TERRITORIAL SOVEREIGNTY IN CYBERSPACE AFTER TALLINN MANUAL 2.0

LUKE CHIRCOP*

Despite its status as a foundational principle of international law, territorial sovereignty has become contested and controversial in its application to cyberspace. Opportunistic states have exploited this circumstance by carrying out harmful cyber operations on the legal margins, with relative impunity, at the expense of peace and stability in the international system. The Tallinn Manual 2.0 sought to provide some needed clarity to this important legal doctrine. The manual’s International Group of Experts unanimously agreed that territorial sovereignty could be violated by cyber operations that caused the permanent loss of functionality to cyber infrastructure or that resulted in physical damage or injury. However, no agreement was reached as to when, if ever, cyber operations below this gravity threshold violated international law. In this context, this article provides a detailed account of when low-intensity or ‘below the threshold’ cyber operations violate territorial sovereignty. Specifically, it argues that state-sponsored cyber operations that interfere with a target state’s data, cyber systems or cyber infrastructure should be viewed as a violation of territorial sovereignty provided that more than de minimis effects are caused.

CONTENTS

I Introduction ................................................. 1
II The Development of Territorial Sovereignty in Cyberspace........................................ 3
   A The Principle of Territorial Sovereignty ........................................ 3
   B Tallinn Manual 2.0 ........................................ 5
   C Controversies on Sovereignty in Cyberspace .................................. 6
III Defining Territorial Interference ........................................ 9
IV Rationale for the Strict Inviolability Approach ........................................ 16
   A The Importance and Ubiquity of Data ........................................ 16
   B Providing Clarity in the International Law of Cyberspace ...................... 18
V Legal Status of the Strict Inviolability Approach ........................................ 19
   A Territorial Sovereignty in Physical Space ..................................... 21
   B Territorial Sovereignty in Cyberspace ......................................... 23
VI Conclusion .................................................... 28

I INTRODUCTION

The status of territorial sovereignty in cyberspace has challenged states and scholars for more than two decades.1 In that time, substantial progress has been made towards achieving consensus and granularity in the application of

---

* BA, JD (Melbourne). Research Associate, Program on the Regulation of Emerging Military Technologies. The author would like to thank Rain Liivoja for his feedback on an early iteration of this article. All views are the author’s own.

international law to cyber activities. This progress has primarily been facilitated at the state level by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (‘GGE on Cyber Security’), and at the academic level by the *Tallinn Manual* project of the North Atlantic Treaty Organization (‘NATO’) Cooperative Cyber Defence Centre of Excellence. Yet, despite this progress there are some legal areas that, owing to the ‘mystifying characteristics’ of cyberspace, remain unsettled.

Foremost among these is uncertainty as to when low-intensity cyber operations violate territorial sovereignty. This uncertainty is undesirable because it inhibits the ability of international law to ambitiously shape the behaviour and standards of states in the international system. Indeed, ambiguity as to the operation of territorial sovereignty in cyberspace has been exploited by opportunist states, who have been able to carry out harmful cyber operations on the legal margins with relative impunity. As such, if international law is a common global language, it has not yet found its voice in relation to this important area.

This article provides a detailed account of territorial sovereignty and the application of this principle to cyber operations. Specifically, it contends that all cyber operations that interfere with a target state’s cyberspace should violate (at least) territorial sovereignty, provided that more than de minimis effects are caused. This will usually include cyber operations that involve the insertion, alteration and deletion of data in targeted cyber systems. Part II discusses key controversies concerning territorial sovereignty in cyberspace, as well as the treatment of this doctrine in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (‘Tallinn Manual 2.0’). Part III provides an analytical framework for assessing cyber operations along an interference

---


8 Schmitt (ed), *Tallinn Manual 2.0* (n 3).
spectrum and sets out competing theoretical approaches to territorial sovereignty in cyberspace. Finally, Part IV and Part V endorse a strict inviolability approach to territorial sovereignty and assess this approach by reference to relevant state practice and *opinio juris*. For all relevant purposes, this article confines its analysis to cyber operations that can be attributed to one or more responsible states with a high degree of certainty under the law of state responsibility.

II THE DEVELOPMENT OF TERRITORIAL SOVEREIGNTY IN CYBERSPACE

A The Principle of Territorial Sovereignty

State sovereignty is the ‘basic constitutional doctrine of the law of nations’, but it is a contested and constantly evolving concept, but fundamentally refers to the legal competency of states, manifesting as corresponding rights and duties. In relation to its content, sovereignty has both an internal and external dimension. Internal sovereignty is the supreme authority of a state to regulate the people and things within its territory, while external sovereignty is the power of a state to act in relation to other equally sovereign states on the international plane.

Sovereignty has a clear textual foundation. Article 2(1) of the *Charter of the United Nations* provides that the United Nations ‘is based on the principle of the sovereign equality of all its Members’. Moreover, the *Friendly Relations Declaration*, adopted by the United Nations General Assembly in 1970, confirms that ‘[e]ach State enjoys the rights inherent in full sovereignty’. International courts and tribunals have also affirmed the eminent status of sovereignty among international law doctrines. In *Corfu Channel (United Kingdom v Albania)* (*Corfu Channel*), the International Court of Justice (*ICJ*) stated that ‘[b]etween...
independent States, respect for territorial sovereignty is an essential foundation'. Similarly, in *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* ('Military and Paramilitary Activities'), the ICJ recognised and applied ‘the principle of respect for State sovereignty’, which ‘extends to the internal waters and territorial sea of every State and to the air space above its territory’.

Territorial sovereignty refers to the sovereign rights and duties exercised by states in relation to their territory. It is a fundamental aspect of the broader notion of sovereignty because the legal competency of states depends on and assumes a ‘stable, physically identified (and normally legally delimited) base’. Indeed, ‘[a] state without a territory is not possible’. In *Island of Palmas (Netherlands v United States of America)*, Max Huber explained that territorial sovereignty is independence, which ‘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’.

The exclusivity of territorial sovereignty was also emphasised by the Permanent Court of International Justice in the *SS ‘Lotus’ (France v Turkey)* ('*Lotus*') case: ‘the first and foremost restriction imposed by international law upon a State is that … it may not exercise its power in any form in the territory of another State’. Territorial sovereignty implies the rights of a state: to exercise and enforce its jurisdiction; to ‘control the access to and egress from its territory’; and (most importantly for present purposes) to have its territory protected against interference by other states.

For completeness, territorial sovereignty should be distinguished from those aspects of sovereignty which are not territorial. For instance, while states have a sovereign right to exercise certain inherently governmental functions, such as the conduct of diplomatic activities, those functions do not necessarily have a connection to territory. Territorial sovereignty should also be distinguished from territorial integrity. While these concepts are related, in traditional legal sources the protection of a state’s territorial integrity is more closely aligned with the prohibition on the use of force. Accordingly, proscriptions against violating territorial integrity contemplate a particularly high threshold of harm that is not appropriate in the context of territorial sovereignty.

---

15 *Corfu Channel (United Kingdom v Albania) (Judgment)* [1949] ICJ Rep 4, 35 (‘*Corfu Channel*’). See also *Island of Palmas (Netherlands v United States of America) (Award)* (1928) 2 RIAA 829, 838 (‘*Island of Palmas*’).
17 *Island of Palmas* (n 15) 838.
20 *Island of Palmas* (n 15) 838.
21 *SS ‘Lotus’ (France v Turkey) (Judgment)* [1927] PCIJ (ser A) No 10, 18.
23 Schmitt (ed), *Tallinn Manual 2.0* (n 3) 21–3 (Rule 4 Commentary [15]–[20]).
24 *Charter of the United Nations* art 2(4); *Friendly Relations Declaration*, UN Doc A/RES/2625(XXV) (n 14) art 1.
B Tallinn Manual 2.0

The Tallinn Manual 2.0 is an operational manual on the international law governing cyber warfare and peacetime cyber operations. It was prepared by an International Group of Experts (‘Experts’) constituted by lawyers, academics and technical specialists.\(^\text{25}\) While its drafting process included consultations with states and international organisations, the manual’s 154 rules were adopted by the Experts, on a consensus basis, acting in their personal capacity.\(^\text{26}\) The Tallinn Manual 2.0 claims to reflect customary international law as it existed in June 2016 — an ‘objective restatement of the lex lata’ — rather than being a best practices guide or an attempt at progressive development of the law.\(^\text{27}\) Its authority should not be overstated though. While it has become an influential text on international law and cyberspace,\(^\text{28}\) the Tallinn Manual 2.0 is not a binding instrument; it is an expression of the opinions of its Experts as to the state of the law at a point in time.\(^\text{29}\)

