Research Paper

Harriet Moynihan
International Law Programme | December 2019

The Application of International Law to State Cyberattacks

Sovereignty and Non-intervention

CHATHAM HOUSE
The Royal Institute of International Affairs

Contents

	Summary	2
1	Introduction	3
2	The Application of Sovereignty in Cyberspace	8
3	The Application of the Non-intervention Principle in Cyberspace	26
4	Application of the Law to Case Studies	37
5	Reflections on the Relationship between Sovereignty and the Non-intervention Principle	48
6	Processes for Reaching Agreement on the Application of International Law to Cyberspace	52
7	Conclusions and Recommendations	56
	Acknowledgments	59
	About the Author	59

Summary

- The vast majority of state-to-state cyberattacks consist of persistent, low-level intrusions that take place below the threshold of use of force. International law, including the principle of non-intervention in another state's internal affairs and the principle of sovereignty, applies to these cyber operations.
- It is not clear whether *any* unauthorized cyber intrusion would violate the target state's sovereignty, or whether there is a threshold in operation. While some would like to set limits by reference to effects of the cyber activity, at this time such limits are not reflected in customary international law. The assessment of whether sovereignty has been violated therefore has to be made on a case by case basis, if no other more specific rules of international law apply.
- In due course, further state practice and *opinio iuris* may give rise to an emerging cyber-specific understanding of sovereignty, just as specific rules deriving from the sovereignty principle have crystallized in other areas of international law.
- Before a principle of due diligence can be invoked in the cyber context, further work is needed by states to agree upon rules as to what might be expected of a state in this context.
- The principle of non-intervention applies to a state's cyber operations as it does to other state activities. It consists of coercive behaviour by one state that deprives the target state of its free will in relation to the exercise of its sovereign functions in order to compel an outcome in, or conduct with respect to, a matter reserved to the target state.
- In practice, activities that contravene the non-intervention principle and activities that violate sovereignty will often overlap.
- In order to reach agreement on how international law applies to states' cyber operations below the level of use of force, states should put their views on record, where possible giving examples of when they consider that an obligation may be breached, as states such as the UK, Australia, France and the Netherlands have done.
- Further discussion between states should focus on how the rules apply to practical examples of state-sponsored cyber operations. There is likely to be more commonality about specific applications of the law than there is about abstract principles.
- The prospects of a general treaty in this area are still far off. In due course, there may be benefit in considering limited rules, for example on due diligence and a prohibition on attacking critical infrastructure, before tackling broad principles.

1. Introduction

1. Hostile cyber operations by one state against another state are increasingly common. It is estimated that over 22 states are responsible for sponsoring cyber operations that target other states, and the number and scale of these operations is growing.[1] Cyber operations that cause injury or death to persons or damage or destruction of objects could amount to a use of force or armed attack under the UN Charter (although the threshold for what constitutes a use of force is itself an area of controversy).[2] But in practice, the vast majority of cyber operations by states take place below the threshold of use of force, instead consisting of persistent, low-level intrusions that cause harm in the victim state but often without discernible physical effects.

2. To take just a few public examples, the NotPetya attack, an indiscriminate malware attack on companies and governments Europe-wide, was attributed to Russia by a number of states in February 2018.[3] A global hacking campaign targeting universities was attributed to Iran by the US and UK in March 2018. An attack aimed at compromising specific routers to support espionage and theft of intellectual property (IP) was jointly attributed to Russia by the US and UK in April 2018.[4] In December 2018, the so-called Five Eyes intelligence-sharing alliance[5] attributed the activities of a Chinese cyber espionage group targeting IP and sensitive commercial property to China's Ministry of State Security. China has also been targeted; the country stated that, in 2017, it suffered nearly $60 billion in economic loss due to cybersecurity incidents, with 93.5 per cent of ransomware attacks in China conducted from overseas.[6] In October 2019, the UK's National Cyber Security Centre revealed that the UK has been on the receiving end of almost 1,800 cyberattacks in the preceding three years (i.e. at least 10 a week), most carried out by state-sponsored hackers.[7]

3. In the past, the ability of states to attribute cyberattacks of this nature to specific perpetrators (whether a state, a proxy acting on behalf of a state or a non-state actor acting independently of a state)[8] was very challenging, particularly in cases where the attackers are operating at speed from multiple servers in different jurisdictions, with the ability to hide their identity. However, developments in technology

[1] For an overview of cyber operations from 2005 to 2018, see Council on Foreign Relations (n.d.), 'Cyber Operations Tracker', https://www.cfr.org/interactive/cyber-operations (accessed 24 Sep. 2019); for a more up to date list of incidents, see Center for Strategic & International Studies (n.d.), 'Significant Cyber Incidents Since 2006', https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf (accessed 24 Sep. 2019).
[2] UN Security Council (n.d.), 'Charter of the United Nations', Article 2(4), https://www.un.org/en/charter-united-nations/.
[3] Council on Foreign Relations (n.d.), 'Cyber Operations Tracker', https://www.cfr.org/interactive/cyber-operations (accessed 24 Sep. 2019).
[4] National Cyber Security Centre (2018), 'Joint US – UK statement on malicious cyber activity carried out by Russian government', https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government (accessed 24 Sep. 2019).
[5] The 'Five Eyes' refers to an alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. These countries are bound by the multilateral UKUSA Agreement for joint cooperation in signals intelligence, military intelligence, and human intelligence.
[6] Ministry of Foreign Affairs of the People's Republic of China (2019), ' The Daily Telegraph Publishes a Signed Article by Ambassador Liu Xiaoming Entitled Dialogue and co-operation are the only way to cyber security', https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zwjg_665342/zwbd_665378/t1631237.shtml (accessed 24 Sep. 2019).
[7] National Cyber Security Centre (2019), 'Annual Review 2019', https://www.ncsc.gov.uk/news/annual-review-2019 (accessed 28 Oct. 2019).
[8] Often states will use non-state actors as proxies to conduct 'state-sponsored' cyber operations in another state on their own behalf. Whether or not these operations fall within the ambit of the non-intervention principle depends on whether their actions can be 'attributed' to a state under the tests set out in international law.

have provided states with a greater ability to accurately attribute cyber intrusions,[9] including through working with private cybersecurity companies. Some non-governmental bodies also work on the attribution of cyber operations.[10]

4. In the last few years, states have become more willing to attribute cyberattacks to other states; something they were reluctant to do previously. The amount of public attributions has increased significantly, as has the number of states making those attributions.[11] There is also a growing trend for states to work together to attribute malicious state-sponsored cyber operations. There are also discussions among states, academics and private-sector bodies about the feasibility of creating an international mechanism, perhaps under the auspices of the UN, with responsibility for attribution of state-sponsored cyber operations that interfere in another state.[12]

> States have agreed that international law, including the principles of sovereignty and non-intervention, does apply to states' activities in cyberspace.

