Careful What You Wish For
*Tackling Legal Uncertainty in Cyberspace*

*Peter B.M.J. Pijpers | ORCID: 0000-0001-9863-5618*
Associate Professor of Cyber Operations, Netherlands Defence Academy, Breda, The Netherlands
Researcher at the Centre of International Law (ACIL), University of Amsterdam, Amsterdam, The Netherlands
b.m.j.pijpers@uva.nl

Received: 4 January 2023 | Accepted: 9 August 2023 | Published online: 13 October 2023

**Abstract**

It is commonly acknowledged that international law applies to cyberspace. But “how” it applies is still a matter of dispute; a matter that was hampered by the limited number of legal opinions by States. It was assumed that an increase in *opinio iuris* and State practice would crystalize how international law applies to cyberspace. However, the recent surge in legal opinions has had a contrary effect, i.e. increasing rather than decreasing the differences – and hence the legal uncertainty. This development could even create legal asymmetry: while some States will comply with international law, others will exploit the ambiguity and cherry-pick the interpretation that supports their strategic goals.

**Keywords**

1 Introduction

The Cold War era saw numerous Russian and American (US) interferences in each other’s sphere of influence, mainly within the legal grey areas of
espionage and covert actions. The nature of these influence activities changed fundamentally with the emergence of cyberspace. Current influence operations go well beyond traditional espionage. Russian agents and State-sponsored media (e.g. RT and Sputnik) have actively been interfering with elections and disseminating antagonistic narratives and manipulated information via social media in order to sow doubt and discord.\(^1\) In a research on Sweden, Wagnsson argued that influence operations endanger democracy, social cohesion and national security,\(^2\) which echoes earlier research by Kragh c.s.\(^3\)

The Russian endeavour to affect voters during the 2016 British (UK) EU referendum and the 2016 US presidential elections were examples of such influence operations making use of cyberspace. Though Russia was exposed after the 2016 US presidential elections,\(^4\) the number of digital influence operations has not declined.\(^5\) In the run-up to the 2020 US presidential elections, Russia shifted its cyber operation primarily towards digital influence, leaving out the cumbersome acts of sabotage and hacks on the digital infrastructure (hardware and software).\(^6\) The intensified use of digital influence operations is also witnessed in the prelude to and during the current Russian invasion of Ukraine.\(^7\)

Influence operations via cyberspace are not activities that use force or amount to an armed attack,\(^8\) this in contrast to cyberattacks on the digital

---

infrastructure that affect cyberspace itself, such as the 2010 Stuxnet attack on the nuclear facilities in Natanz.9

The fact that influence activities remain below these thresholds does not render them lawful. States executing foreign influence operations via cyberspace may violate sovereignty and non-intervention.10 Still, States are reticence in their response to such a breach since the threshold of violations is ambiguous. The UK and US response after the 2016 UK EU referendum and the US presidential elections respectively was marginal. Even the Russian violations of sovereignty in the months before the invasion on 24 February 2022 were hardly reacted to.11

While ambiguity in the interpretation of international law is not new, the emergence of cyberspace appears to have increased legal uncertainty.12 The assumption was that the issuance of legal opinions (opinio iuris), combined with evolving State practice, would fill the gaps in how to interpret international law in cyberspace. States were encouraged to share their opinio iuris which, paradoxically enough, has widened rather than narrowed divergence in interpretation. Some States still stay silent on how to interpret international law;13 Israel and the US are powerful and prominent examples of States that have not yet put forward their opinio iuris.14 Others did articulate their legal opinions, but the views expressed were far from aligned.

The problem of the resulting legal uncertainty is that States show restraint in responding to alleged internationally wrongful acts in cyberspace; after all, invoking a countermeasure in response to a dodgy State activity could itself be unlawful. While the legal ambiguity ipso facto means room to manoeuvre, which is useful when confronted with novel developments, legal ambiguity could also be used as an instrument of power; States might pick and choose

13 Which can very well be a calculated decision, see: R. Alcala, ‘Opinio Juris and the Essential Role of States’, *Articles of War* (2021).
the one interpretation that supports their strategic rationale. These diverging avenues will create an unwanted legal asymmetry.\(^\text{15}\)

The objective here is to explore how legal uncertainty in cyberspace emerges, why this leads to legal asymmetry and how to tackle it. To answer these questions, first a brief explanation on the case study of the article, i.e. influence operations in cyberspace (section 2), is given, after which the standards of sovereignty and non-intervention (section 3) are explained. This is followed by an analysis of how sovereignty and non-intervention apply to (influence operations in) cyberspace (section 4) and how this can result in legal uncertainty (section 5). Legal uncertainty might be inducive to an asymmetrical application of international law, and the question is how to tackle this (section 6).