Rule 4 of the Tallinn Manual 2.0 provides that a state ‘must not conduct cyber operations that violate the sovereignty of another State’.\(^\text{30}\) In the commentary, the Experts expanded on the kinds of operations that they considered would fall foul of this rule. They agreed that cyber operations conducted from within a target state’s territory against that state (or entities or persons located within that state), violated its territorial sovereignty.\(^\text{31}\) Most also agreed that cyber operations conducted remotely (that is, from outside the target state’s territory) violated territorial sovereignty where they resulted in ‘physical damage or injury’,\(^\text{32}\) or caused cyber infrastructure to lose functionality ‘necessitating repair or replacement’.\(^\text{33}\) No consensus was reached as to when, if ever, remote cyber operations below this gravity threshold breached international law.\(^\text{34}\) Finally, the

\(^{25}\) Schmitt (ed), Tallinn Manual 2.0 (n 3) xii–xviii. For the avoidance of doubt, the Tallinn Manual 2.0’s International Group of Experts (‘Experts’) is distinct from the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (‘GGE on Cyber Security’).

\(^{26}\) Ibid 2.

\(^{27}\) Ibid 2–3.


\(^{30}\) Schmitt (ed), Tallinn Manual 2.0 (n 3) 17 (Rule 4).

\(^{31}\) Ibid 19 (Rule 4 Commentary [6]).

\(^{32}\) Ibid 20 (Rule 4 Commentary [11]).

\(^{33}\) Ibid 20–1 (Rule 4 Commentary [13]).

\(^{34}\) Ibid 21 (Rule 4 Commentary [14]).
Experts agreed that cyber operations violated sovereignty where they usurped the ‘inherently governmental functions of another State’. The phrase ‘inherently governmental functions’ was not defined with precision, but was said to overlap with the concept of domaine réservé and could otherwise be informed by the notion of acta jure imperii used in the context of state immunity.

This article seeks to provide greater granularity than is contained in the Tallinn Manual 2.0 to the principle of territorial sovereignty in cyberspace. In particular, it presents a detailed account of when, and why, low-intensity cyber operations — those which do not result in physical damage or injury, or cause cyber infrastructure to lose functionality — might violate a target state’s territorial sovereignty. The inability of the Experts to find agreement on this point confirms that it is an important and unresolved ‘grey zone’ in the international law of cyberspace.

C Controversies on Sovereignty in Cyberspace

There have been at least two central controversies concerning the nature and operation of sovereignty in cyberspace. The first controversy concerned whether state sovereignty applies to cyber activities at all. In 1996, John Barlow contended, in his Declaration of the Independence of Cyberspace, that because of its unique and ubiquitous nature, cyberspace could not be subject to sovereignty, or indeed other legal concepts, in any traditional sense. In the subsequent two decades, however, this view has been widely rejected by states and scholars alike. In two consecutive reports, the United Nations Group of Governmental Experts on Cyber Security (‘UN GGE’) confirmed that sovereignty and the international norms that flow from sovereignty apply to cyber activities. Similarly, the Tallinn Manual 2.0’s Experts unanimously agreed that existing international law applies to cyber operations. On this basis, Professor Sean Watts has observed that the ‘argument that cyberspace constitutes a law-free zone is no longer taken seriously’.

A second controversy, which has arisen more recently, concerns whether territorial sovereignty constitutes a primary rule of international law capable of independent breach, or whether it is instead a general Westphalian principle from

---

35 Ibid (Rule 4 Commentary [15]).
36 Ibid 24 (Rule 4 Commentary [22]).
37 Ibid 22 n 26. In addition, the following were given as examples of ‘inherently governmental functions’: the delivery of social services; the conduct of elections; the collection of taxes; the conduct of diplomatic activities; the conduct of national defence activities; official communications among a state’s leadership; the payment of government employee salaries; the exercise of law enforcement functions; and the protection of critical governmental data: at 22–3 (Rule 4 Commentary [16]–[19]).
38 Schmitt, ‘Grey Zones in the International Law of Cyberspace’ (n 7) 6. While the precise meaning of ‘inherently governmental functions’ also warrants further discussion, this article is principally concerned with the violation of sovereignty by territorial interference.
40 GGE Report 2013, UN Doc A/68/98* (n 2) 8 [19]–[20]; GGE Report 2015, UN Doc A/70/174 (n 2) 7 [11], [13].
41 Schmitt (ed), Tallinn Manual 2.0 (n 3) 11 (Rule 1). See also Schmitt (ed), Tallinn Manual 1.0 (n 3) 15 (Rule 1).
which primary rules of international law emanate. The ‘sovereignty as principle’ position has been propagated by Gary Corn, former Staff Judge Advocate to United States Cyber Command, and Robert Taylor, former Principal Deputy General Counsel to the United States Department of Defense. Corn and Taylor believe that 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’. In their view, until a more cogent body of state practice and opinio juris develops, cyber operations can only violate international law by amounting to a prohibited intervention or a use of force. This has been echoed by former United Kingdom Attorney-General Jeremy Wright, who also rejected ‘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’. Wright’s observations are particularly salient because, when made, they reflected the official position of the UK government, and therefore amounted to state practice.

Before addressing the merits of the ‘sovereignty as principle’ view, there are some conceptual assumptions within this debate in need of clarification. Importantly, it is not disputed that sovereignty is a foundational principle of international law, which gives rise to various primary rules including the prohibitions on intervention and the use of force. However, minds differ on whether, below the threshold of a prohibited intervention, cyber activities can violate a state’s territorial sovereignty. Territorial sovereignty can imply various different rights, but here, it refers specifically to a state’s right to have its territory free from interference by other states (and the corresponding duty not to interfere with the territory of other states). Moreover, proponents of the ‘sovereignty as rule’ position do not seek to establish a ‘cyber specific’ principle of international law.

---


44 Corn and Taylor (n 43) 208.

45 Ibid.


49 Corn and Taylor (n 43) 208–9; Corn (n 43); Jeremy Wright (n 46); Schmitt and Vihul, ‘Respect for Sovereignty in Cyberspace’ (n 43) 1642–3; Schmitt (ed), Tallinn Manual 2.0 (n 3) 11–12 (Rule 1 Commentary [1]–[3]).

50 See above Part II(A).
law, as Wright assumed.\textsuperscript{51} Instead, they consider that a state’s right to be free from territorial interference is one of the ‘international norms … that flow from sovereignty’, and that it applies in cyberspace as it does in physical space.\textsuperscript{52}

As to the merits, while it will no doubt remain contentious, the balance of authority currently favours the ‘sovereignty as rule’ position. The ICJ has enforced territorial sovereignty as a primary rule of international law on several occasions. In the \textit{Military and Paramilitary Activities} case, the Court acknowledged that territorial sovereignty was ‘closely linked with the principles of the prohibition of the use of force and of non-intervention’, but nonetheless applied each respective rule separately.\textsuperscript{53} Crucially, the Court found that some instances of less grave conduct (such as unauthorised aerial overflights) amounted to a standalone violation of territorial sovereignty.\textsuperscript{54} Likewise, in \textit{Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua)} (‘\textit{Certain Activities}’), the Court ordered Nicaragua to ‘make reparation for the damage caused by its unlawful activities’ on the basis of its finding that Nicaragua had violated Costa Rica’s territorial sovereignty.\textsuperscript{55} The Court did not consider separate submissions on the prohibition of the use of force because the finding of a territorial sovereignty violation was considered adequate to establish the ‘unlawful character’ of the impugned activities.\textsuperscript{56} While decisions of the ICJ are a ‘subsidiary means for the determination of rules of law’,\textsuperscript{57} in practice they are of highly persuasive force.\textsuperscript{58}

In addition, the \textit{Tallinn Manual 2.0}’s Experts unanimously endorsed the ‘sovereignty as rule’ position by adopting Rule 4 and its accompanying commentary.\textsuperscript{59} The \textit{Tallinn Manual 2.0} itself likely constitutes a subsidiary source of international law.\textsuperscript{60} Moreover, Professor Michael Schmitt and Liis Vihul (the Director and Managing Editor of \textit{Tallinn Manual 2.0}, respectively) have noted that opposition to the ‘sovereignty as rule’ position did not surface during the seven years of deliberations preceding the manual’s publication in 2017.\textsuperscript{61} These deliberations included unofficial consultations with over 50 states and international organisations.\textsuperscript{62} Schmitt and Vihul have defended the ‘sovereignty as rule’ position on the basis of an extensive body of supportive state practice and

\textsuperscript{51} Schmitt and Vihul, ‘Respect for Sovereignty in Cyberspace’ (n 43) 1647; Michael N Schmitt and Liis Vihul, ‘Sovereignty in Cyberspace: Lex Lata Vel Non?’ (2017) 111 AJIL Unbound 213, 214 (‘Sovereignty in Cyberspace’). Cf Jeremy Wright (n 46).