5. States have agreed that international law, including the principles of sovereignty and non-intervention, does apply to states' activities in cyberspace.[13] But how the law applies is the subject of ongoing debate. Not only is the law in this area unclear; states are also often ambiguous in invoking the law or in how they characterize it.[14] For example, in relation to the hacking of Sony Pictures Entertainment, which the US government attributed to North Korea, the then Secretary of State John Kerry stated that North Korea had 'violated international norms'. But when President Obama was asked if the Sony hack was an act of war, he responded, 'No, it was an act of cyber vandalism that was very costly… We will respond proportionately, and we will respond in a place and time and manner that we choose'. The reference to exercising a right to respond assumes an underlying breach of international law, but the precise nature of the breach remains unclear.[15]

6. The lack of agreement on how international law applies to states' cyber activities has created legal uncertainty. Some states may prefer this state of affairs, as it may be thought that any agreed regulation of cyber operations could be contrary to their interests.[16] But for states that adhere to the rules-based system of international affairs, a clear legal basis should be necessary both to carry out cyber operations and to make assertions that another state has violated international law. States that are the victim

[9] See Rowe, N. C. (2015), 'The Attribution of Cyber Warfare', in Green, J. A. (ed) (2015), *Cyberwarfare: A Multidisciplinary Analysis*, Routledge, pp. 61–72.
[10] For example, the NGO Bellingcat: Bellingcat (2017), 'Bahamut Revisited, More Cyber Espionage in the Middle East and South Asia', https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/ (accessed 24 Sep. 2019). At the same time, private companies publishing attribution reports may face a conflict of interests when identifying responsible state actors, depending on their location and state affiliations.
[11] For further discussion on attribution, see the AJIL Symposium on Cyber Attribution (2019), *AJIL Unbound*, 113, Cambridge University Press; Tsagourias, N. (2012), 'Cyber attacks, Self-defence and the Problem of Attribution', *Journal of Conflict and Security Law*, 17(2).
[12] The Federmann Cyber Security Center at the Hebrew University of Jerusalem is running a project on *The Prospects for an International Attribution Mechanism for Cyber Operations,* https://csrcl.huji.ac.il/book/prospects-international-attribution-mechanism-cyber-operations (accessed 24 Sep. 2019). RAND and Microsoft have proposed a Global Consortium for Cyber Attribution, Mueller, M. (2017), 'A Global Cyber-Attribution Organization – Thinking it through', Internet Governance Project, https://www.internetgovernance.org/2017/06/04/a-global-cyber-attribution-org/ (accessed 24 Sep. 2019).
[13] UNGA (n.d.), 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', 24 June 2013, UN Doc A/68/98, paras 19–20, https://undocs.org/A/68/98 (accessed 22 Oct. 2019). This was repeated in the report of the same Group in 2015: Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, para 28(b), https://undocs.org/A/70/174 (accessed 22 Oct. 2019).
[14] Efrony and Shany refer to a 'policy of silence and ambiguity' that is designed to preserve high levels of operational flexibility within the cyber domain, Efrony, D. and Shany, Y. (2018), 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice', *American Journal of International Law,* 112: pp. 583–657, p. 588.
[15] Similarly, in 2018, the UK's National Cyber Security Centre attributed a series of cyberattacks against targets in the UK to Russia's military intelligence service, stating that they were 'conducted in flagrant violation of international law', but did not specify which international obligation had been breached: National Cyber Security Centre (2018), 'Reckless campaign of cyber attacks by Russian military intelligence service exposed', https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed (accessed 24 Sep. 2019).
[16] Efrony and Shany (2018), 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice', p. 653.

of cyberattacks by other states need to be able to identify which rules of international law have been breached in order to know what action they are permitted to take in response, including whether they are entitled to take countermeasures (action in response to an internationally wrongful act by another state, which would otherwise be unlawful but which is permissible under certain conditions).[17] Similarly, states contemplating or undertaking cyber operations need to understand the parameters of the law in order to ensure that their actions do not violate it.

7. While states are still at a relatively early stage in deciding and voicing how they consider that the principles of international law apply to states' cyber actions, there is a trend for states to be more vocal about their views on the law in this area. Even when states put their positions on record, there will inevitably be some differences and debates among states (and commentators) on how the law applies, as there are in many other areas of international law, including the rules on the use of force and international humanitarian law. It is also not unusual for states to adopt deliberately ambiguous positions about the application of the law, to give them greater flexibility to act. But progress can be made in analysing, and as far as possible agreeing, how existing concepts of international law apply in the cyber domain.

I. Purpose and scope of paper

8. The aim of this paper is to analyse the application of the sovereignty and non-intervention principles in relation to states' cyber operations in another state below the threshold of the use of force (while accepting that the determination of when a state's cyber operation constitutes a use of force raises its own challenges). In doing so, the paper seeks to address some of the questions and ambiguities in this area, and to offer interpretative possibilities at a time when a number of states are starting to form and publicize their views on how these principles might apply in relation to states' actions in cyberspace. The paper takes into account state practice to date, including examples of states' cyber operations in other states, in order to clarify where the limits of the law might lie with reference to specific scenarios in practice. It is hoped that by analysing applicable principles or rules in this area, and identifying gaps or disagreements, this may contribute to rule-making in this space, and even increase the prospects of states working towards common approaches or resolving differences.

9. The paper recognizes that this aspect of cyber and international law is just one part of the legal architecture that regulates cyberspace. Cyberspace has many different strands and is governed by a diverse set of norms that are developing in parallel to the issues discussed in this paper, for example in relation to digital rights, cybercrime and cyber terrorism.

10. The paper draws on the state practice available, including statements by certain governments about how they consider international law to apply, both in general and in relation to particular cyber intrusions. The paper has also had the benefit of considerable scholarly writing in this area. It has also been able to draw upon discussions at meetings with experts from states, international organizations, academics and practitioners.

11. The paper is divided into seven chapters, including this introduction. Chapter 2 discusses the application of the international law concept of sovereignty in cyberspace. Chapter 3 discusses the application of the non-intervention principle in cyberspace. Chapter 4 applies the conclusions

[17] Such action is governed by strict conditions and is permissible if aimed at returning relations between the hostile state and the victim state to one of lawfulness, and bringing an end to the prior unlawful act (Art 49 of the International Law Commission's Draft Articles on State Responsibility ('the ILC's Articles on State Responsibility').

reached in chapters 2 and 3 to examples of state-sponsored cyber operations. Chapter 5 reflects on the relationship between sovereignty and non-intervention. Chapter 6 considers the procedures available for states and other actors to reach agreement on the application of rules in this area. Chapter 7 offers conclusions on the law and recommendations for governments, the private sector and civil society working in this area.

12. Some areas are not covered. The paper does not address the application of the use of force or international humanitarian law to states' cyber operations in another state. Nor does the paper address certain other aspects of international law that are potentially relevant to states' cyber operations, such as international human rights law. In practice, states sometimes use non-state actors as proxies to carry out cyber operations in another state on their behalf. The activities of such non-state actors are covered by this paper only insofar as they can be attributed to a state under the international law of attribution (and in this paper, the term 'state-sponsored' refers to cyber operations that may be attributed to a state accordingly).[18] Cyber activities that are performed by individuals or corporate entities whose actions are not attributable to a state are therefore outside the scope of this paper. The paper does not seek to address remedies, including countermeasures, in any detail.

13. States sometimes use cyber operations in response to what they consider to be an internationally wrongful act committed by another state (whether or not by cyber activity), and seek to justify them as countermeasures.[19] If the operations in question meet the conditions for applying countermeasures, it will not be necessary to consider whether or not the activity violates sovereignty or any other rule of international law.

14. In seeking to apply existing rules of international law to cyber operations, researchers are hampered by a lack of publicly available evidence of state practice. States conduct cyber operations in secret, and to date few states have put on record how they think the law applies.[20] But there is currently a great deal of activity, inter-governmental and otherwise, dedicated to attempts to reach agreement on the application of international law in this area.

II. Existing work in this area

15. There have been some significant developments at the inter-state level. In the UN, the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) has held a number of meetings since 2004 to discuss the application of international law to cyber activities. This group, whose membership started with 10 states and has now grown to 25, has been closely followed by other states. In 2013 and 2015,[21] the UN GGE agreed that the principles of the UN Charter apply to states' actions in cyberspace, but the 2017 GGE ended in deadlock without a consensus report. In 2018, the UN General Assembly established a new GGE to work on these issues from 2019–21, as well as an Open-Ended Working Group (OEWG), with a similar mandate, to report to the General Assembly in 2020.

[18] The rules of attribution are predominantly set out in the ILC's Articles on State Responsibility.
[19] For example, it has been suggested that the reported use of cyber operations by the US against Iran may have been a countermeasure in response to the shooting down of a US drone, Schmitt, M. (2019), 'Top Expert Backgrounder: Aborted US Strike, Cyber operation against Iran, and International Law', *Just Security*, https://www.justsecurity.org/64669/top-expert-backgrounder-on-aborted-u-s-strike-and-cyber-operation-against-iran-and-international-law/ (accessed 24 Sep. 2019).
[20] See paras 22–25 for a summary of the positions of those states that have put on record their views.
[21] Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, para 28(b).