2 The Concept of Influence Operations in Cyberspace

Influence operations, whether they are described as Active Measures or Political Warfare, are nothing new.\(^\text{16}\) The inception of cyberspace has, however, changed the dynamics and characteristics of influence operations, not least by adding new digital layers in our information environment in which influence can be exerted.\(^\text{17}\)

Cyberspace is a man-made domain encompassing the virtual dimension (the logical and the virtual persona layer) and part of the physical dimension (the physical network layer) (figure 1). Operations in cyberspace can target the layers in cyberspace but can also use them as a vector to affect the cognitive dimension. Activities involving the use of cyberspace can entail (i) digital


FIGURE 1 Information Environment and Cyberspace

---

Espionage, or Computer Network Exploitation (CNE), extracting data confined in virtual repositories; (ii) operations that undermine or subvert cyberspace itself (Computer Network Attacks (CNA)) with binary code, in order to modify or manipulate data, and to degrade or destroy the ICT infrastructure, resulting in (virtual and physical) effects in cyberspace; or (iii) influence operations that use cyberspace as a vector, and target the cognitive dimension, using content, words, memes and footage as a “weapon”.

Not only has cyberspace widened the engagement area by allowing numerous actors (State and non-State) to enter at low cost, but it has also made communication faster and more diffusional. Digital influence operations surgically target specific audiences with bespoke messages based on algorithms and big data analysis, in order to gain insight into the correlation (rather than causality) between activity and effect. Manipulative influence operations lure audiences away from rational decision-making processes towards biased judgements using techniques (e.g. disinformation, trolling or the leaking of sensitive data) that render the targeted audiences unable to validate the authority of the data provided. This in turn prevents the deliberate verification of the information.

The main characteristics of digital influence operations are the absence of the threat or use of force, the focus on the cognitive dimension, and the objective to change the behaviour of other actors directly or indirectly via a change in attitude. These activities can potentially violate sovereignty and the prohibition to intervene in the affairs of another State.

---

Infringements of State Sovereignty

In general, there are different forms of infringement of the integrity of a State related to the use of force, coercion or milder forms of interference (see figure 2). These infringements are often interrelated. The unauthorised use of (armed) force is not only a violation of a peremptory norm, it also breaches the prohibition of intervention and violates the sovereignty of the State. In the 1986 Nicaragua Case, it was stated that the “effects of the principle of respect for territorial sovereignty inevitably overlap with those of the principles of the prohibition of the use of force and of non-intervention”. The reverse, however, is not the case: a violation of sovereignty, such as unauthorised overflight or the exercise of jurisdiction on foreign territory without permission, does not in itself constitute a breach of the prohibition of the use of force. Moreover, the lawful response to an armed attack differs fundamentally from response options related to violations of sovereignty or non-intervention.

Digital influence operations are predominantly executed below the threshold of the (threat or) use of force. Consequently, this analysis focuses

---

**Figure 2 Infringement Overlaps**


---
on interferences of sovereignty and interventions caused by digital influence operations.

3.1 Sovereignty

The legal basis for sovereignty as a primary rule of customary international law is found in State practice and *opinio iuris*, as reflected in decisions of international courts and tribunals, multilateral conventions, and resolutions of the UN General Assembly.

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) of the UN Charter.

Case law on sovereignty is substantial. The 1927 *Lotus* Case argues 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, the political independence and sovereign equality of States which are elements most prominently articulated in the 1928 *Island of Palmas* Arbitral Award: “Sovereignty 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.”

In the 1949 *Corfu Channel* Case, the International Court of Justice (ICJ) highlights the importance of sovereignty by arguing that “[B]etween independent States, respect for territorial sovereignty is an essential foundation of international relations.” In the 1974 *Nuclear Test Case (Australia v. France)*, Australia claimed that the radioactive fall-out from French atmospheric

---

nuclear testing landed on Australian soil, violating its territorial integrity and, hence breaching international law.\textsuperscript{36}

The 1986 Nicaragua Case referred to territorial integrity and sovereignty numerous times, including the obligation under customary international law not to violate these norms. Although in this case violation of sovereignty is often a consequence of a breach of the prohibition of intervention or use of force, sovereignty is also breached as a stand-alone legal obligation in the case of laying mines in Nicaraguan territorial waters,\textsuperscript{37} and in relation to unauthorised overflights by US military aircraft in Nicaraguan airspace.\textsuperscript{38}

The legal obligation of respect for the sovereignty of States in customary international law is echoed in numerous declarations of the UN. The 1970 UN General Assembly (UNGA) Declaration on Friendly Relations emphasises the importance of sovereign equality of States.\textsuperscript{39} The sovereign equality entails not only the judicial equality of States but also highlights the inviolability of territorial integrity and political independence of States and their right to freely choose and develop political, social, economic and cultural systems.\textsuperscript{40}

Based on the 1928 Island of Palmas Arbitral Award, sovereignty of a State is violated if one of its core elements – territorial integrity and political independence – is infringed.\textsuperscript{41}

### 3.2 Non-Intervention

The prohibition of intervention is the corollary to every State’s right to sovereignty.\textsuperscript{42} Non-intervention not only safeguards States from unlawful interference but also gives substance to the concept of sovereign equality.