\textsuperscript{52} Schmitt and Vihul, ‘Respect for Sovereignty in Cyberspace’ (n 43) 1667; Schmitt and Vihul, ‘Sovereignty in Cyberspace’ (n 51) 214. See also below Part V(A).

\textsuperscript{53} \textit{Military and Paramilitary Activities} (n 16) 111 [212].

\textsuperscript{54} Ibid 128 [251].


\textsuperscript{56} Ibid 704 [97].

\textsuperscript{57} \textit{Statute of the International Court of Justice} arts 38(1)(d), 59.

\textsuperscript{58} \textit{Draft Conclusions}, UN Doc A/73/10 (n 48) 149–50 (Conclusion 13 Commentary [2]–[5]); Crawford (n 10) 37–9.

\textsuperscript{59} Schmitt (ed), \textit{Tallinn Manual 2.0} (n 3) 17–27 (Rule 4). In the commentary to Rule 4, the Experts refer to \textit{violations} of sovereignty (which is the language of state responsibility) and acknowledge that countermeasures may be used in response to sovereignty violations: at 18. They also expressly distinguish between sovereignty violations and violations of the non-intervention principle and the prohibition of the use of force: at 20, 22, 24, 26.

\textsuperscript{60} \textit{Statute of the International Court of Justice} art 38(1)(d).

\textsuperscript{61} Schmitt, ‘Grey Zones in the International Law of Cyberspace’ (n 7) 4–5.

\textsuperscript{62} Schmitt (ed), \textit{Tallinn Manual 2.0} (n 3) 6.
opinio juris, including state responses to unwelcome aerial and marine incursions, drone operations, counterterrorism activity and the public comments of state officials.\textsuperscript{63} Moreover, preliminary research conducted under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence concluded that the ‘sovereignty as rule’ position was adopted ‘more often than not’ by states in their national cyber security documents.\textsuperscript{64} Thus, this article proceeds on the assumptions that sovereignty does prima facie apply to cyberspace, and that territorial sovereignty constitutes a primary rule of international law capable of being breached.

III DEFINING TERRITORIAL INTERFERENCE

A state-sponsored cyber operation will violate the territorial sovereignty of a target state when it interferes with that state’s territory to a requisite degree. However, the degree of interference at which a sovereignty violation occurs is disputed, as is the method by which territorial interference should be measured in cyberspace. As such, to inform the subsequent discussion of these matters from a practical perspective, below is a proposed Scale Chart which classifies cyber operations along a spectrum from the least to the most grave examples of interference by cyber means:\textsuperscript{65}

\begin{itemize}
\item \textsuperscript{63} Schmitt and Vihul, ‘Respect for Sovereignty in Cyberspace’ (n 43) 1655–65.
\end{itemize}
<table>
<thead>
<tr>
<th>Scale Number</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Surveilling or</td>
<td>These are cyber espionage operations in which data stored on or transiting through targeted cyber infrastructure is surveilled remotely. This includes cyber operations that result in the copying or exfiltration of data to a remote cyber system for storage or review.</td>
</tr>
<tr>
<td></td>
<td>exfiltrating data</td>
<td>Examples: In 2010, Chinese hackers infiltrated the servers of Google in the United States and exfiltrated data in an attempt to access the email accounts of Chinese human rights activists. Further examples of Scale 1 cyber operations discussed in this article include the Office of Personnel Management hack of 2015, and the Democratic National Committee hack of 2016.</td>
</tr>
<tr>
<td>2</td>
<td>Inserting data</td>
<td>These are cyber operations in which data, sometimes containing false or 'bogus' information, is temporarily or permanently placed onto targeted cyber systems.</td>
</tr>
<tr>
<td>3</td>
<td>Manipulating data</td>
<td>These are cyber operations in which the data stored on targeted cyber systems is temporarily or permanently manipulated (but not deleted).</td>
</tr>
<tr>
<td>4</td>
<td>Deleting data</td>
<td>These are cyber operations in which the data stored on targeted cyber systems is corrupted, so that it cannot be used, or is deleted altogether.</td>
</tr>
</tbody>
</table>

---


<table>
<thead>
<tr>
<th>Scale Number</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Causing temporary loss of functionality</td>
<td>These are cyber operations that cause a temporary loss of functionality to the targeted cyber infrastructure. Common examples of this kind of operation include distributed denial-of-service (‘DDoS’) attacks and ransomware attacks.</td>
<td></td>
</tr>
<tr>
<td>6 Causing permanent loss of functionality</td>
<td>These are cyber operations that cause the permanent loss of functionality of targeted cyber infrastructure in a way that necessitates the repair or replacement of physical components.</td>
<td></td>
</tr>
</tbody>
</table>

Examples:
- In 2007, Estonia was targeted by a DDoS attack that prevented public access to online government, banking and news services for up to a month.69 Similar DDoS attacks were conducted against Georgia in 200870 and Kyrgyzstan in 2009.71 Further examples of Scale 5 cyber operations discussed in this article include the NotPetya and Bad Rabbit ransomware attacks of 2017.72
- In August 2012, the Shamoon virus infected Saudi Aramco’s computers, deleting substantial quantities of its data and necessitating the repair of thousands of its hard drives.73 A further example of a Scale 6 cyber operation discussed in this article is the Sony hack of 2014.74

---


70 Watts, ‘Low-Intensity Computer Network Attack and Self-Defense’ (n 69) 70–2; Franzese (n 69) 4–5.

71 Franzese (n 69) 4–5.


<table>
<thead>
<tr>
<th>Scale Number</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Causing physical damage or injury</td>
<td>These are cyber operations that cause physical damage to targeted cyber infrastructure (or to other physical components which rely on the targeted infrastructure to operate) or cause physical injury to people. Example: In 2010, the US and Israel allegedly deployed the Stuxnet virus against the Supervisory Control and Data Acquisition system of the Natanz uranium enrichment plant in Iran. The malware was reported to have changed the rotor speeds of gas centrifuges at the facility, causing vibrations and distortions that ultimately damaged the centrifuges.75</td>
</tr>
</tbody>
</table>

Of course, this Scale Chart is not exhaustive of the countless types of cyber operations states are capable of conducting. Fine technical distinctions may be drawn between cyber operations that have been grouped together for analytical convenience. Further, there may be instances where cyber operations with a low classification on the Scale Chart nonetheless constitute a violation of international law, or otherwise have serious political, social or economic consequences. This is particularly the case for cyber espionage operations (Scale 1), which may only involve a modest degree of territorial interference, but which can undermine the confidentiality of highly sensitive commercial or governmental information. Finally, certain levels of the Scale Chart are not mutually exclusive. To illustrate, a cyber operation involving the manipulation of data (Scale 2) may cause the temporary loss of functionality to targeted cyber infrastructure (Scale 5). As such, for the avoidance of doubt, cyber operations involving the insertion, manipulation and deletion of data should only be classified from Scale 2 to 4 in so far as they do not cause the more serious effects contemplated at Scale 5 to 7. These observations notwithstanding, the Scale Chart is a useful tool for evaluating competing formulations of the degree of interference required for a cyber operation to violate territorial sovereignty.