16. At the academic level, the international group of experts involved in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (the 'Tallinn Manual 2.0')[22] looked at the applicability of the international law concepts of sovereignty and non-intervention to cyberspace, which are discussed in chapters 2 and 3. Tallinn Manual 2.0 provides a valuable reference point and platform for debate on these issues, while acknowledging that it does not answer all of the questions, and that there were disagreements among the experts on certain points. Tallinn Manual 2.0 was designed to be the beginning of a longer and more significant discussion about the application of international law to states' cyber operations in peacetime[23] and it is hoped that this paper will contribute to that discussion.

17. In applying the principles of sovereignty and non-intervention to cyber operations conducted by a state against another state, a fundamental question arises about the application of *any* principles of international law to the actions of states. Does a novel form of state act, such as cyber operations, need to have its own principles and rules of international law created for it, or is it appropriate to apply the existing rules of international law to all state acts? Not only does the common practice of the law lead to acceptance of the latter approach, but it also appears that the UN GGE opted for it, by saying that international law applies to the cybersphere – that is, that entirely new international legal principles do not have to be created for it. The assumption in this paper is therefore that the objective should be to ascertain *how* the existing principles apply – not *whether* they do. State practice, such as it is, will be useful in deciding how the principles apply, but not whether they apply at all.

[22] Schmitt, M. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed, Cambridge University Press.
[23] See Jensen, E. (2017), 'The Tallinn Manual 2.0: Highlights and Insights', *Georgetown Journal of International Law*, 48: p. 778.

2. The Application of Sovereignty in Cyberspace

18. The use of cyber operations by states to harm, to disrupt, to influence or even simply to irritate citizens and institutions in other states is a phenomenon that fits, but not without controversy, into existing paradigms of international law. While there was formerly some dispute about whether the existing rules of international law were applicable to cyberspace at all,[24] states agreed at the UN GGE in 2013 and 2015 that international law, including the principles of sovereignty and non-intervention, does apply to states' activities in cyberspace, as it does in the non-cyber context:

> State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.[25]

19. The experts also agreed that the principles of the UN Charter applied:

> (b) In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States.[26]

As well as individual states, numerous international bodies have recognized this.[27] In brief, the principle of state sovereignty encapsulates the supreme authority of a state to territorial integrity, sovereign equality and political independence within its territory to the exclusion of all other states. The rule prohibiting intervention in another state's internal affairs derives from the sovereignty principle, and consists of coercive behaviour by one state in relation to the inherently sovereign powers of another state.

20. In the West at least, there are two schools of thought about how international law applies to state-sponsored cyber activity that takes place below the threshold of use of force. One is that the non-intervention principle applies to certain state-sponsored cyber intrusions, and that below the threshold of that principle, the activity may be unfriendly but will not constitute a breach of international law giving rise to state responsibility. On this view, sovereignty is a principle

[24] See reference to the dispute between Johnson and Post on the one hand, and Goldsmith on the other, in Tsagourias, N. (2018), 'Law, Borders and the Territorialisation of Cyberspace', *Indonesian Journal of International Law*, 15(4): p. 11.
[25] UNGA (2013), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 24 June 2013, UN Doc A/68/98, para 20; UNGA (2015), *Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015, para 27.
[26] UNGA (2013), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 24 June 2013, UN Doc A/68/98, paras 19–20; UNGA (2015), *Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015, para 28(b). The 2015 UN GGE also agreed 11 voluntary and non-binding norms, rules and principles of responsible state behaviour in the ICT environment.
[27] See, for example, NATO (2014), Wales Summit Declaration, 5 September 2015, para 72, https://www.nato.int/cps/en/natohq/official_texts_112964.htm (accessed 22 Oct. 2019); Organization for Security and Co-operation in Europe (OSCE) (2016), OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, Decision No. 1202, Permanent Council, 10 March 2016, PC.DEC/1202, calling on the international community to 'develop a peaceful, secure, fair and open information space based on the principles of cooperation and respect for sovereignty and non-interference in the internal affairs of other countries'; Embassy of the Republic of Uzbekistan to the Republic of Latvia (2016), 'The Tashkent Declaration of the Fifteenth Anniversary of the Shanghai Cooperation Organization', https://uzbekistan.lv/en/the-tashkent-declaration-of-the-fifteenth-anniversary-of-the-shanghai-cooperation-organization/ (accessed 22 Oct. 2019); Council of the EU (2017), 'EU Council Conclusions of 20 November 2017', https://www.consilium.europa.eu/media/31666/st14435en17.pdf (accessed 22 Oct. 2019); The Commonwealth (2018), 'Commonwealth Cyber Declaration', https://thecommonwealth.org/commonwealth-cyber-declaration (accessed 22 Oct. 2019).

of international law that may guide state interactions, but it does not amount to a standalone primary rule, at least not in the cyber context.[28]

21. Another view holds that cyber operations below the non-intervention threshold may be unlawful as violations of the target state's sovereignty.[29] This is the approach adopted in the Tallinn Manual 2.0, which draws rules from both sovereignty and non-intervention and applies them to operations in cyberspace.[30]

State practice

22. Since the publication of the Tallinn Manual 2.0, the 'sovereignty as a rule' debate has been much discussed among commentators in the cyber context,[31] but until recently there has been little public state practice to help inform that debate. States have chosen to adopt a 'policy of ambiguity and silence' about how international law applies in cyberspace.[32] Some states have commented generally on the application of international law in cyberspace but without stating how they consider the principles of sovereignty and non-intervention to apply. Estonia's statement on cyber and international law, for example, addressed a number of aspects of the application of international law to cyberspace, but did not explicitly address sovereignty and non-intervention.[33] Iran has stated that 'malicious use of ICTs [is] a serious and impending threat of violating States' sovereignty and internal affairs' but without specifying how these principles apply in practice.[34]

23. The UK have put on record their view that the non-intervention principle applies to states' cyber operations and have provided specific examples of situations in which they consider that the principle may apply. The UK have also stated that in their view, there is no additional prohibition on cyber activity to be extrapolated from the sovereignty principle.[35] A 2017 Memorandum issued by the outgoing General Counsel of the US Department of Defense took a similar position on sovereignty,[36] although this is in tension with other statements by US government officials, which have foreseen a role for sovereignty in the application of international law to cyberspace.[37] Other states have

[28] The UK favours this view.
[29] See, for example, Schmitt, M. N. and Vihul, L. (2017), 'Sovereignty in Cyberspace: Lex Lata Vel Non?', *AJIL Unbound,* 111: pp. 213–218.
[30] The Tallinn Manual 2.0 has become an important reference point for states, international organizations and academics; see, for example, the NATO cyber toolkit, NATO CCDCOE (n.d.), 'Cyber Law Toolkit', https://cyberlaw.ccdcoe.org/wiki/Main_Page (accessed 3 Oct. 2019). For a critique of both Tallinn Manuals, drawing the conclusion that there is currently limited support in state practice to support certain key rules, see Efrony and Shany (2018), 'A Rule Book on the Shelf?', p. 585; and discussion of this article in the Symposium on 'Sovereignty, Cyberspace and Tallinn Manual 2.0', *AJIL Unbound* 2017.
[31] See Corn, G. P. (2019), 'Cyber National Security: Navigating Gray-Zone Challenges in and through Cyberspace', in Williams, W. S. and Ford, C. M. (eds)(2019), *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, Oxford University Press, p. 59. The AJIL Symposium on 'Sovereignty, Cyberspace and Tallinn Manual 2.0', *AJIL Unbound* 2017, contains several articles debating the normative character of sovereignty in the cyber context.
[32] Shany and Efrony (2018), 'A Rule Book on the Shelf?', pp. 583–657. The authors argue that the goal of such an approach is to maintain as much leeway as possible under the legal, technological and political uncertainties of cyberspace.
[33] Kaljulaid, K. (2019), 'President of the Republic of Estonia at the opening of CyCon 2019', https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/ (accessed 4 Oct. 2019). In the context of noting that states are responsible for their activities in cyberspace, the President stated that 'sovereignty entails not only rights, but also obligations', but beyond that did not address the issue of how sovereignty applies in cyberspace.
[34] Submission by the Islamic Republic of Iran to the Open Ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security, para 10.
[35] The former attorney general for England and Wales stated: 'I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is that there is no such rule as a matter of current international law', Wright, J. (2018), '*Cyber and International Law in the 21st Century*', speech at Chatham House event May 2018.
[36] Memo from Jennifer M. O'Connor to the US Combatant Command, entitled *International Law framework for employing Cyber Capabilities in Military Operations*: '[m]ilitary cyber activities that are neither a use of force nor that violate the principle of non-intervention are largely unregulated by international law at this time…' (the memo is no longer publicly available but is quoted by Watts, S. and Richard, T. (2018), 'Baseline Territorial Sovereignty and Cyberspace', p. 827).
[37] See U.S. Department of Defense, Office of General Counsel (1999), *An Assessment of International Legal Issues in Information Operations* 19 (2nd edition), which argued that, 'an unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty' (discussed by Watts at p. 853); Koh, H. H. (2012), 'International Law in Cyberspace', speech, response to question 9 on state sovereignty, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm (accessed 4 Oct. 2019).