---


\textsuperscript{37} Case Concerning Military and Paramilitary Activities in and against Nicaragua, supra note 26, para 213. The prohibited use of force regarding the laying of mines is discussed in para 227.


\textsuperscript{39} United Nations General Assembly, supra note 32, under ‘the principle of sovereign equality of States’.

\textsuperscript{40} See e.g.: 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.


\textsuperscript{42} Jennings and Watts, supra note 28 p. 428.
among States. An unlawful intervention breaches a legal obligation and constitutes an internationally wrongful act if attributable to a State.

The prohibition of intervention is widely considered to be both a principle and a rule of customary international law. The legal basis for this primary rule between States vis-à-vis each other can be found in (regional) treaties and in customary international law. Article 2(7) of the UN Charter contains an element of non-intervention stipulating that the UN – not States – should refrain from any form of interference in matters that are essentially within the domestic jurisdiction of the States.

Non-intervention as a customary rule is reflected in case law. In the 1949 Corfu Channel Case, the ICJ rejected the alleged right to intervene. The 1986 Nicaragua Case is a seminal judgment related to the legal interpretation of non-intervention. The ICJ stated that the prohibition of intervention is “part and parcel” of customary international law, and argued (echoing the 1970 UNGA Declaration on Friendly Relations) explicitly that the principle of non-intervention forbids States from intervening directly or indirectly in internal or external affairs of other States.

---


46 See e.g. International Conference of American States, Montevideo Convention on the Rights and Duties of States, Articles 3 and 8; OAS, Charter of the Organization of American States. Articles 9 and 13; Vienna Convention on Diplomatic Relations, Article 41.


49 Corfu Channel Case supra note 35 p. 35.

50 Case Concerning Military and Paramilitary Activities in and against Nicaragua, supra note 26 p. 106.

51 Case Concerning Military and Paramilitary Activities in and against Nicaragua, supra note 26 para 205. On this topic, see also the Case Concerning Armed Activities on the Territory of the Congo, supra note 27 para 165.
The **UNGA** has issued several resolutions related to non-intervention,\(^{52}\) most importantly the 1970 Declaration on Friendly Relations\(^{53}\) mentioned above. **UNGA** resolutions are non-binding, but they can be seen as a confirmation of customary international law.\(^{54}\)

Deriving from customary international law, an intervention contains two elements:\(^{55}\) the interference impacts upon the domestic jurisdiction – *domaine réservé* – of another State, and is coercive in nature.\(^{56}\)

### 4 International Law on Influence Operations in Cyberspace

In general, international law – including the principles of sovereignty and non-intervention – applies to cyberspace.\(^{57}\) Ample legal opinions of States underpinning this have been provided via unilateral statements,\(^{58}\) reports by international organisations, and ad hoc declarations.\(^{59}\) Nonetheless, there is room for interpretation. The question *how* international law applies to cyberspace is still subject to legal discourse.\(^{60}\)

---


\(^{53}\) United Nations General Assembly, see *supra* note 32.


\(^{56}\) *Case Concerning Military and Paramilitary Activities in and against Nicaragua, supra* note 26 para 205; Jennings and Watts, *supra* note 28 p. 430.


4.1 **Sovereignty in Cyberspace**

Sovereignty has a firm foundation in international law, a violation of which is a wrongful act and open to redress. Sovereign equality is one of the cornerstones of the system of international law and it is recognised in Article 2(1) of the UN Charter.\(^61\) To assess the characteristics of a non-coercive violation of sovereignty, this contribution assesses territorial integrity and political independence separately.

Territorial integrity relates to the territory of the State. Territorial integrity signifies the exclusive authority and power the State has over its territory and its public and private residents.\(^62\) This encompasses the inviolability of, and respect for, the territorial boundaries and connected territorial sea and airspace.\(^63\) Cyberspace is partially linked to that territory. The physical network layer,\(^64\) (the computers) that supports the Internet and activities in cyberspace, is generally located on the sovereign soil of a State.\(^65\)

The nature of the incursion is related to the State’s control of the territory but also to the authority and protection of persons, materiel and infrastructure in the territory of the State.\(^66\) An infringement that damages the ICT infrastructure, whether held in public or private hands,\(^67\) could constitute a

---


violation of territorial integrity, since sovereignty “protects all infrastructure within a state”.