There are four prevailing approaches to territorial sovereignty in cyberspace that will be canvassed with reference to the Scale Chart. The first approach, referred to here as the ‘material damage approach’, provides that only cyber operations that cause a permanent loss of functionality to cyber infrastructure (Scale 6), or that result in physical damage or injury (Scale 7), are to be considered violations of territorial sovereignty. The material damage approach has been endorsed by various scholars, who have described this interference threshold using different but synonymous terms: ‘physical damage or hardware malfunction’,76 ‘material damage’,77 and ‘actual physical damage’.78 Broadly, these scholars observe that there is no clear consensus on whether, and if so when, cyber

---

75 Roscini (n 73) 243. See also Brown and Poellet (n 66) 131–2; Messerschmidt (n 66) 288–9.
76 Kozik (n 11) 98.
78 Pirker (n 9) 201.
operations below this threshold will violate territorial sovereignty.\textsuperscript{79} For proponents of the material damage approach, only state practice and \textit{opinio juris} over the course of time are capable of lowering the bar for territorial sovereignty violations in cyberspace.\textsuperscript{80} While this approach is not without merit, it represents a particularly conservative view of the application of international law to cyberspace. At best, it fails to account for the substantial harm that can be caused to states by cyber operations below the Scale 6 threshold.\textsuperscript{81} At worst, it is doctrinally inconsistent with the operation of territorial sovereignty in relation to land, sea and airspace interference.\textsuperscript{82}

Secondly, a number of different ‘intermediate approaches’ have been formulated pursuant to which moderately severe cyber operations are capable of violating territorial sovereignty. Some of these were identified by the \textit{Tallinn Manual 2.0}'s Experts, including: cyber operations ‘causing cyber infrastructure or programs to operate differently’,\textsuperscript{83} ‘emplacing malware into a cyber system’ (Scale 2);\textsuperscript{84} ‘altering or deleting data stored on cyber infrastructure without causing physical or functional consequences’ (Scales 3 and 4);\textsuperscript{85} ‘installing backdoors’ (Scale 2);\textsuperscript{86} and ‘causing a temporary, but significant, loss of functionality’ (Scale 5).\textsuperscript{87} The Experts who endorsed each of these formulations did so on the basis that they were considered to be ‘consistent with the object and purpose of the principle of sovereignty that affords States the full control over access to and activities on their territory’.\textsuperscript{88} However, none of these intermediate formulations have been subsequently expanded upon or affirmed by states or scholars. Further, it is not immediately apparent that these particular standards can be justified on a principled basis. For instance, it is unclear why a state’s territory would be infringed by the emplacement of malware on its cyber infrastructure, but not the emplacement of other kinds of data on the same infrastructure. Likewise, if the touchstone of wrongfulness is causing targeted cyber infrastructure to operate differently, operations which have dormant or covert effects (even if

\textsuperscript{79} Schmitt (ed), \textit{Tallinn Manual 2.0} (n 3) 21 (Rule 4 Commentary [14]); Pirker (n 9) 201; von Heinegg, ‘Legal Implications of Territorial Sovereignty in Cyberspace’ (n 22) 11.


\textsuperscript{82} For further explanation on this point, see below Part V(A).

\textsuperscript{83} This standard is not directly referable to the Scale Chart, as the touchstone of wrongfulness is effects-based, not any particular degree of cyber interference. Schmitt (ed), \textit{Tallinn Manual 2.0} (n 3) 21 (Rule 4 Commentary [14]).

\textsuperscript{84} While this is most analogous to a Scale 2 cyber operation, it is a marginally narrower standard in that it does not capture data other than ‘malware’. The \textit{Tallinn Manual 2.0} defines ‘malware’ as ‘“Software” … that may be stored and executed in other software, firmware, or hardware that is designed adversely to affect the performance of a computer system. Examples of malware include Trojan horses, “rootkits”, “viruses” and “worms”’: ibid 566.

\textsuperscript{85} Ibid (Rule 4 Commentary [14]).

\textsuperscript{86} Ibid. While this is most analogous to a Scale 2 cyber operation, it is a narrower standard in that it only captures data insertions which create a backdoor in the targeted cyber infrastructure.

\textsuperscript{87} Ibid.

\textsuperscript{88} Ibid.
substantial over a period of time) would be unjustifiably excluded.\textsuperscript{89} Perhaps the most sensible intermediate approach is that which captures cyber operations causing temporary but significant losses of functionality. But again, this lacks a clear doctrinal justification. General or sweeping reliance on the ‘the object and purpose of the principle of sovereignty’\textsuperscript{90} in support of these formulations is unhelpful. The term ‘sovereignty’, without further specification, ‘is susceptible to multiple meanings and justifications’, and ‘is rather descriptive in character, referring in a “catch-all” sense to the collection of rights held by a state’.\textsuperscript{91}

The third approach, referred to here as the ‘strict inviolability approach’, provides that all cyber operations that interfere with a target state’s cyber infrastructure violate territorial sovereignty, as long as they cause more than de minimis effects.\textsuperscript{92} This approach involves a two-stage inquiry. At the first stage, a territorial sovereignty violation is premised on evidence of a prima facie interference. While this is a relatively low threshold, it is not exceeded by mere cyber espionage operations (Scale 1), which do not typically result in any change to the targeted data or cyber infrastructure. This is consistent with the weight of authority, which currently favours the view that cyber espionage is not per se prohibited under international law.\textsuperscript{93} All other cyber operations contemplated on the Scale Chart (Scale 2 to 7) exceed the prima facie interference threshold, as they each have a definite and measurable impact on data or infrastructure. For example, in the case of a Scale 2 cyber operation, evidence of interference is satisfied by the presence of data on a cyber system that previously did not exist. At the second stage of inquiry, a territorial sovereignty violation requires the causing of more than de minimis effects. The principle of \textit{de minimis non curat lex} provides that international law does not concern itself with trifles.\textsuperscript{94} On this basis, certain harms are considered to be so minor, variable or intangible, that they ‘must be accepted


\textsuperscript{90} Schmitt (ed), \textit{Tallinn Manual 2.0} (n 3) 21 (Rule 4 Commentary [14]).

\textsuperscript{91} Crawford (n 10) 448.

\textsuperscript{92} von Heinegg, ‘Legal Implications of Territorial Sovereignty in Cyberspace’ (n 22) 11. See also Pirker (n 9) 201.


as the price of living in society’. While ‘harm’ is a difficult concept to define in the cyber context, it is not limited to the causing of physical consequences. Instead, under the strict inviolability approach, ‘harm’ includes the degradation of a target state’s data or cyber infrastructure without its consent. Thus, without being exhaustive, cyber operations may have more than de minimis effects when they: create a cyber vulnerability which can later be exploited; limit the accessibility of data; cause data, a network or cyber infrastructure to lose functionality or function in a manner that was not intended; or cause physical damage or injury. In contrast, cyber operations that have no material or practical adverse consequence on the targeted cyber system or infrastructure (even if they involve the insertion, manipulation or deletion of data) likely would not exceed the de minimis effects threshold. As states exercise sovereignty over all of their territory equally, it is inconsequential whether the cyber infrastructure targeted in a given case is personal, private or governmental.

This article endorses the strict inviolability approach and, in Parts IV and V, sets out the normative and legal basis on which it may emerge as a norm of customary international law.

The fourth (and final) approach, worth briefly acknowledging, provides that all intrusions into another state’s cyber infrastructure, including cyber espionage operations, amount to a violation of territorial sovereignty. This position has been defended on the basis that ‘States exert sovereignty over information in cyberspace which belongs to entities and individuals over which they exercise jurisdiction’. Interestingly though, while it has been described by one of its proponents as a ‘majority view’, it was not identified as such, or expanded upon in any meaningful way, in the Tallinn Manual 2.0. Further, it is contrary to the balance of state practice and opinio juris arising from cyber operations that have involved the exfiltration of data. For instance, between 2010 and 2013, a Chinese government-sponsored hacker group called APT1 (Unit 61398)...