commented that the non-intervention principle applies, but have not commented on whether a more general principle of sovereignty applies in cyberspace,[38] perhaps preferring to adopt a position of 'wait and see',[39] or of strategic ambiguity.

24. China's International Strategy for Co-operation in Cyberspace of March 2017 provides that the principle of sovereignty applies in cyberspace, and that 'No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in, condone or support cyber activities that undermine other countries' national security'.[40] However, as violations of sovereignty can cover a spectrum of activity, including in the context of specific rules on the use of force and non-intervention that derive from the principle of sovereignty, the extent to which China or other states consider activity below the non-intervention threshold to be a violation of sovereignty is unclear. Government statements about sovereignty in general terms also need to be read with care since sovereignty is a word that can be used in different senses in both the non-cyber and cyber contexts.[41]

> As violations of sovereignty can cover a spectrum of activity, the extent to which China or other states consider activity below the non-intervention threshold to be a violation of sovereignty is unclear.

25. In the past year, certain states have started to publish their positions on sovereignty in more detail. In July 2019, the Netherlands set out its view that both the internal and external aspects of sovereignty apply in full in the cyber domain and that states are not permitted to perform cyber operations that violate the sovereignty of another state.[42] In September 2019, France set out in some detail its views on the application of international law to cyberspace, including that unauthorized state cyber intrusions into French systems, or any production of effects on French territory caused by cyber means, may constitute a violation of sovereignty.[43] The notion that cyber operations below the non-intervention threshold may be unlawful as violations of the target state's sovereignty appears to be the unpublicized view of certain other governments too.[44]

26. To date, relatively few states have been prepared to put on record how they think these principles apply in practice; nor are there any treaties in this regard.[45] In the meantime, as with any other state activity, existing principles and rules of customary international law are applicable to state activities in cyberspace, unless there is state practice with *opinio iuris* to indicate that a relevant principle or rule is not applicable.

---

[38] See 2019 International Law Supplement to Australia's International Cyber Engagement Strategy, Annex A, p. 1/5: 'harmful conduct in cyberspace that does not constitute a use of force may still constitute a breach of the duty not to intervene in the internal or external affairs of another state'. The statement makes no reference to sovereignty. Australian Government Department of Foreign Affairs and Trade (2019), 'Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace', *Australia's International Cyber Engagement Strategy*, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/2019_international_law_supplement.html (accessed 20 May 2019).

[39] The then legal adviser to the US State Department, Brian Egan, has stated that interference with an election would be a clear violation of the rule of non-intervention, but was more nuanced when discussing sovereignty: 'Precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and *opinio juris* of States', Egan, B. (2017), 'International Law and Stability in Cyberspace', *Berkeley Journal of International Law*, 35(1): p. 13.

[40] Xinhuanet (2017), 'International Strategy of Cooperation on Cyberspace', http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_5.htm (accessed 4 Oct. 2019).

[41] For example, 'cyber sovereignty' is a term used by China to describe its self-asserted right to control access to the internet within its territory.

[42] Government of the Netherlands (2019), 'Letter to the parliament on the international legal order in cyberspace', https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace (accessed 25 Nov. 2019).

[43] Ministère des Armées (2019), 'Droit International Applique Aux Operations Dans Le Cyberspace', https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international (accessed 5 Oct. 2019).

[44] Views given informally by government representatives in workshops held to discuss drafts of this paper.

[45] Aside from the Council of Europe's Budapest Convention on Cybercrime, which focuses on criminal justice for cybercrime.

27. This chapter and the following look afresh at the relevance of sovereignty and non-intervention to states' cyber operations below the level of use of force. This chapter starts by discussing the international law concept of sovereignty and then considers how it can apply to states' actions in cyberspace. The following chapter then discusses the principle of non-intervention, which reflects and protects sovereignty, and considers how the non-intervention principle applies to state-sponsored cyber intrusions.

I. General rules on sovereignty

28. Sovereignty is fundamental to statehood. Oppenheim refers to the different aspects of sovereignty thus:

> Inasmuch as it excludes subjection to any other authority, and in particular the authority of another state, sovereignty is *independence.* It is *external* independence with regard to the liberty of action outside its borders. It is *internal* independence with regard to the liberty of action of a state inside its borders. As comprising the power of a state to exercise supreme authority over all persons and things within its territory, sovereignty involves *territorial* authority.[46]

29. Sovereignty encompasses a bundle or package of rights. Judge Alvarez in the *Corfu Channel* case stated that, by sovereignty 'we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other states, and also in its relations with other States'.[47] The Friendly Relations Declaration refers to the 'rights inherent in full sovereignty',[48] and this language is reflected in other international instruments. The Helsinki Final Act, for example, records that participating states will:

> respect each other's sovereign equality and individuality as well as all *the rights inherent in and encompassed by its sovereignty,* including in particular the right of every State to juridical equality, to territorial integrity and to freedom and political independence. They will also respect each other's right freely to choose and develop its political, social, economic and cultural systems as well as its right to determine its laws and regulations.[49]

30. Distilling the sources cited above, the three core rights inherent in sovereignty (with correlative duties on other states) may be characterized as:

- the right to territorial integrity and territorial authority (territorial sovereignty);
- the right to independence of state powers;[50] and
- the equality of states in the international order, sometimes referred to as 'external sovereignty'.[51]

The rights that are embodied in the concept of sovereignty will be the basis of any claim a state makes that another state has engaged in a violation of its sovereignty.

---

[46] Oppenheim, L. (1996), *Oppenheim's International Law, Vol. 1: Peace*, 9th edn, Jennings, R. Y. and Watts, A. (eds), London; New York: Longmans, p. 382.
[47] *Corfu Channel Case (United Kingdom v. Albania)*; Separate Opinion, 9 April 1949, ICJ Rep 43.
[48] Resolution 2625 (XXV) of 24 October 1970 containing the Declaration of Principles of International Law, Friendly Relations and Cooperation Among States in Accordance with The Charter of the UN, UN Doc. A/Res/2625.
[49] Article I of Conference on Security and Cooperation in Europe Final Act ('Helsinki Final Act'), Helsinki 1975, emphasis added; see also, as a random example, The Treaty of Friendship, Good Neighbourliness and Cooperation between Spain and Morocco, which refers to 'all the rights inherent and embodied in… sovereignty, in particular, the right to equality before the law, territorial integrity, freedom and political independence. [The Parties] shall, moreover, respect the right of each Party freely to choose and develop its political, social, economic and cultural system', Treaty of Friendship, Good-Neighbourliness and Cooperation between Spain and Morocco, signed at Rabat on 4 July 1991, General Principle 2.
[50] The ILC Draft Declaration on the Rights and Duties of States provides in Article 1 that, 'Every State has the right to independence and hence to exercise freely, without dictation by any other State, all its legal powers, including the choice of its own form of government'.
[51] This principle refers to recognition in the international order of the absolute equality and independence of all states, rather than to their equality in power or in fact.