Though sovereignty is a legal rule in all domains of engagement, including cyberspace, the challenge is how to apply the notion of territorial integrity to the virtual dimension of cyberspace that – with its dematerialised, detemporalised and deterritorialised characteristics – differs from other domains (land, sea, air) in scale, reach and effect.

Activities in cyberspace can be executed from within the territory of the targeted State, which constitutes a (physical) violation of sovereignty by unauthorised access of foreign State agents. During the 2016 US presidential elections, Russian agents executed digital influence activities from within the US without the latter’s consent, thereby violating its territorial integrity.

Cyber activities can also be executed remotely – from abroad – in which case no border is physically crossed and a violation of territorial integrity is more difficult to substantiate. The most prominent scholarly work qualifying the impact on sovereignty is the second iteration of the Tallinn Manual (Tallinn Manual 2.0). The Tallinn Manual 2.0 lists three criteria for a remotely executed cyber operation violating territorial integrity: physical damage, functional damage and infringements falling below the threshold of functional damage.

---


70 See Schmitt, supra note 43 pp. 11–13. But also, the UN GGE reports, e.g. the United Nations GGE Report, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174 (2015)).

71 Moynihan, supra note 55 pp. 13–14.


73 See the analogous 1960 Eichmann abduction, Schmitt and Vihul, supra note 30 p. 1659; or the Russian attempt to hack the OPCW from within Netherlands’ territory, see: Government of the Netherlands, Russian Cyber Operations Disrupted <https://english.defensie.nl/topics/cyber-security/russian-cyber-operation> visited 8 August 2023.


First, causing physical damage by remote means may qualify as a violation of sovereignty.\textsuperscript{76} Damage to the physical network layer of public or private ICT infrastructure can result from the malfunctioning of systems due to malware.

Second, functional damage could also qualify as a violation of territorial integrity. Where physical damage relates to the physical network layer, the loss of functionality relates to the logical and the virtual persona layers of cyberspace and is at the core of cyber-related interference with sovereignty (especially undermining activities or CNA). Although the experts of the \textit{Tallinn Manual 2.0} could not agree on exact thresholds, permanent functional impairment stems from the degradation, destruction, or disruption of data and is an infringement of the confidentiality, integrity or availability (CIA) of the data or of the system as a whole.\textsuperscript{77}

Due to the lack of a demarcation of functional impairment, activities that do not result in physical or permanent functional damage of systems in cyberspace are difficult to define. Examples are the temporary loss of functionality, CNE including data theft (by copying) or port scanning (reconnaissance) with malicious intent, and the creation of a backdoor for future cyberattacks. Within this remit, there are two interpretations. Either every cyberattack on, or exploitation of, the cyber infrastructure by another State is a violation of sovereignty – what Roguski has called the penetration-based approach.\textsuperscript{78} This is the French\textsuperscript{79} and Iranian\textsuperscript{80} view and in line with Heller’s notion of “pure sovereignty”.\textsuperscript{81} Or an attack requires at least a minimum impact,\textsuperscript{82} which is in line with the German position – what Roguski named the intrusion-based


\textsuperscript{77} See also: Roguski, \textit{supra} note 75 p. 79.


\textsuperscript{80} Armed Forces of the Islamic Republic of Iran, ‘Declaration Regarring International Law Applicable to the Cyberspace’, \textit{Nour News} (2020).


\textsuperscript{82} The maxim of \textit{de minimis non curat lex}, i.e. “the law is not concerned with trivial things”. See also: Jensen, \textit{supra} note 65 pp. 302–303.
approach, arguing that not all infringements violate sovereignty. Regular use of ICT infrastructure located in other States would not, referring to international law, be an unlawful intrusion, neither would unauthorised access. Related to the CIA-trigram, Roguski argues that if the integrity (not the availability or confidentiality) of the data is compromised that would constitute a violation. This interpretation in essence introduces a minimum impact threshold, hence a qualified threshold to assess violations of sovereignty in cyberspace. While this distinction has merit for attacks undermining cyberspace itself, it does not encompass digital influence operations.

The Tallinn Manual 2.0 criteria largely relate to digital undermining operations (CNA) raising the question whether any remotely executed digital influence operation could violate territorial integrity. The remotely executed influence operations during the 2016 UK EU referendum or the 2016 US presidential elections did not meet the criteria of violation of territorial integrity as stipulated in the Tallinn Manual 2.0. The disinformation and trolling campaigns, the fabricated content, misleading media sources or information deluges due to political advertisements did not cause physical damage or (permanent or temporary) loss of functionality to (persons or materiel on) the territory of the State. Furthermore, the digital influence operations did not infringe upon the confidentiality, availability or integrity of ICT system since data were not deleted or altered. The Russian influence operation as such did not violate territorial integrity.