96 See below Part IV(A).
97 von Heinegg, ‘Legal Implications of Territorial Sovereignty in Cyberspace’ (n 22) 12, quoted in Buchan, ‘Cyber Espionage and International Law’ (n 94) 186 n 90. See also Schmitt and Vihul, ‘Respect for Sovereignty in Cyberspace’ (n 43) 1647; Schmitt (ed), Tallinn Manual 2.0 (n 3) 13–14 (Rule 2 Commentary [3]).
99 Buchan, ‘Cyber Espionage and International Law’ (n 94) 184.
100 Watts, ‘International Law and Proposed US Responses to the DNC Hack’ (n 98).
101 Schmitt (ed), Tallinn Manual 2.0 (n 3) 169 (Rule 32 Commentary [5]). An isolated but commonly cited counter-example is a statement given by the President of Brazil to the UN General Assembly following public reporting of the US global cyber espionage program in 2013: at 169 n 384; HE Dilma Rousseff, President of the Federal Republic of Brazil, ‘Opening of the General Debate of the 68th Session of the United Nation’s General Assembly’ (Speech, United Nations General Assembly, 24 September 2013). See also Buchan, ‘Cyber Espionage and International Law’ (n 94) 179–80.
conducted numerous cyber espionage operations against US corporations.\textsuperscript{102} Rather than treating these as violations of international law, the US responded by having recourse to its domestic criminal jurisdiction, indicting five Chinese hackers thought to be responsible for the operations.\textsuperscript{103} Similarly, in 2015, the US refrained from characterising the Office of Personnel Management hack, which resulted in the theft of the personal information of more than 20 million government employees, as a violation of international law.\textsuperscript{104}

IV RATIONALE FOR THE STRICT INVOLIABILITY APPROACH

A The Importance and Ubiquity of Data

The principal rationale for adopting the strict inviolability approach is that it appropriately recognises the importance and ubiquity of data in modern society. Data is necessary for the effective functioning of critical systems, including those that support government services, national security, defence, financial markets, commercial transactions, energy grids, water supply, public health and transport.\textsuperscript{105} Interference with data has the capacity to degrade and impair each of these systems. Data is also a valuable commodity at an individual level. People reasonably expect a legal (intellectual property) right to the integrity of their unique self-generated data, and expect privacy to attach to the data that captures their sensitive personal information.\textsuperscript{106} These interests and expectations are clearly undermined when data is destroyed, degraded or deprived of being the genuine


\textsuperscript{103} Nakashima and Wan (n 102); ‘DOJ Summary of Indictment against Chinese Military Hackers’ (n 102).


\textsuperscript{106} McCormack, ‘International Humanitarian Law and the Targeting of Data’ (n 105) 223.
source of information it otherwise would have been.\textsuperscript{107} On this basis, Professor Tim McCormack has observed that in a digitally connected world ‘data is more than a complex succession of 1s and 0s’.\textsuperscript{108} The strict inviolability approach acknowledges the importance of data in modern society by positing that states exercise territorial sovereignty over the data emanating from the cyber infrastructure on their territory, and that consequently, a state’s data is protected from external interference under international law.

The application of territorial sovereignty to cyberspace has most commonly been explained by reference to the domain’s physical features. That is, cyberspace needs a physical architecture to exist, which includes servers, computers, cables and other components.\textsuperscript{109} This physical architecture is located on the sovereign territory of states, and is owned by governments, corporations and individuals. As such, by extension of the control states exercise over their territory, they also exercise control (in the form of territorial sovereignty) over cyber infrastructure located on their territory.\textsuperscript{110} There is thus wide agreement that state-sponsored cyber operations that cause physical damage to another state’s cyber infrastructure amount to, at least, a violation of the latter state’s territorial sovereignty.\textsuperscript{111} But physicality is clearly not the only basis on which sovereignty applies to cyberspace.\textsuperscript{112} For instance, states exercise territorial sovereignty over the individuals engaged in cyber activities on their territory,\textsuperscript{113} and can accordingly prohibit cybercrime under their domestic laws.\textsuperscript{114} The critical next step is to recognise that states also exercise territorial sovereignty over data emanating from their cyber infrastructure. The basis of a state’s claim to territorial sovereignty over data remains physical, in that it is limited to data that emanates from infrastructure located on its territory. As a state’s sovereign rights and duties in respect of data are independent and complete, territorial sovereignty can be violated by interference with data alone, even when the interference does not have ancillary effects on the underlying physical infrastructure.\textsuperscript{115} That states exercise territorial sovereignty over data was seemingly accepted, but not explained, in the Tallinn Manual 2.0. The manual’s Experts agreed that cyberspace has a ‘logical layer’,

\begin{itemize}
\item \textsuperscript{107} Haataja (n 105) 180, citing Massimo Durante, ‘Violence, Just Cyber War and Information’ (2015) 28(3) Philosophy and Technology 369, 382–3.
\item \textsuperscript{108} McCormack, ‘International Humanitarian Law and the Targeting of Data’ (n 105) 223.
\item \textsuperscript{109} von Heinegg, ‘Legal Implications of Territorial Sovereignty in Cyberspace’ (n 22) 9; Franzese (n 69) 33; Jensen (n 80) 296.
\item \textsuperscript{110} Schmitt (ed), Tallinn Manual 2.0 (n 3) 11 (Rule 1 Commentary [1]); von Heinegg, ‘Legal Implications of Territorial Sovereignty in Cyberspace’ (n 22) 9–10; Jupillat (n 6) 944; GGE Report 2013, UN Doc A/68/98* (n 2) 8 [20]; GGE Report 2015, UN Doc A/70/174 (n 2) 12 [28(a)].
\item \textsuperscript{111} Schmitt (ed), Tallinn Manual 2.0 (n 3) 20 (Rule 4 Commentary [11]); Kozik (n 11) 98; Osula (n 77) 726; Pirker (n 9) 200–1; von Heinegg, ‘Legal Implications of Territorial Sovereignty in Cyberspace’ (n 22) 11.
\item \textsuperscript{112} Jupillat (n 6) 944; Schmitt (ed), Tallinn Manual 2.0 (n 3) 11 (Rule 1 Commentary [1]).
\item \textsuperscript{113} Schmitt (ed), Tallinn Manual 2.0 (n 3) 11–12 (Rule 1 Commentary [1], [4]).
\item \textsuperscript{115} See Buchan, Cyber Espionage and International Law (n 93) 54.
\end{itemize}
consisting of ‘applications, data, and protocols that allow the exchange of data’ across physical infrastructure, and agreed that sovereignty applies to this logical layer. However, no view was reached as to the circumstances in which data interference would constitute a sovereignty violation.

One limitation of the strict inviolability approach, worth noting here, is that a state’s data will not always emanate from cyber infrastructure located on its territory. Global technology companies like Amazon, Microsoft and Google store customer data on cloud systems, which make use of ‘server farms’ in many different countries around the world. Moreover, since June 2017, Estonia has stored some of its critical governmental data in a ‘data embassy’ hosted by servers in Luxembourg. This practice could result in competing claims to sovereignty in a case where, for instance, the data of state A was interfered with, but that data emanated from physical infrastructure located on the territory of state B. In such a case, it would be difficult for state A to sustain a claim to territorial sovereignty over the affected data. But state A may nonetheless be able to assert a violation of its sovereignty if the interference usurped one of its inherently governmental functions, or amounted to a prohibited intervention in its internal affairs. Separately, state B may be able to assert a violation of its territorial sovereignty on the basis that the interference affected data emanating from cyber infrastructure located on its territory. These issues will require further examination as companies and states continue to make use of cloud-based systems for the storage of important personal and governmental information.

B Providing Clarity in the International Law of Cyberspace

A subsidiary rationale for adopting the strict inviolability approach is that it provides granularity to the operation of territorial sovereignty in the case of low-intensity cyber operations. Low-intensity cyber operations ‘present a far more likely picture of future State cyber interactions’ than violent or destructive ones. States engage in this kind of cyber activity because it is an inexpensive and potentially anonymous way of degrading adversaries during conflict or peacetime. The application of international law to cyberspace remains particularly unsettled in respect of low-intensity cyber operations, which has allowed opportunistic states to engage in harmful cyber conduct while making it difficult for target states to lawfully respond. The strict inviolability approach

---

116 Schmitt (ed), Tallinn Manual 2.0 (n 3) 12 (Rule 1 Commentary [4]).
120 See also Schmitt, ‘Below the Threshold’ (n 5) 698–9.
121 Watts, ‘Low-Intensity Cyber Operations and the Principle of Non-Intervention’ (n 42) 138.
122 Schmitt, ‘Grey Zones in the International Law of Cyberspace’ (n 7) 2–3.
has the potential to ameliorate this circumstance by providing a clear (and protective) framework for the application of territorial sovereignty to cyber operations at the lower end of the gravity spectrum.

