencies.

On election day, the anti-colonial candidate won with 85% of the votes. The national election commission protested since they found irregularities in the electronic voting system and stated that the results were out before the last polling stations were closed.

State B has addressed State A on the issue during a UN meeting, referring to the due diligence responsibilities. State A denied all accusations and argued that they would gladly discuss the issue with the new president-elect.

C. Sovereignty in the 'virtual usurpation-case

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

Territorial integrity is based on the territory of the State. Activities (cyber or other) of agents of State A which are present in State B would constitute a breach of territorial integrity if these agents are in State B without permission, such as during the 1960 Eichmann case or in the run-up to the 2016 U.S. presidential election.⁹⁷ A remote cyber operation as in this

⁹⁷ By June 2014 the Russian agents travelled to the U.S., see: Todd C Helmus, *Social Media and Influence Operations Technologies: Implications for Great Power Competition*, in STRATEGIC COMPETITION 2020 (Thomas F. Lynch ed., 2020). 156; United States District Court, Indictment (United States v Internet Research Agency LLC), 1:18-32 (2018). 12-13. For the Eichmann case, see e.g.: Hans W. Baade, *The Eichmann Trial: Some Legal Aspects*, 1961 DUKE LAW J. 400 (1961).

case 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 directly connected to the territory of a State. Even 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.⁹⁸ 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,⁹⁹ 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.¹⁰⁰

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.¹⁰¹ Even in Roguski’s interpretation of the intrusion-based approach, not all intrusions constitute a violation of sovereignty. Regular use of ICT infrastructure located on other States would not be an unlawful intrusion, and even unauthorized access would not.¹⁰² The *de minimis*, but also the thresholds on display in the Tallinn Manual are an elaboration of the effect-based doctrine.¹⁰³ 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’,¹⁰⁴

⁹⁸ Roguski, *supra* note 70. ROGUSKI, *supra* note 7.; MOYNIHAN, *supra* note 66. 21-24.

⁹⁹ The French legal opinion has both elements of the act-based and the effect-based approach, see: Ministre de l’Europe et de Affaires Etrangères, *Stratégie Internationale de La France Pour Le Numérique* — (2017).

¹⁰⁰ MOYNIHAN, *supra* note 66. 20.

¹⁰¹ *Id.* 48.

¹⁰² Roguski, *supra* note 56. 79.

¹⁰³ SCHMITT, *supra* note 9. Rule 4. 17ff.

¹⁰⁴ *Id.* Rule 4, 17.

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,¹⁰⁵ a breach of territorial integrity can be agreed upon. In the virtual usurpation case, in which a remote cyber-attack and an influence operation via cyberspace took place, persons were not hurt nor was infrastructure damaged or destroyed.¹⁰⁶

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.¹⁰⁷ This threshold is not reached in the virtual usurpation case. While the election infrastructure was monitored and data was copied and stolen, no permanent (functional) damage to the hard- or software was inflicted.

The third category entails 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 Tallinn Manual experts could not agree if and when these effects would constitute a violation of sovereignty.¹⁰⁸ In the virtual usurpation case, there is no direct effect for the users of the election infrastructure. From a penetration-based approach, however, the possible installment of malware would entail an infringement in the network of a public or private entity which resorts under the State's territorial authority, which is in line with the French *opinio iuris*. It can also be argued that the integrity of the election infrastructure – especially the software – has been violated with the installment of malware. If so, this would also cross the *de minimis* threshold, meaning that States adhering to the German, Netherlands or Canadian opinion would argue that sovereignty is breached. The UK, however, would not and probably neither would the U.S. and Israel.

Much focus is on territorial integrity while the violation in the virtual usurpation case can also be judged against the criterion of political independence, related to the inherently governmental functions. The Tallinn

¹⁰⁵ Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFL. SECUR. LAW 212 (2012), 219- 221.

¹⁰⁶ Bradley Boyd & Herbert S. Lin, *Affecting the Cognitive Dimension of the Information Environment through Cyber-Enabled Information Operations*, 18 J. INF. WARF. 49 (2019), 51.

¹⁰⁷ SCHMITT, *supra* note 9. Rule 4 (13) 20-21.

¹⁰⁸ *Id.* Rule 4 (14) 21.

Manual offers two thresholds for violation of political independence. First the interference with the inherently governmental functions and second, the usurpation thereof.¹⁰⁹

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

In the virtual usurpation case, State A not only interfered with the governmental task of conducting elections, but (to some extent) even took over this function, hence usurping an inherently governmental functions of State B,¹¹⁰ similar to the 1965s Rhodesian case study. Targeting the minorities in State B is an element of interference with the elections of State B since subjects of State B should be free to make their own (political) choice. Taking over the voting system, either via installing manipulated software, or via manipulating the broadcasting agencies that published the election results, is in clear breach with the inherently governmental functions of State B.

III. REFLECTIONS

In the 1965 Rhodesian case study the sovereignty of the UK was violated since a minority in Southern Rhodesia took over the functions of the State thereby breaching the political independence of the UK.

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 fits poorly 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 virtual usurpation 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- or penetration-based approach is followed, arguing that any incursion into the cyber infrastructure of another State would account to a violation of sovereignty. The danger of this approach is

¹⁰⁹ *Id.* Rule 4 (15-19) 21-23; Schmitt and Vihul, *supra* note 16. 1660.

¹¹⁰ Schmitt and Vihul, *supra* note 16. 1660.

that sovereignty will be interpreted subjectively from the position of the offended State, while international law must be applied objectively.¹¹¹ Following this line of argument, with a focus on territorial integrity as the core element of sovereignty, the rationale of speech by UK Attorney General Wright,¹¹² and the reticence of many States to be more outspoken on the matter, is understandable.

However, in the virtual usurpation case, sovereignty was violated, not primarily 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.

IV. 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.¹¹³ It is, therefore, only logical that a large part of the discourse of sovereignty in cyberspace focuses on the territorial aspect of sovereignty and less on 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.

¹¹¹ MOYNIHAN, *supra* note 66. 20. Cognizant that States have different interpretations of aspects of international law, see also: Schmitt, *supra* note 6. 38-40.

¹¹² Wright, *supra* note 8. 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."

¹¹³ Phil Spector, *In Defense of Sovereignty, in the Wake of Tallinn 2.0*, 111 AJIL UNBOUND 219 (2017). 222.

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

Relying on territorial integrity to ascertain that sovereignty as a rule of international law in cyberspace, might prove to be a dead-end street in case of remotely executed operations in the virtual dimension. Not least since a breach thereof is difficult to prove. Conversely, the notion of political independence 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 virtual usurpation case, sovereignty was violated. It was difficult to substantiate that territorial integrity was violated not least since the notion of territoriality is difficult to align with 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,¹¹⁴ as it is in other (physical) domains, based on their political independence. 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.¹¹⁵

¹¹⁴ See SCHMITT, *supra* note 9. 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*, 12404 (2015)..

¹¹⁵ MOYNIHAN, *supra* note 66. 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, *supra* note 64.; Corn and Taylor, *supra* note 61. 210-211. Michael N. Schmitt, *International Cyber Norms: Reflections on the Path Ahead*, MIL. RECHTEL. TIJDSCHR. (2018). 17.