Territorial sovereignty

31. Within this aspect of sovereignty are encompassed a state's rights in relation to its land territory and boundaries, aerial space, territorial sea and other maritime zones. Treaty provisions and customary law duties regarding land and maritime and aerial zones reflect and safeguard a state's territorial integrity; so too does the law on the prohibition of the use of force.

32. Breaches of territorial sovereignty are not always accompanied by the use of force. In *Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v. Nicaragua),* the International Court of Justice (ICJ), without finding it necessary to consider the separate allegation that there had been an unlawful use of force, found that 'Nicaragua carried out various activities in the disputed territory since 2010, including excavating three *caños* and establishing a military presence in parts of that territory. These activities were in breach of Costa Rica's territorial sovereignty.'[52]

33. The principle of territorial sovereignty includes the right of a state to exercise jurisdiction within its own territory. Jurisdiction here can usefully be divided into powers of prescription, enforcement and adjudication. A state's right to exercise all forms of jurisdiction within its territory may also be regarded as one of the rights flowing from the aspect of sovereignty relating to the independence of state powers.

Independence of state powers

34. A related aspect of the bundle of sovereign rights is the freedom of states to conduct their own affairs independently as regards their own territory. This element of sovereignty, tied in with territorial sovereignty, is referred to in the *Island of Palmas* case: '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'.[53] The ILC Draft Declaration on the Rights and Duties of States provides in Article 1 that, 'Every State has the right to independence and hence to exercise freely, without dictation by any other State, all its legal powers, including the choice of its own form of government'.[54] The right is reflected in Article 2(7) of the UN Charter, with its reference to matters 'essentially within the domestic jurisdiction of any state'.[55]

35. The powers and rights of states that come within this aspect of sovereignty include the right of a state to political independence, including the right freely to choose and develop its political, social, economic and cultural system, and the right to exercise jurisdiction.[56] While these governmental powers are quite wide, states must act within the framework of international law. In addition to any applicable treaty obligations, states must also abide by rules of customary law, such as those in relation to non-intervention and respect for sovereignty, alongside obligations relating to the status and protection of the individual under international humanitarian and human rights law.

---

[52] *Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v Nicaragua),* Judgment, ICJ Reports 2015, para. 93. See also *Corfu Channel* (Merits) Judgment 9 April 1949.
[53] *Island of Palmas* case (USA v Netherlands) PCA 4 April 1928, pp. 829, 838; see also paras 117–8.
[54] Draft Declaration on the Rights and Duties of States with commentaries, text adopted by ILC in 1949.
[55] UN Security Council (n.d.), 'Charter of the United Nations', Article 2(7). 'Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state'.
[56] See the International Court of Justice in *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Merits, 27 June 1986, ICJ 14 ('the *Nicaragua* case'), which referred to 'matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy' (para 205). Although this was stated in the context of the non-intervention principle, it is still relevant to sovereignty as the non-intervention principle is itself a reflection of the principle of sovereignty.

Sovereign equality

36. A further aspect of sovereignty is the equality of states in the international order, sometimes referred to as 'external sovereignty'. The principle refers to recognition in the international order of the absolute equality of all states in terms of their rights and duties in international law, rather than to their equality in power or in fact. The principle reinforces the notion that each state enjoys the rights inherent in sovereignty while being bound to respect the independence and authority of other states. The principle reflects the fact that sovereignty must be applied in an objective manner, as opposed to sovereignty simply being what a state says it is.

> Each state enjoys the rights inherent in sovereignty while being bound to respect the independence and authority of other states.

37. It is clear from the above that while the various elements of sovereignty can be separated out and are sometimes referred to individually, in practice they are inextricably linked and work together. The right of a state to exercise jurisdiction on its territory involves both territorial sovereignty and the right of a state to exercise independent state powers. The independent and exclusive nature of that right derives from the principle of sovereign equality. Oppenheim treats breaches of internal independence and territorial sovereignty together, without distinguishing which aspect is breached.[57]

Sovereignty as an all-embracing principle

38. There are some specific rules that reflect the general principle of sovereignty and that regulate or prohibit the exercise of authority by one state in another's territory. These include the rules on the use of force, which are to be found in the UN Charter and customary international law;[58] the principle of non-intervention into the internal affairs of other states; and the law of the sea and air law, as incorporated in the UN Convention on the Law of the Sea and the Convention on International Civil Aviation (Chicago Convention), as well as customary international law. There are also treaties giving consent to or regulating specific activities within a state's territory, such as Status of Forces Agreements and the Vienna Conventions on Diplomatic Relations and on Consular Relations.

39. These rules and other specific rules may apply as *lex specialis* in relation to the exercise of a state's authority in relation to an area over which that state has exclusive state powers. Where there is no *lex specialis* in place, the exercise of state power by one state in relation to another state continues to be governed by the general rules on sovereignty discussed above.

II. Sovereignty as it applies to states' activity in cyberspace

40. There has been some debate about the extent to which the notion of territorial sovereignty applies to cyberspace at all.[59] Violation of a state's territorial sovereignty is typically associated with some physical incursion into a state's territory, whether by land, sea or air. But while states' cyber activities

[57] For example in para. 119, headed 'Violations of independence and territorial and personal authority', Oppenheim notes that 'It is not feasible to enumerate all such actions as might constitute a breach of a state's duty not to violate another state's independence or territorial or personal authority', and then goes on to give some examples; Oppenheim (1996), *Oppenheim's International Law, Vol. 1: Peace*, p. 385.
[58] Including consensus resolutions of the UN General Assembly, e.g. the Friendly Relations Declaration and Resolution 3314 (XXIX) of December 14, 1974 recommending to the United Nations Security Council a definition it should use for the crime of aggression.
[59] See Tsagourias, N. (2015), 'The legal status of cyberspace,' in Buchan, R. and Tsagourias, N. (eds) (2015), *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, p. 13 for a summary of this debate.

have a physical, tangible aspect (for example in the form of computer hardware and infrastructure), interactions in cyberspace also have a 'virtual' dimension, through the transmission of data, signalling, and sending of content between physical devices.

41. Further, cyberspace as such has no fixed territorial boundaries. There are many varieties of network architecture and numerous ways in which data is stored, which may cross territorial boundaries. Cyber infrastructure such as internet servers may be located in a particular territory, but interactions in cyberspace are often deterritorialized, and sometimes subject to greater regulatory control by global technological corporations, such as Google and Facebook, than states.[60] Some academics have pointed out that network frontiers do not map directly to geographical borders.[61]

42. Nevertheless, cyberspace does have a physical aspect, which consists of computers, integrated circuits, cables and communications infrastructure. It also has a logical layer, which consists of software logic, data packets and electronics; and a social layer, which includes human beings.[62] This physical equipment is located within the territory of a state, and is owned by governments and companies. Thus, cyberspace does not exist independently from the physical world but is instead rooted in it.[63] Transactions in cyberspace involve real people in one territorial jurisdiction either transacting with real people in other territorial jurisdictions or engaging in activity in one jurisdiction that causes real-world effects in another territorial jurisdiction.[64]

43. A state can exercise its sovereignty over cyber infrastructure within its territorial borders (and in relation to satellites, within its jurisdiction),[65] and over persons within its territory and with regard to its citizens, outside. The principle of sovereignty therefore does apply in relation to states' cyber activities, through the ability of a state to regulate such matters within its territorial borders and to exercise independent state powers.[66] As noted above, the principle has legal consequences.