This rationale is not immune from normative criticism, though. Some states might resist the relatively low gravity threshold of this formulation because it represents an expansion of the scope for potential state responsibility in cyberspace.\textsuperscript{123} It might also be contended that a strict inviolability approach could have a destabilising effect on the international system by making countermeasures more readily available to target states, including as a means of response to low-intensity cyber operations.\textsuperscript{124} These concerns are legitimate, but they are not insurmountable. Overall, greater clarity in the international law of cyberspace should promote, rather than undermine, peace and stability in the relations between states.\textsuperscript{125} That is because states would be deterred from carrying out hostile cyber operations if they could face equivalent (and lawful) countermeasures in response. Further, the risk of conflict escalation as a result of over-reliance on the countermeasures regime is mitigated by the evidential certainty and strict procedural requirements that must be satisfied before countermeasures can be properly invoked.\textsuperscript{126} In this way, assuming international law sets a behavioural benchmark for states in the international system, a stricter view of territorial sovereignty in cyberspace should ultimately have a prophylactic effect on the harmful conduct of aggressor states.\textsuperscript{127}

V LEGAL STATUS OF THE STRICT INVIOLABILTY APPROACH

The strict inviolability approach to territorial sovereignty in cyberspace would constitute customary international law if it was consistent with generally uniform state practice and \textit{opinio juris}.\textsuperscript{128} However, evidence of the existence of customary law is famously difficult to distil in cyberspace, in part, because of the significant challenges associated with attribution in this domain.\textsuperscript{129} The attribution of cyber conduct to a responsible state is a necessary prerequisite to concluding that

\begin{enumerate}
\item See, eg, Schmitt, ‘Grey Zones in the International Law of Cyberspace’ (n 7) 20.
\item See, eg, Crook (ed) (n 6) 247; Jupillat (n 6) 939.
\item \textit{Statute of the International Court of Justice} art 38(1)(b); \textit{North Sea Continental Shelf (Federal Republic of Germany v Denmark) (Merits)} [1969] ICJ Rep 3, 43 [74] (‘North Sea Continental Shelf’); \textit{Military and Paramilitary Activities} (n 16) 97–8 [184]–[186].
\item See above n 9.
\end{enumerate}
international law has been violated under the state responsibility framework, and when attribution is not possible, target states have generally refrained from publicly commenting on whether a particular cyber operation might have otherwise violated territorial sovereignty. Even when attribution can be made out with a high degree of certainty, target states have often refused to comment on, or respond to, hostile cyber operations for diplomatic or strategic reasons. Indeed, it has been observed that many states are ‘inclined to take a “wait and see” approach toward the manner in which cyberspace ought to be regulated, maintaining, in effect, a policy of silence and ambiguity’. Against this background, the strict inviolability approach cannot yet sensibly be described as a crystallised rule of customary international law.

In the remainder of this article, it is shown that the strongest argument in favour of the strict inviolability approach is that an equivalent standard of territorial sovereignty has long been accepted by states in respect of physical space, and that the content of the principle should not differ across the physical and cyber domains. On the other hand, states have been acting in cyberspace and officially commenting on cyber conduct for more than a decade, and the resulting body of practice cannot be ignored. As will be seen, state practice and opinio juris in respect of cyberspace is broadly consistent with the strict inviolability approach, but the outer limits of territorial sovereignty in this domain remain untested or controversial in a few important respects. Therefore, this article contends that the strict inviolability approach provides a principled account of an unresolved legal area, and constitutes lex ferenda, or an emerging view of customary international law.


133 Efrony and Shany (n 5) 584.

134 See below Part V(A).

135 While the earliest publicly recorded state-sponsored cyber operation arguably occurred in 1982, when a trans-Siberian pipeline explosion was allegedly caused by US computer malware, the majority of states have been meaningfully engaged in international law discourse in respect of cyberspace since the distributed denial-of-service attacks against Estonia in 2007: Brown and Poellet (n 66) 130.

136 See below Part V(B).
A Territory Sovereignty in Physical Space

In the context of physical space, a state’s right to freedom from interference with territorial sovereignty is strictly protected. The physical territory of a state consists of its land, its territorial sea (if any) and its airspace. Accordingly, unwelcome state-sponsored incursions into each of these spaces has consistently been treated as a violation of territorial sovereignty, even where such incursions are of a low gravity.

First, in relation to airspace, Estonia has protested several incursions by Russian planes since 2016. While at least one of these incursions lasted less than 60 seconds, Estonia’s Ministry of Foreign Affairs has regularly characterised them as airspace violations, and has issued complaint notes to Russian ambassadors in response. As a further example, in 1960, the Soviet Union downed an unarmed American U-2 reconnaissance aircraft because it was flying through Soviet national airspace. The US did not protest the shoot down, and the absence of protest has been taken as an acknowledgement that the U-2’s entry into Soviet airspace without consent was a violation of international law. The ICJ considered the lawfulness of airspace interference in Military and Paramilitary Activities. That case concerned, among other things, various incursions into Nicaraguan airspace attributed to the US, including high-altitude reconnaissance overflights, and low-altitude overflights which emitted ‘sonic booms’. In respect of both kinds of overflights, the Court held that they directly infringed the principle of respect for territorial sovereignty.

Secondly, in relation to territorial sea, there are similarly prominent examples of unlawful interference worth noting. For instance, the US has conducted several ‘Freedom of Navigation’ operations in the South China Sea since 2015, which typically involve the sailing of warships through parts of the sea claimed by China to be within its maritime boundary. China’s Defence Ministry has responded by

---

137 Crawford (n 10) 203; Jennings and Watts (eds) (n 19) 572–3.
139 ‘Estonia Says Russian Aircraft Violated Airspace Again’ (n 138); ‘Russian Aircraft Violates Estonian Airspace’ (n 138).
142 Military and Paramilitary Activities (n 16) 52–3 [91].
143 Ibid 128 [251].
sending its own naval ships to ward off foreign vessels, and has described the operations as ‘seriously threatening [to] China’s sovereignty and security’.\textsuperscript{145} Similarly, in \textit{Corfu Channel}, the ICJ considered various potential sovereignty violations arising from an incident in which UK warships struck mines in Albanian territorial waters. The Court found that the presence of UK vessels in Albanian waters did not violate international law because of an ‘innocent passage’ exception to Albania’s prima facie claim to territorial sovereignty.\textsuperscript{146} However, the subsequent minesweeping operations carried out by the UK in Albanian waters fell outside of this exception, and so constituted a violation of international law.\textsuperscript{147}

Thirdly, in relation to land, instances of territorial interference are often less innocuous. For instance, Russia’s interference with the Crimean Peninsula in 2014 was characterised by 42 states in a joint statement to the Human Rights Council as an ‘ongoing violation of Ukraine’s sovereignty and territorial integrity’.\textsuperscript{148} Likewise, in \textit{Certain Activities}, the ICJ held that Nicaragua’s conduct on Costa Rican territory, which included the excavation of three caños and ‘establishing a military presence in parts of that territory’, violated Costa Rica’s territorial sovereignty.\textsuperscript{149}

Cumulatively, this state practice and \textit{opinio juris} provide strong support for the view that, at least in respect of physical space, territorial interference is strictly prohibited. A strict view of territorial sovereignty in physical space is important for the development of an equivalent standard in cyberspace, as the rights and duties that flow from sovereignty should not materially change across domains.\textsuperscript{150} International courts commonly have recourse to an analogical methodology when determining rules of customary international law, whereby ‘the rationale of an existing rule is extended to a situation that does not fall within the wording of that rule’ because of a common link or cause between the two situations.\textsuperscript{151} This allows the avoidance of pronouncements of \textit{non liquet} in circumstances where state practice is non-existent or disparate owing to the novelty of a legal question.\textsuperscript{152} To illustrate, in the \textit{Continental Shelf (Libyan Arab Jamahiriya v Malta) (‘Libya–Malta Continental Shelf’)} case, the ICJ found that the ‘distance criterion’, which