Violation of territorial integrity traditionally relates to physical incursions into the territory of the State. Though remote cyberattacks could cause physical damage or injury and subsequently violate the territorial integrity (and sovereignty) of the State, digital influence operations seldom cause functional impairment, let alone physical damage.

83 Without stating that these intrusions, even in the form of political or economic espionage, will never violate international law, see also: R. Buchan, Cyber Espionage and International Law (Bloomsbury, London, 2019) pp. 53–54.
84 Roguski, supra note 75 p. 79.
85 Moynihan, supra note 55 pp. 21–24.
88 Spector, supra note 38 p. 222.
89 Milanovic and Schmitt, supra note 76 p. 253.
Political independence, on the other hand, can be violated by digital influence operations. Political independence refers to the authority States have over their “inherently governmental functions,” including collecting taxes, defending the State and holding elections.

The State functions can be meddled with (also in cyberspace) via interference or – more severely – usurpation. Usurpation means taking over and performing governmental functions of another State. In cyberspace, a foreign State can usurp the electoral process by changing the results of the voting machines, as was the case in Ukraine in the May 2014 presidential elections.

Interference with the inherently governmental functions means tampering with or frustrating the State’s functions – physical or functional damage is not a requirement. Not all forms of digital influence operations (using social media platforms) interfere with the inherently governmental functions of another State. Unwelcome propaganda and even fabricated information is not unlawful per se. However, when a State uses subterfuges to propagate misleading content – factual or fabricated – or impersonate national citizens, to dissuade voters, or manipulate their ability to make a free and fair appreciation, their political choice is severely impaired. While the Russian influence operation did not violate territorial integrity, political independence was breached during the 2016 UK EU referendum and the 2016 US presidential election.

90 Schmitt, supra note 55 p. 45; Schmitt, supra note 43 p. 20 rule 4(10, 16, 17).
91 Other State functions are conducting diplomacy, enforcing the law, managing crises or establish a system of social welfare official and public communication (e.g. on Covid-19), see also Milanovic and Schmitt, supra note 76 p. 255.
92 As stated in the 1927 Case of the S.S. Lotus, supra note 33 p. 18.
94 Xiao, supra note 87 p. 372.
96 Schmitt, supra note 55 p. 46.
4.2 Non-Intervention in Cyberspace

An intervention is a coercive incursion in the reserved domain of another State. The prohibition of intervention is considered to be both a principle and a rule of customary international law,99 also in cyberspace.100

The domaine réservé, or reserved domain,101 is the area “in which each State is permitted, by the principle of State sovereignty to decide freely. This area is the choice of a political, economic, social and cultural system, and the formulation of foreign policy.”102 The domaine réservé relates to the jurisdiction of a sovereign State,103 a jurisdiction that is not unrestricted.104 The size of the reserved domain of the State is “a relative question”,105 as alluded to in the 1923 Nationality Decrees Case, and the 1923 Wimbledon Case,106 and dependent on the international obligations of the State (figure 3).

The domain of non-intervention is not an uncontested notion. Kilovaty rhetorically questions whether the domaine réservé still is distinctive in “a world where social media platforms have transformed online communications and political campaigning?”107 Moreover, are there still domestic areas that are...
exempt from the effects of international law, especially taking international human rights law into account? However, most ambiguity is connected to the nature of the incursion: coercion.

Intervention is perceived to be wrongful when it “uses methods of coercion in regard to such choices, which must remain free ones.” Coercion is “the very essence of prohibited intervention.” Or as Joyner states: “Coercion in inter-State relations involves the government of one State compelling the government of another State to think or act in a certain way by applying various kinds of pressure, threats, intimidation or the use of force.”

Coercion has been described in different ways in legal writing and case law. Though it “has not yet fully crystallised in international law,” it has legal consequences. In the Nicaragua Case, the ICJ mentioned that coercion

---

108 See Article 49 of the ‘The Charter of Fundamental Rights of the European Union’ articulating the ‘Right to vote and to stand as a candidate at municipal elections.’
109 Case Concerning Military and Paramilitary Activities in and against Nicaragua, supra note 26 para 205.
110 Ibid. para 205.
112 See also Gill, supra note 44 p. 219, providing an outline of the different forms of coercion.
113 Netherlands Ministry of Foreign Affairs, supra note 104 p. 3.
“is particularly obvious in the case of an intervention which uses force in the direct form of military action”.115 Aside from the coercive use of force,116 coercion can be “otherwise coercive”117 when it deprives another State of control, broadening the concept to diplomacy, the economy and other means if they are coercive in nature.118 Coercion can also have a more subtle and psychological dimension, manipulating the opponent’s choices and reducing the number of options to choose from by applying subversive, psychological or manipulative means.119