44. States have the right to exercise their sovereign powers over cyber infrastructure in their territory exclusively and independently, as in the non-cyber context. These powers over cyber infrastructure are subject to states' obligations under international human rights law.[67] Some states choose to regulate certain aspects of cyber activity in their territory, for example through laws about the processing

[60] Increasingly state cyber activity takes place in relation to other state's territories through cyber infrastructure owned or controlled by powerful private companies such as Facebook or Google rather than by states, see Shapshak, T. (2019), 'Google and Facebook to Build Own Undersea Cables Around Africa', *Forbes*, 3 July 2019, https://www.forbes.com/sites/tobyshapshak/2019/07/03/google-and-facebook-to-build-own-undersea-cables-around-africa/ (accessed 4 Oct. 2019). Efrony and Shany argue that the deterritorialized and virtual aspects of cyberspace put in question the long-term sustainability of key assertions of the Tallinn Manual 2.0, Efrony and Shany (2018), 'A Rule Book on the Shelf?', p. 652.

[61] Yuan Yi for example has argued that it is unfair to use the geographic locations of cyber infrastructure, as in the Tallinn Manual 2.0, as the sole criterion to define network frontiers: 'If we applied this rule, much of the internet would be American territory and subject to US sovereignty, as most Internet root servers and many enterprise servers are located there': Zeng, J., Stevens, T., and Chen, Y. (2017), 'China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"', *Politics & Policy,* 45(3): pp. 432–464.

[62] Tsagourias (2018), 'Law, Borders and the Territorialisation of Cyberspace', p. 16.

[63] Buchan, R. (2018), *Cyber Espionage and International Law*, Hart Publishing, p. 50.

[64] Goldsmith, J. L. (1998), 'Against Cyberanarchy', *The University of Chicago Law Review,* 65(2): p. 32.

[65] Under the Outer Space Treaty, satellites remain under the jurisdiction of the nation that launched them. Thus, a state cyberattack that targeted another state's satellite in outer space could constitute interference with the sovereign functions of a state regardless of the fact that the satellite is located outside the state's territorial borders.

[66] The international group of experts involved in the Tallinn Manual 2.0 agreed that '[a] State enjoys sovereignty authority with regard to the cyber infrastructure… located within its territory', Schmitt (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 13. See also Tsagourias, N. (2019), 'The Slow Process of Normativizing Cyberspace', *AJIL Unbound*, 113: pp. 71–75, p. 73; Schmitt and Vihul (2017), 'Respect for Sovereignty in Cyberspace', *Texas Law Review*, 95(7): pp. 1639–1670.

[67] The UN Human Rights Council has held that human rights such as freedom of expression, freedom of assembly and privacy apply online as much as offline: Resolution on the Promotion and Protection and Enjoyment of Human Rights on the Internet, UN Doc A/HRC/20/L.13. One of the voluntary, non-binding norms for responsible state behaviour in the use of ICT technology agreed by the UN GGE in 2015 was that states should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the internet (para 13(e) of the UN GGE's 2015 report).

of personal data and permissible content on the internet.[68] Some authoritarian states exert tighter controls over access to the internet and personal data, a concept that has been referred to as 'cyber sovereignty'.[69] States that adopt a wide approach to the existence of their powers over all aspects of citizens' behaviour take a similarly wide view of the duties of other states to respect their sovereignty and may invoke violations of sovereignty or the non-intervention principle more regularly than others.[70] But the powers that states choose to assume under domestic law in relation to cyber activity (whether or not compatible with international human rights law) are a separate issue from the scope of a state's inherently sovereign functions.

> The principle of sovereignty therefore does apply in relation to states' cyber activities, through the ability of a state to regulate such matters within its territorial borders and to exercise independent state powers.

45. The content of 'inherently sovereign powers' or 'inherently governmental functions' is established in international law; the rules on state immunity provide one context.[71] Such functions are understood as activity at the very core of state authority, including the activities of the authorities responsible for foreign and military affairs; legislation and the exercise of police power; and the administration of justice. These functions do not include a state's regulation of the activities of private citizens or commercial matters. This approach is reflected in the *Nicaragua* case, in which the ICJ cited 'the choice of a political, economic, social and cultural system, and the formulation of foreign policy', as examples of matters in which a state could decide freely under the principle of state sovereignty. Thus, the term 'inherently sovereign functions' has to be given an objective reading.

III. Violation of sovereignty

46. When a state[72] exercises its authority[73] in another state's territory without consent in relation to an area over which the territorial state has the exclusive right to exercise its state powers independently, that constitutes a violation of sovereignty. This formulation is reflected in the international jurisprudence. The Permanent Court of International Justice (PCIJ) said in the *Lotus* case that the 'first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State'.[74]

[68] For example, Germany's Network Enforcement Act (known as NetzDG), and France's Law against the Manipulation of Information, which came into force on 23 December 2018.
[69] In China, the government considers that it should have sole jurisdiction over what content, data and services can be provided or accessed on the internet within the state's territory ('cyber sovereignty', manifested partly through the 'Great Firewall'). China has largely succeeded in controlling its citizens' access to cyberspace within its territorial boundaries, a model that is being copied in a number of other states. In November 2019, Russia enacted a law (known as the 'sovereign internet law') that introduces wide-ranging powers to restrict internet traffic within Russia.
[70] States' views on what reaches the threshold of a violation may also be informed by their own history and politics; for example, states with a colonial past have sometimes placed greater emphasis on sovereignty and non-intervention in international law than those that have not been colonized.
[71] Where the distinction between acts *jure imperii* and acts *jure gestionis* provides an analogy. See, for example, Fox, H. and Webb, P. (2015), *The Law of State Immunity*, 3rd edition, Oxford University Press, p. 399.
[72] 'State' here is intended to include state agents, state organs, or non-state actors and proxies if their actions can be attributed to the state under the rules on attribution set out in the ILC's Articles on State Responsibility.
[73] 'Authority' here refers to sovereignty in the sense of the supreme authority of the state, and is capable of covering all the elements discussed above. Oppenheim refers to a violation of 'another state's independence or territorial or personal authority', Oppenheim (1996), *Oppenheim's International Law, Vol. 1: Peace*, p. 385.
[74] *S. S. Lotus (France v Turkey),* Judgment, 7 September 1927, PCIJ (series A) No. 1, p. 18, emphasis added.

47. In *Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v. Nicaragua)*, the ICJ considered violation of territorial integrity and sovereignty to involve the exercise of authority in another state.[75] The court held that Nicaragua had violated the territorial sovereignty of Costa Rica by conducting certain activities on its territory without consent.[76] In *Military and Paramilitary Activities in and against Nicaragua*, the ICJ referred to 'the duty of every State to respect the territorial sovereignty of others'.[77] In the *Corfu Channel* case, the ICJ held that the UK violated Albania's sovereignty by routing warships and conducting demining operations in Albania's territorial waters without consent.[78] In each of these cases, the court considered violation of sovereignty separately from the rules on use of force and intervention, and considered it to have legal consequences.

Remote violations of sovereignty

48. Many examples of infringement of a state's sovereignty involve intrusions on physical space such as airspace, territorial waters, or exercise of political powers such as law enforcement. But a state can also violate another state's sovereignty by activity that the perpetrating state conducts outside the territory of the victim state and without physical effects in the affected territory. For example, FBI agents interrogate bankers in Switzerland by telephone without the consent of Switzerland by forcing them to complete a questionnaire under threat of subpoena if they do not. This is an exercise of authority in an area over which Switzerland has the exclusive right to conduct law enforcement activity. It could thus amount to interference in the exercise of Switzerland's independent state powers on its own territory, and thus a violation of Switzerland's sovereignty.