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{146} \textit{Corfu Channel} (n 15) 27–32.
  \item \textsuperscript{147} Ibid 34–5.
  \item \textsuperscript{149} \textit{Certain Activities} (n 55) 703 [93]. Some of these examples of territorial interference, as well as several others, are cited and expanded upon in Schmitt and Vihul, ‘Respect for Sovereignty in Cyberspace’ (n 43) 1650–65.
  \item \textsuperscript{150} Buchan, \textit{Cyber Espionage and International Law} (n 93) 54.
  \item \textsuperscript{152} Ibid 422–3.
\end{itemize}
\end{footnotesize}
applied when determining exclusive economic zones, also applied when determining the continental shelf of adjacent states. The Court reasoned that there ‘cannot be an exclusive economic zone without a corresponding continental shelf’ and therefore ‘for juridical and practical reasons, the distance criterion must now apply to the continental shelf as well as to the exclusive economic zone’. A clear parallel can be drawn to territorial sovereignty in cyberspace. The relevant existing rule is that a state’s territorial sovereignty includes a strict right to have its land, sea and airspace free from external physical interference. A common link can be drawn between physical space and cyberspace because cyberspace is a domain that cannot exist without corresponding cyber infrastructure located on a state’s territory and subject to its jurisdiction. Thus, the ‘juridical and practical’ considerations that seized the Court in the Libya–Malta Continental Shelf case favour applying a strict right of freedom from territorial interference in cyberspace as well as in physical space. Indeed, it would be curious if the rule of territorial sovereignty provided a state’s sovereign cyber infrastructure with less protection from intrusion than a state’s sovereign physical territory.

For completeness, it should be acknowledged that cyberspace is different from physical space in some respects. It is not always possible to demarcate where one state’s cyberspace ends and another state’s cyberspace begins. This ubiquitous quality makes cyberspace immune from exclusive appropriation, in that it cannot be subject to the sovereignty of any single state in the way physical territory can be. Nonetheless, all serious attempts to designate cyberspace as res communis, a global commons, have been abandoned. Moreover, state-based efforts to apply international law to cyberspace have invariably proceeded on the common assumption that standards of appropriate state behaviour in the cyber domain are to be derived from existing international norms and commitments. And if territorial sovereignty is not to be conceptualised under international law in a fundamentally different way for cyberspace than for physical space, doctrinal coherence would seem to require that territorial sovereignty be capable of violation by the cyber equivalent of a 60-second airspace incursion.

The next section of this article considers whether this analogical reasoning is consistent with the state practice and opinio juris that have actually manifested in respect of cyberspace.

**B Territorial Sovereignty in Cyberspace**

Evidence of state practice and opinio juris in respect of territorial sovereignty in cyberspace has arisen in two ways: first, states have publicly commented on and

153 Continental Shelf (Libyan Arab Jamahiriya v Malta) (Judgment) [1985] ICJ Rep 13, 33 [34].
154 Ibid (emphasis added).
155 Island of Palmas (n 15) 838; Corfu Channel (n 15) 35; Military and Paramilitary Activities (n 16) 111 [212]. See also the state practice and opinio juris set out in this Part V(A).
156 Buchan, Cyber Espionage and International Law (n 93) 54.
157 von Heinegg, ‘Legal Implications of Territorial Sovereignty in Cyberspace’ (n 22) 9–10.
responded to several significant, recent cyber incidents, sometimes by reference to international law principles; and secondly, states have issued policy statements and strategy documents that express views on their rights and responsibilities in cyberspace. Regarding the former, while non-exhaustive,\(^\text{160}\) the cyber incidents analysed here are notable because they were each attributed to a responsible state by one or more other states with a high degree of certainty, and prompted various publicly recorded verbal and physical responses from the international community.

In 2014, North Korea hacked Sony Pictures Entertainment, causing the release of commercially sensitive information, the destruction of data and the loss of functionality to thousands of Sony computers located on US territory.\(^\text{161}\) This cyber operation coincided with the impending release of The Interview, a satirical film about the assassination of Kim Jong-un.\(^\text{162}\) It also clearly amounted to a violation of territorial sovereignty under the strict inviolability approach. That is, it involved a prima facie interference, being the deletion of data (Scale 4) and the loss of functionality to Sony computers (Scales 5 and 6), and it exceeded the de minimis effects threshold by limiting accessibility to the targeted cyber systems. The US pledged a ‘proportional’ response, imposing various sanctions on North Korea, and allegedly also causing a widespread internet outage in North Korean territory.\(^\text{163}\) The Sony hack was never officially characterised by the US as a breach of its territorial sovereignty (or any other rule of international law, for that matter),\(^\text{164}\) but the severity of the US response suggests that it was treated as such. This is not surprising. Cyber operations that cause targeted cyber infrastructure to lose functionality are of a high gravity, and there is general agreement that these operations amount to a violation of territorial sovereignty.\(^\text{165}\)

In 2016, Russia hacked into the Democratic National Committee’s (‘DNC’) servers during the US presidential election and subsequently published private emails retrieved from those servers.\(^\text{166}\) In this instance, the US characterised the


\(^{161}\) Payne (n 74) 684; McCormack, ‘The Sony and OPM Double Whammy’ (n 104) 379–80; Schmitt, ‘International Law and Cyber Attacks: Sony v North Korea’ (n 74).

\(^{162}\) The Interview (Columbia Pictures, 2014). See Payne (n 74) 684.


\(^{165}\) Schmitt (ed), Tallinn Manual 2.0 (n 3) 20 (Rule 4 Commentary [11]); Kozik (n 11) 98; Osula (n 77) 726; Pirker (n 9) 200–1; von Heinegg, ‘Legal Implications of Territorial Sovereignty in Cyberspace’ (n 22) 11.

cyber operation as a ‘violation of established international norms of behavior’, imposed sanctions against certain Russian individuals and entities, and promised to take a ‘variety of [further] actions [against Russia] … some of which will not be publicized’.\footnote{Barack Obama, ‘Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment’ (Press Release, The White House, Office of the Press Secretary, 29 December 2016) <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity>, archived at <https://perma.cc/A7NR-7RB3>.} The DNC hack offers an interesting case-study because it provoked a particularly strong US response, despite causing only minor effects in the targeted cyber infrastructure. Indeed, under the strict inviolability approach, the remote surveillance or collection of sensitive data (Scale 1) does not violate territorial sovereignty, as it does not exceed the prima facie interference threshold.\footnote{The release of data gathered by means of cyber espionage would also not typically implicate territorial sovereignty.} It is more likely that the means employed in carrying out the surveillance operation or the overall impact of this hack in the context of the presidential election implicated a rule of international law other than territorial sovereignty, such as the prohibition of non-intervention.\footnote{See, eg, Barela (n 166). One scholar has suggested that the hack might have constituted a violation of the right to self-determination: Òhlin (n 93) 1596. A further possibility is that the DNC hack constituted a violation of US sovereignty for usurping one of its inherently governmental functions: Schmitt (ed), \textit{Tallinn Manual 2.0} (n 3) 21–2 (Rule 4 Commentary [15]).} It is certainly doubtful that the US would have responded in the same way to the DNC hack if it were conducted against a private actor or outside of the election campaign. As such, despite its high profile, relatively little can be discerned from this cyber operation for present purposes.

In June 2017, Russia carried out the NotPetya ransomware attack against cyber infrastructure primarily in the Ukraine associated with the financial, energy and government sectors.\footnote{‘NotPetya and WannaCry Call for a Joint Response from International Community’ (n 72); Henley (n 72).} The ransomware encrypted and prevented access to affected computers, and requested a cryptocurrency payment in exchange for a decryption key.\footnote{Henley (n 72).} As with all state-sponsored ransomware attacks, NotPetya constituted a violation of territorial sovereignty under the strict inviolability approach. Evidence of a prima facie interference was satisfied by the insertion of malware onto Ukrainian cyber systems (Scale 2) and also by subsequently causing the temporary loss of functionality to those systems (Scale 5). Moreover, the de minimis effects threshold was exceeded because access to targeted cyber systems was restricted until decryption of the ransomware or some other kind of system restoration was possible. The UK was not directly targeted by the NotPetya attack, but it nonetheless denounced Russia’s conduct as demonstrating ‘disregard for Ukrainian sovereignty’.\footnote{Foreign and Commonwealth Office, National Cyber Security Centre and Lord Ahmad of Wimbledon, ‘Foreign Office Minister Condemns Russia for NotPetya Attacks’ (Press Release, 15 February 2018) <https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks>, archived at <https://perma.cc/6ZLM-NRGE>.} Similarly, the US described NotPetya as ‘reckless’
behaviour that would be met with ‘international consequences’. These verbal responses were notable because they explicitly invoked state sovereignty and contemplated that a proportionate retorsion or countermeasure might be taken. On the other hand, the language used was sufficiently vague as to leave unclear which aspects of Ukraine’s sovereignty were taken to have been disregarded, and whether that disregard violated a specific rule of international law.