Apart from deliberately undermining control, the coercer must also pursue a change of policy,120 or intend to effectuate a particular course of action. The intent of the coercer is pivotal,121 as it objectifies the pursuit of a change to the policy. Therefore, coercive interferences that fail to reach a desired outcome still breach the prohibition of intervention.122

While coercion traditionally relates to the threat (or use) of force,123 in cyberspace coercive behaviour will most likely take the shape of non-violent, manipulative, subversive threats through informational means.124 The Tallinn Manual 2.0-experts also struggled with this topic.125 Disseminating foreign propaganda or even fabricated news during elections will not immediately qualify as an intervention, but when digital influence operations (during elections) have the purpose to undermine faith in the integrity of the electoral process, or to alter or manipulate the perceptions and beliefs of the audience.....
in another State,\textsuperscript{126} they might well qualify as intervention, since these coercive efforts are “designed to influence outcomes in ... matters reserved to a target State”.\textsuperscript{127}

The question that remains is: When are (manipulative) digital influence operation coercive? Though different in magnitude, it can be argued that the influence operations during the 2016 UK EU referendum and the 2016 US presidential elections amounted to interventions. The Russian influence operations entailed manipulative activities against the reserved domain – the ability to conduct popular votes – which could amount to coercion, as they constituted a deliberate act to undermine the decision-making process of the targeted States with the aim of policy changes (for the UK leaving the EU, and for the US not to have Clinton elected). Russia sought ways to lure voters into making decisions they might otherwise not have made, using deceitful and manipulative techniques including bots, repetitive social media utterances and political advertising. In the US case, the Internet Research Agency (IRA)\textsuperscript{128} “created fake Facebook accounts and purchased politically charged advertisements intending to influence the outcome of a U.S. election”.\textsuperscript{129} Schmitt argues that the “covert nature of the troll operation deprived the American electorate of its freedom of choice”.\textsuperscript{130}

Manipulation is not coercive per se. However, if coercion can be defined as having the deliberate intent to change the policy of another State by denying the target State its autonomous decision-making capability, then some manipulative influence operations are coercive in nature.

All in all, digital influence operations can violate the prohibition of intervention, as well as political independence, but they are more difficult to align with the notion of territorial integrity since they lack a physical or tangible component.

\textsuperscript{126} A. Reynolds (ed), \textit{Social Media As a Tool of Hybrid Warfare}, (NATO Strategic Communication Centre of Exellence, Latvia 2014). p. 8.


\textsuperscript{129} Denton, supra note 95 p. 199.

\textsuperscript{130} Schmitt, supra note 55 p. 51.
5 Legal Uncertainty

Digital influence operations with malign intent feed the growing distrust in traditional media and governmental institutions and increase cynicism, which can take shape in unwillingness to accept election results and scepticism toward public announcements.\(^\text{131}\) Digital influence operations do not solely create unwanted societal effects, they also amplify ambiguity and legal uncertainty.

5.1 Uncertainty regarding Sovereignty in Cyberspace

International law is not set in stone, and legal leeway provides room to absorb new developments.\(^\text{132}\) However, the lack of clarity, conducive to several interpretations of the law, can also lead to unwanted ambiguity. A case in point is the debate on whether sovereignty is a rule in cyberspace or not.

While most States agree that sovereignty is a primary rule of law in any domain including cyberspace, not all are convinced. In 2018 the UK argued it is not persuaded that a specific rule on sovereignty exists for cyber activities beyond a prohibited intervention.\(^\text{133}\) Academics participated in the debate: Corn and Tayler state that there are sufficient proscriptions against unlawful uses of force and interventions in treaty law and customary international law, but that “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”.\(^\text{134}\)

Despite the silence of some, a growing number of States have since provided their legal opinions on the applicability of international law, including sovereignty, in cyberspace. These States not only include Western States

---


such as France,135 the Netherlands,136 Germany,137 Switzerland,138 Canada,139 Finland140 and Sweden,141 but also China, Russia and Iran.142

Unfortunately, many of them use generic terms that reiterate existing law without expounding on how international law applies to cyberspace. The Australian legal opinion “recognises that activities conducted in cyberspace raise new challenges for the application of international law, including issues of sovereignty”.143 Estonia argues that the “violation of sovereignty through cyber means can breach international law, and therefore may give the victim

135 Ministère des Armées, supra note 79.
136 Netherlands Ministry of Foreign Affairs, supra note 104.
141 Government Offices of Sweden, supra note 58.
state the right to take measures, including countermeasures. Views on what constitutes a breach of sovereignty in cyberspace differ.144

Apart from the UK legal opinion, which was not a one-off,145 also within the group of States accepting that sovereignty is a rule, differences in interpretation exist. A case in point is the interpretation of sovereignty as a rule by France and Switzerland that favour a purist approach to sovereignty, versus Germany, Canada and the Netherlands who argue that “activities causing negligible or de minimis effects would not constitute a violation of territorial sovereignty”.146

Russia and Iran take a different perspective highlighting the legal vacuum existing at the moment.147 China further argues that cyberspace sovereignty is a “natural extension of state sovereignty in cyberspace”,148 whereby cyberspace is governed by domestic law and no distinction is made between virtual and physical elements of cyberspace.