49. A state may also conduct activity from outside the territory with physical effects in the target state's territory. For example, a state allows its territory to be used for a factory that emits fumes into a neighbouring state polluting the latter state's rivers. The neighbouring state is unable to stop the fumes entering its territory and has to divert significant financial resources to provide alternative sources of water. Such harm is now dealt with generally under the separate head of environmental law, but duties in environmental law to avoid causing environmental harm in another state (however those are framed) have their roots in the principle of sovereignty.[79] In *Certain Activities carried out by Nicaragua*, the ICJ found that Nicaragua was responsible for a breach of sovereignty by reason of its physical incursions and then in a subsequent case fixed the amount of damages for environmental harm caused in Costa Rica by that breach.[80]

50. It may be more difficult in practice to establish violations of sovereignty that are conducted from outside the territory with effects in the territory, as the activity will be less tangible than the physical presence of an agent on the territory and may be harder to prove. Regardless of these potential

[75] *Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v Nicaragua),* Judgment, ICJ Reports 2015, paras 221–3: 'There is no evidence that Costa Rica exercised any authority on Nicaragua's territory or carried out any activity therein… Therefore, Nicaragua's claim concerning the violation of its territorial integrity and sovereignty must be dismissed'.
[76] Ibid., para 93, the ICJ found that 'Nicaragua carried out various activities in the disputed territory since 2010, including excavating three *caños* and establishing a military presence in parts of that territory. These activities were in breach of Costa Rica's territorial sovereignty'.
[77] Ibid., para 213.
[78] *Corfu Channel (UK v Albania)* Judgment (Merits) 1949 ICJ Rep 4, 9 April, 2015 Judgment, paras 69–70. States frequently conclude agreements to permit activity within one another's territory (such as Status of Forces Agreements, which typically authorize presence, manoeuvres, training, commercial activity etc). Without these, the sovereignty of the territorial state could be violated by the activity in question.
[79] In the *Trail Smelter* arbitration (Trail Smelter Arbitration (*United States v. Canada*), Arbitral Trib., 3 U.N. Rep. Int'l Arb. Awards 1905 (1941)), the US made a claim for violation of its sovereignty in respect of the damage caused by a smelter located on Canadian territory. The Tribunal did not refer explicitly to sovereignty in its judgment but did note that 'under the principles of international law… no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties of persons therein, when the case is of serious consequence and the injury established by clear and convincing evidence'.
[80] *Certain Activities carried out by Nicaragua in the Border Area (Costa Rica V. Nicaragua); Compensation Owed By The Republic Of Nicaragua To The Republic Of Costa Rica* judgment of 2 February 2018.

differences in application and proof, the same rules regarding violation of sovereignty apply whether the exercise of authority by the perpetrating state is carried out through a physical presence on the territory of the affected state or remotely from outside the affected territory. In practice, remote violations with a coercive element have tended to be considered through the lens of the non-intervention principle or via specific rules of international law that have developed.[81]

Is there a threshold to violations of sovereignty?

51. Some scholars consider sovereignty to be a 'catch-all' principle capturing any interference with a state's exclusive internal and external authority not included in more specific rules such as those on non-intervention or non-use of force.[82] Those taking this position assert that *any* non-consensual incursion by a state agent into the territory of another state can amount to an exercise of state authority sufficient to violate the territorial state's sovereignty, regardless of whether that incursion produces damage or otherwise breaches international or national law, and regardless of whether the exercise of authority is manifested through a physical presence on the territory or remotely.[83]

52. Others consider that not all exercises of authority carried out without consent that are not included in specific rules will amount to a violation of sovereignty. One area where the question of what is unlawful is not clear is in relation to the acts of states' intelligence agencies, which routinely operate on the territory of other states without being officially disclosed to the authorities. Certain scholars argue that territorially intrusive forms of espionage violate the principle of territorial sovereignty.[84] A major counterpoint to this argument is the ubiquity of states' intelligence agents in other states, usually without comment by the latter states. While states routinely outlaw forms of espionage under their domestic law, and while specific activities may provoke protest, for the most part the activities of intelligence agencies have not been treated by states or commentators as internationally unlawful per se.[85] Espionage is considered more fully in Chapter 4.[86]

53. The idea of a threshold for violation of sovereignty appears more obvious in the context of remote exercises of power by one state in relation to the sovereignty of another state's territory. The remote exercise of authority by one state usually affects the political independence of the victim state – as in the case of political or economic interference in another state's affairs, or the exercise of extraterritorial enforcement jurisdiction. Oppenheim observes that, 'independence is a question of degree',[87] and whether or not this aspect of sovereignty is violated will also be a question of degree. For example, diplomatic protests or mere criticism of a foreign government, or the issue of propaganda about

[81] See, for example, Higgins, R. (2009), 'Intervention and International Law', in *Themes and Theories: Selected Essays, Speeches and Writings in International Law, Vol. 1* (2009), OUP, pp. 275–5, discussing specific rules relevant to economic intervention. The non-intervention principle is considered in Chapter 3.
[82] Tsagourias (2018), 'Law, Borders and the Territorialisation of Cyberspace', p. 19. See also Watts, S. and Richard, T. (2018), 'Baseline Territorial Sovereignty and Cyberspace', *Lewis & Clark Law Review,* 22(3): pp. 803–872.
[83] Buchan (2018), *Cyber Espionage and International Law*, p. 51 ff.; Watts and Richard (2018), 'Baseline Territorial Sovereignty and Cyberspace', pp. 866–867.
[84] Buchan argues that a growing body of national court decisions support this, in particular *Re Canadian Security Intelligence Service Act* [2008] FC 301, in which the Federal Court of Canada refused to grant a warrant to the Canadian Security Intelligence Service to conduct espionage activities abroad on the basis that the activities would contravene international law. In refusing to issue the warrant, the Federal Court observed that the intrusive activities contemplated would 'clearly impinge upon the… principles of territorial sovereign equality and non-intervention' (*Re Canadian Security Intelligence Service Act* [2008] FC 301 paras 50–52), cited in *Cyber Espionage and International Law*, p. 52. Buchan also cites some cases from other national courts (at footnote 27) and statements by certain states objecting to the activities of the US's National Security Agency leaked by Snowden as a violation of their sovereignty (pp. 54–55).
[85] For a more detailed discussion, Huang, Z. and Mačák, K. (2017), 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches', *Chinese Journal of International Law*, 16(2): pp. 271–310, p. 303; Watts and Richard (2018), 'Baseline Territorial Sovereignty and Cyberspace', pp. 849–850.
[86] At paras 141–145.
[87] Oppenheim (1996), *Oppenheim's International Law, Vol. 1: Peace*, p. 391.

another state's government, will not violate the principle of sovereignty,[88] but the clandestine provision of financial and logistical support to another state's opposition party in an attempt to force the government from power may well do. The line between lawful diplomacy and violation of sovereignty is difficult to draw and it will be a fact-specific enquiry in each case.[89]

> The limits of the sovereignty rule are not established. It is not clear whether there is some form of *de minimis* rule in action, as evidenced by the way that states treat the activities of other states in practice.

54. In sum, the limits of the sovereignty rule are not established. It is not clear whether there is some form of *de minimis* rule in action, as evidenced by the way that states treat the activities of other states in practice. The assessment of whether sovereignty has been violated therefore has to be made on a case by case basis, if no other more specific rules of international law apply.

Violations of sovereignty in the cyber context

55. In the cyber context, some scholars argue that there is no specific rule of sovereignty with legal consequences. In their view, the differences in how sovereignty is reflected in international law with respect to the domains of space, air and the seas support the view that sovereignty is a principle, subject to adjustment depending on the domain and the practical imperatives of states rather than a hard and fast rule.[90] But it is clear from the case law above that it is possible for a state's sovereignty to be violated without reference to rules of international law dealing with specific areas, and that such violation amounts to the commission of an internationally wrongful act with legal consequences. As Specter has argued, 'Whether one chooses to call it sovereignty, or territorial sovereignty, or territorial integrity, or something else entirely, an overwhelming and unavoidable body of treaties, jurisprudence, and scholarly opinion stands for the proposition that there is a primary rule of international law that requires one state to refrain from taking public act or exercising authority in the territory of another state, in the absence of consent or another provision of international law to the contrary.'[91]

56. Rule 4 of the Tallinn Manual 2.0 states that 'A State must not conduct cyber operations that violate the sovereignty of another State'. This invites the question of *when* a state-sponsored cyber operation is in breach of a state's sovereignty.