Finally, in October 2017, Russia conducted another ransomware attack against Ukraine, this time targeting an airport and underground railway in Kiev. This iteration of ransomware, named Bad Rabbit, also prompted a strong international response. The UK stated that the cyber operation (among others also attributed to Russia at the same time) was a ‘flagrant violation of international law’. Australia observed that Bad Rabbit formed part of a ‘pattern of malicious cyber activity by Russia’ which showed disregard for international law and the norms of responsible state behaviour that apply in cyberspace. These comments left no doubt that, in the view of the commenting states, a violation of international law had occurred. Again though, the particular rule of international law that had allegedly been violated was not identified with precision. This is important because Bad Rabbit targeted, in part, critical national infrastructure, which may have led to its classification as a higher order violation of international law.

In sum, recent practice demonstrates a growing willingness of states to characterise a reasonably wide range of cyber operations as violations of international law, and to respond commensurately with either verbal or physical acts. However, the examples above do not amount to widespread, representative or consistent evidence that the strict inviolability approach has crystallised into a rule of customary international law. While the state responses in each case were decisive, they were not explicitly justified by reference to specific rules of international law, or a particular account of territorial sovereignty. As such, the inferences that might be drawn about the opinio juris of each state are open to doubt. Further, the stark absence of publicly reported state practice in respect of


174 Recall the UK’s position that sovereignty does not constitute a primary rule of international law capable of independent breach: see above Part II(C).

175 “Bad Rabbit” Ransomware Strikes Ukraine and Russia’ (n 72); Perekalin (n 72).

176 “Bad Rabbit” Ransomware Strikes Ukraine and Russia’ (n 72).


179 Draft Conclusions, UN Doc A/73/10 (n 48) 135–6 (Conclusion 8). See also North Sea Continental Shelf (n 128) 43 [74]; Fisheries Jurisdiction (United Kingdom v Iceland) (Merits) [1974] ICJ Rep 3, 23–6 [52]–[58]; Military and Paramilitary Activities (n 16) 108–9 [207].
low and moderate intensity cyber operations (Scale 2 to 4) means that the full scope of the strict inviolability approach remains untested.

Additional evidence of state practice and opinio juris can be found in the policy statements and national cyber security documents of states.\(^\text{180}\) It is now ‘generally accepted’ that, along with physical conduct, verbal acts can be a manifestation of state will.\(^\text{181}\) Moreover, they can be particularly instructive in the context of cyberspace because they allow states to express views on international law unconstrained by the particular circumstances and diplomatic sensitivities that attend a given cyber incident. Perhaps unsurprisingly then, states have increasingly had recourse to their policy statements and strategy documents to communicate their approach to, and the possible content of, territorial sovereignty in cyberspace.

In February 2018, France released its Strategic Review of Cyber Defence, which emphasised the need to ‘fully exercise’ digital sovereignty.\(^\text{182}\) Digital sovereignty was defined as the ability ‘to retain in the digital space the autonomous ability of appreciation, decision and action’.\(^\text{183}\) This sentiment was echoed in the Paris Call for Trust and Security in Cyberspace, in which France committed, inter alia, to ‘[p]revent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet’.\(^\text{184}\) In a joint statement in 2016, Russia and China advocated respect for, and opposed infringements on, state sovereignty in ‘information space’.\(^\text{185}\) China subsequently expanded on this position in its International Strategy of Cooperation on Cyberspace, which asserted that the principle of sovereignty entitled states to ‘protect their ICT [Information and Communications Technology] systems and resources from threat, disruption, attack and destruction’.\(^\text{186}\) Finally, in an October 2018 joint statement on information and telecommunications, Canada, Japan, New Zealand

---

\(^\text{180}\) Crawford (n 10) 24; Draft Conclusions, UN Doc A/73/10 (n 48) 133 (Conclusion 6(2)).

\(^\text{181}\) Draft Conclusions, UN Doc A/73/10 (n 48) 133 (Conclusion 6 Commentary [2]).


\(^\text{183}\) Ibid.


and several other countries emphasised that ‘cyber threats should not be used to... hinder the free flow of information’.  

At their highest, these statements can be seen as a reflection of what some states consider to be the minimum rights that flow from their sovereignty (if not territorial sovereignty) over cyberspace: that is, an autonomous, accessible and available cyberspace, free from interferences that undermine the integrity of the domain or that cause destruction. These are some of the same rights that are protected under the strict inviolability approach. Again though, this state practice and opinio juris cannot be seen as conclusive evidence that the strict inviolability approach has crystallised into accepted customary law. In particular, these policy statements and strategy documents contain imprecise language, falling short of ‘recognition that a rule of law or legal obligation is involved’. The density of this kind of state practice is also not sufficiently extensive or uniform. A considerable number of states have refrained from publicly commenting on the nature of territorial sovereignty in cyberspace altogether, and silence may denote agreement, disagreement or indifference depending on the circumstances. There is also, of course, the directly inconsistent position taken by the UK, that territorial sovereignty is not a specific rule of international law capable of independent breach. For the UK, the sovereign rights that states enjoy in respect of cyberspace are limited to those which flow from the principle of non-intervention and the prohibition on the use of force. Thus, the preliminary question of whether territorial sovereignty can be violated in cyberspace will likely require resolution before the question of when territorial sovereignty is violated can be answered.

VI CONCLUSION

This article has contended that the strict inviolability approach articulates an appropriate and principled standard against which the lawfulness of cyber operations should be measured; specifically, that all state-sponsored cyber operations which interfere with a target state’s cyber infrastructure violate (at least) territorial sovereignty, as long as more than de minimis effects are caused. This approach is consistent with the operation of territorial sovereignty in physical space, and a small but growing body of state conduct in respect of cyberspace. Nonetheless, it has not yet crystallised into a binding rule of customary international law. For this to occur, a greater density of uniform state practice and


188 North Sea Continental Shelf (n 128) 43 [74].

189 Crawford (n 10) 24–5; Draft Conclusions, UN Doc A/73/10 (n 48) 135 (Conclusion 8); North Sea Continental Shelf (n 128) 43 [74].

190 Crawford (n 10) 25; Draft Conclusions, UN Doc A/73/10 (n 48) 141–2 (Conclusion 10 Commentary [8]); Sovereignty over Pedra Branca v Pulau Batu Puteh, Middle Rocks and South Ledge (Malaysia v Singapore) (Judgment) [2008] ICJ Rep 12, 50–1 [121], citing Delimitation of the Maritime Boundary in the Gulf of Maine Area (Canada v United States of America) (Judgment) [1984] ICJ Rep 246, 305 [130].

191 Jeremy Wright (n 46).
Opinio juris is required, and the prevailing uncertainty as to whether territorial sovereignty amounts to a binding rule of international law capable of independent breach needs to be resolved.

These obstacles appear considerable. Indeed, after state participants to the UN GGE on Cyber Security failed to produce a consensus report in 2017, some commentators questioned whether state cooperation in this area had altogether come to an end.192 However, states have recently recommitted to collaboratively developing rules and norms of responsible behaviour in cyberspace through international fora.193 In December 2018, the United Nations General Assembly adopted two resolutions, establishing: a new GGE on Cyber Security to continue the work of previous GGEs, with a view to submitting a final report to the General Assembly in 2021;194 and, separately, an Open-Ended Working Group made up of the entire UN membership to pursue the same objective as the GGE on Cyber Security, but in a more open and consultative format.195 If either of these groups achieve the same success as the earlier GGEs on Cyber Security, the status and content of territorial sovereignty in cyberspace may be clarified sooner than expected.

---