The lack in alignment between and granularity of legal opinions, and the divergence between these opinions and actual State practice fuel ambiguity.

The uneasy fit between digital influence operations and the notion of territorial integrity furthers ambiguous interpretations. Digital influence operations executed remotely by foreign agents do not violate the territorial integrity of the targeted State because no borders are physically crossed. Furthermore, digital influence operations that target the cognitive dimension are unlikely to cause damage and are therefore unlikely to affect the territorial integrity of another State.

Interference with political independence is a more suitable threshold for assessing violations of sovereignty by digital influence operations, although it is not devoid of ambiguity. Defining interference with inherently governmental

146 Government of Canada, supra note 139 bullet 17.
functions is challenging, since both interference and State functions “lack granularity”.

5.2 Uncertainty Regarding Non-Intervention in Cyberspace

Ambiguity is not limited to the interpretation of sovereignty. Contrary to sovereignty, the legal opinions regarding non-intervention are aligned though not always explicit in “how” the rule applies. The Australian legal opinion argues that interventions are prohibited. Estonia states that the principle of non-intervention applies to state conduct in cyberspace but is more explicit in how the reserved domain and coercion applies to cyberspace.

The reserved domain – the domestic jurisdiction that is not regulated by international law – is an inherently relative notion. When applied to cyberspace, the question arises whether the virtual realm erodes this notion even further.

The essential element for an intervention, i.e. coercion, is ill-defined, and it becomes even more intangible when applied to cyberspace. Coercion is obvious when an intervention uses force, but digital influence operations are characteristically below the level of threat (or use) of force. An unwanted development is that the elusiveness of cyberspace has increased the complexity of coercion in cyberspace and the criteria needed to establish it. Cyberspace has significantly increased coercive potential, not only due to the increasing number of (non-State) actors but also because its attributes facilitate the use of covert and subconscious activities. Finally, the veiled operating methods that States use make it difficult to uncover the true purpose and intent of an alleged intervention. The elusive and intangible nature of influence operations
in cyberspace, combined with the need for (legal) clarity, could significantly raise the threshold for establishing coercion. Following this rationale, coercion will only apply when activities bear the semblance of the threat or use of force. This approach – combined with the discourse on sovereignty in cyberspace – does not limit but rather facilitates manipulative influence operations.

6 Tackling Legal Uncertainty

The more States act in cyberspace without a common interpretation of sovereignty and non-intervention, the greater the normative uncertainty will be. This ambiguity could even lead to legal asymmetry.

6.1 From Legal Uncertainty to Asymmetry

Although the grey area\textsuperscript{156} of ambiguity may be unwanted from a legal point of view, it could be beneficial from a political point of view. Differing interpretations of international law concerning cyberspace are conducive to “cherry-picking”.\textsuperscript{157} States can apply international law in a manner that is beneficial to their interests.\textsuperscript{158} The “uneasy fit”\textsuperscript{159} between traditional State-based international law and the a-territorial cyberspace creates tension between States due to the desire to preserve freedom of action for oneself while developing rules to restrict the others.\textsuperscript{160}

The ambiguity surrounding the application of international law in cyberspace is not only “susceptible to exploitation when conducting cyber operations”;\textsuperscript{161} the variations in interpretation also have legal ramifications. After all, a violation of international law, or internationally wrongful act,\textsuperscript{162} implies the

\footnotesize
\begin{itemize}
\item \textsuperscript{156} Schmitt, supra note 55 p. 33.
\item \textsuperscript{157} Schmitt, supra note 86 p. 33.
\item \textsuperscript{159} Kilovaty, supra note 155 p. 89.
\end{itemize}
breach of a primary rule of law, not of non-obligatory principles. Perceiving sovereignty as a non-binding principle implies that it does not constitute an international obligation and that, even if the act can be attributed, the injured State cannot invoke an internationally wrongful act and consequently demand reparation including a reset of the system of international law.\textsuperscript{163} If sovereignty is not a rule of international law, interferences of a non-coercive nature are not unlawful.

6.2  \textit{Tackling Legal Uncertainty and Asymmetry}

Legal uncertainties can be reduced through awareness, resilience and reactive actions. Being aware of uncertainties and analysing how they originate constitutes the first step towards their acceptance and acknowledgement. We could, on the one hand, accept that not all States recognise sovereignty as a binding rule of international law in cyberspace. While on the other we should persistently underline that though territorial integrity might not be a perfect fit with the virtual dimension,\textsuperscript{164} political independence can be violated in cyberspace just as in other (physical) domains. Political independence is the short-term lever for acceptance of sovereignty in cyberspace as a customary rule of international law in the long run. After all, uncertainty will be reduced if States align their interpretations regarding sovereignty, or better yet, recognise sovereignty – based on political independence – as a primary rule of law in cyberspace.

Adherents of the interpretation that political independence is a binding notion in cyberspace can facilitate advocacy of that interpretation by speaking with one voice at international conferences including the OEWG – following the example of the Scandinavian block. The idea of aligning the legal interpretation of like-minded States can grow incrementally both in areas of law and in number of States.\textsuperscript{165}

Resilience can be defined as the capacity to recover or adapt.\textsuperscript{166} This ability is facilitated by redundancy: if one avenue is cut off, another should remain

\begin{thebibliography}{9}
\bibitem{163} Schmitt, \textit{supra} note 55 p. 41.
\bibitem{165} See also: F. Delerue, ‘Reinterpretation or Contestation of International Law in Cyberspace?’, \textit{52:3 Israel Law Review} (2019) pp. 310–312.
\end{thebibliography}
open. If a State is unable or reticent to invoke a breach of sovereignty due to the uncertainty surrounding this notion, other justifications for responses can be found in the force majeure and distress, but particularly in a plea of necessity.\textsuperscript{167} Necessity should not be invoked lightly and will only preclude wrongfulness if invoked to protect a State’s essential “interest against a grave and imminent peril” without violating the rules or interests of other States. However, if sovereignty is not accepted as a binding legal norm, the threshold for a plea of necessity is lowered while at the same time the sovereignty of other States is not violated. Redundancy in legal avenues partially takes away the asymmetry.

The legal asymmetry will obviously vanish once all States lower their norms, which is an untenable slippery slope for rule-of-law States. Legal asymmetry can, however, also be addressed using non-legal instruments. If sovereignty (or any other notion of international law) is breached in cyberspace, and wrongfulness cannot be invoked since the target State does not recognise sovereignty as a binding legal rule, the victim State can counter the act with measures that are informational (narratives, propaganda), economic (sanctions) or diplomatic (démarche), comparable to the EU’s nascent Diplomatic Cyber Toolbox – all unfriendly but lawful measures to take.

7 Conclusions and Reflections

The objective of this article was to explore how legal uncertainty in cyberspace arises, why it leads to legal asymmetry, and how to tackle it.

While it is generally accepted that international law applies to cyberspace,\textsuperscript{168} “how” it applies is still subject to interpretation.\textsuperscript{169} The expectation was that an increase in legal opinions and State practice would provide clarity.\textsuperscript{170} Paradoxically, with the increase in legal opinions the differences have grown, intensifying rather than lessening uncertainty. The effect of the diverging interpretations of legal norms is that some are reluctant to respond to possible

\textsuperscript{170} Moynihan, supra note 55 p. 61.
internationally wrongful acts, while others see opportunities to exploit the ambiguity, creating legal asymmetry.

The main reasons for uncertainty can be summarised as follows. On sovereignty: some States refrain from sharing their *opinio iuris* altogether, while those that do are not aligned on whether sovereignty is a binding rule *and* a principle in cyberspace or solely a principle. Moreover, in their *opinio iuris*, many States regurgitate standards of international law without articulating how to apply them to cyberspace, and those that are outspoken differ in how to apply sovereignty as a rule in cyberspace. This is understandable as territorial integrity is difficult to apply to activities in the virtual dimension, especially related to remotely executed digital influence operations. Political independence, however, can be breached in cyberspace, which forms a basis for the existence of sovereignty in cyberspace; but still the notions of interference and State functions also lack clarity. On non-intervention: though non-intervention is an accepted rule in cyberspace, it is not without ambiguity. The virtual dimension has made the reserved domain of the State more intangible, and coercion is ill-defined in legal terms. Furthermore, international law is struggling to apply these standards to non-State (cyber) actors. Lastly, the covert and elusive methods employed by malign actors make it difficult to grasp the purpose and intent of their actions.

The effects of legal uncertainty can be mitigated by awareness and analysing how and why they emerge, but also by acceptance of the current state of (legal) affairs. From there pre-aligned block of like-minded nations could advocate those rules that are applicable in cyberspace (such as political independence) and build from there, expanding in legal rules and States involved. Creating resilience in international law will also ease the asymmetry. The plea of necessity which could serve as a redundancy in case sovereignty is too ambiguous as a legally binding rule of cyberspace. Finally, non-legal countermeasure can be taken if principles of international law are violated and States are reticent to invoke legal means.

All in all, given the current geopolitical turmoil, it is better to find satisfactory grassroot fixes than perfect but unrealistic universal solutions.