57. One scenario is that unauthorized cyber activity is carried out by an agent of one state while physically present on the territory of another state.[92] A recent example is the attempted hack of the Organisation for the Prevention of Chemical Weapons (OPCW), based in The Hague in the Netherlands,

[88] Oppenheim (OUP 2008) Vol I, at p. 403 (para 122). Oppenheim states that 'intervention must neither be confounded with good offices, nor with mediation, nor with intercession, nor with co-operation, because none of these imply a dictatorial interference' [p. 222]; Jamnejad and Wood discuss rules relevant to allegedly interventionary activities of diplomats: Jamnejad, M. and Wood, M. (2009), 'The Principle of Non-intervention', *Leiden Journal of International Law*, 22(2): p. 364.

[89] Jamnejad and Wood when discussing the funding of political parties in another state, cite potential factors that may be relevant when assessing whether this kind of activity violates the non-intervention principle; ibid., pp. 368–9.

[90] For example, Corn and Taylor argue that 'Law and state practice … indicate 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'; Corn, G. P. and Taylor, R. (2017), 'Sovereignty in the Age of Cyber', *AJIL Unbound*, 111: p. 210.

[91] Spector, P. (2017), 'In Defense of Sovereignty, in the Wake of Tallinn 2.0', *AJIL Unbound*, 111: pp. 219–223; Ginsburg, T. (2017), 'Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0', *AJIL Unbound*, 111: p. 222. For a detailed discussion of the evidence in support of violation of sovereignty having legal consequences see Schmitt and Vihul (2017), 'Respect for Sovereignty in Cyberspace', p. 1649 ff.

[92] The Tallinn Manual 2.0 gives the example of one state using a USB flash drive to introduce malware into cyber infrastructure located in another state: para 6 of commentary to Rule 4, Schmitt (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

by Russia's military intelligence agency, the GRU. In April 2018, Russian intelligence officers had moved to a location close to the OPCW headquarters and were making preparations to hack into OPCW networks. In order to protect the integrity of the OPCW, the Netherlands Defence Intelligence and Security Service pre-empted the GRU cyber operation and escorted the Russian intelligence officers out of the Netherlands the same day. In this case, the non-intervention principle would appear not to be applicable, since the activity does not meet the requirement of coercion.[93] The Dutch minister of defence stated that 'GRU cyber operations such as this one are at odds with the international rule of law',[94] suggesting that the government considered the GRU's activity to be internationally wrongful, without specifying in what way.[95]

58. More often, state cyber intrusions are conducted remotely from outside the territory of the target state rather than by agents physically present within the affected state's territory.[96] As in the non-cyber context, the perpetrating state's remotely conducted cyber intrusion (for example, an agent hacking into and shutting down a state's national power grid from outside the victim state's territory) could be considered to be 'accessing' (without consent) the victim state's sovereign territory, if the affected server is located on the victim state's territory. Sometimes the remotely caused cyber intrusion will have physical effects on the territory, for example physical damage to a computer. Similarly, in the non-cyber context, transboundary environmental harm caused remotely can have physical effects in the affected state's territory. Sometimes there will be no physical footprint at all on the territory, for example, a state simply sitting on another state's server, gathering information; or using malware to alter data on a computer's hard drive without leaving a trace. The cyber intrusion nevertheless accesses infrastructure on the victim state's territory without the victim state's consent. As long as the servers affected are located in the victim state's territory (or in the case of satellites, within the jurisdiction of the affected state), then an unauthorized exercise of authority by one state by cyber means in another state's territory could constitute a violation of the victim state's sovereignty.[97]

> More often, state cyber intrusions are conducted remotely from outside the territory of the target state rather than by agents physically present within the affected state's territory.

59. This analysis proceeds on the basis that sovereignty is a bundle of rights that are inextricably linked. Cyber intrusions into another state's cyber infrastructure can involve interference with the affected state's exercise of its independent state powers in some way (for example disruption of the target state's ability to control its critical infrastructure or other independent state functions), but they also have a territorial dimension as the intrusions take place on the territory of the victim state. There

[93] Coercion is discussed at paras 84–103 below.
[94] Government of the Netherlands (2018), 'Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW', https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw (accessed 5 Oct. 2019).
[95] See also Global Affairs Canada (Canada's Foreign Ministry) citing inter alia the GRU attack on the OPCW, which stated that such activities 'underscore the Russian government's disregard for the rules-based international order, international law and established norms': Government of Canada (2018), 'Canada identifies malicious cyber-activity by Russia', *Canada Global Affairs*, https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html (accessed 5 Oct. 2019).
[96] As a reflection of this, the EU's restrictive measures against cyberattacks threatening the EU or its member states only focus on cyberattacks that originate from outside the EU.
[97] See in this regard Watts and Richards,'If one accepts that sovereignty is an aspect of the existing international law that States have conceded applies to cyberspace and if one accepts that sovereignty, at a minimum, protects states from interference with the independent and exclusive control of their territory by other States, the conclusion that interferences with cyber infrastructure violate sovereignty is not an especially difficult one to reach', Watts and Richards (2018), 'Baseline Territorial Sovereignty and Cyberspace', p. 866. The international group of experts involved in the Tallinn Manual 2.0 were in agreement that a cyber operation that interferes with data or services that are necessary for the exercise of inherently governmental functions is prohibited as a violation of sovereignty (and in some cases the prohibition of intervention), para 16 of commentary to Rule 4.

seems to be no reason in principle to distinguish physical violations (i.e. activity carried out by a state agent physically on the territory of the victim state) and remote violations (i.e. activity carried out from outside the affected state's territory).[98] Indeed, it would be strange to say that if a state agent shuts down another state's power grid while on the latter state's territory, that is a violation of sovereignty, but that the same would not be true if the perpetrating state did so by operating remotely.

Limits on the application of the sovereignty rule in the cyber context

60. As in the non-cyber context, there remains the question of whether *any* unauthorized exercise of authority in the affected state constitutes a violation of sovereignty or whether there is some form of *de minimis* threshold in operation. If one adopts the position of sovereignty as a 'catch-all', that makes the potential for violations very large indeed. On this view, it would technically be a violation of sovereignty and thus an internationally wrongful act for a state to install an access mechanism on another state's infrastructure without any interference with the functionality of the target state's cyber infrastructure; or to gather information for espionage purposes; or to undertake exploratory cyber activity by states looking to identify a weakness within the system that may be useful for a future attack.

61. This open-ended, maximally protective approach to violation of sovereignty in the cyber context appears to be at odds with the reality of states' day to day interactions in cyberspace. As Egan has observed, 'the very design of the internet may lead to some encroachment on other sovereign jurisdictions'.[99] The reality of the interconnected online world is that states constantly transit through each other's portals, often without explicit authorization, especially states' intelligence agencies. State cyber activity may 'access' other states' territory in a variety of ways including for 'virtuous' purposes such as the urgent defeat of a counterterrorism attack, without other states being aware, at least in real time. Under an open-ended approach to sovereignty, which we might term that of the 'pure sovereigntist', the sovereignty of states would technically be in a constant state of violation, with violations taking place with no response by states.

62. The pure sovereigntist might argue that in practice states have discretion as to whether they wish to frame such activity in the language of violation of sovereignty, or to deal with them in other ways, for example diplomatically or through domestic criminal law. But if such activities could indeed constitute violations of sovereignty, this could increase the risk of confrontation and escalation, since violation of sovereignty gives the affected state the right to take countermeasures in response if the perpetrating state fails to remedy the situation. It is also to be expected that states that claim a wide concept of sovereignty, including powerful cyber active states such as Russia and China, will invoke violations of sovereignty against other states' international activity of any kind more frequently than others. This is one of the problems of relying on an open-ended conception of sovereignty in this context. International law must be applied objectively, rather than sovereignty simply meaning whatever a state says it is, but the lack of any specific criteria for violations increases the risk of states interpreting sovereignty subjectively.

63. Where states have made statements regarding state cyber intrusions, they have not usually framed these intrusions as violations of sovereignty. It is not clear whether this is because the states concerned do not want to elevate the situation to this level (with the implication that the victim state is then

[98] International courts and commentators in the non-cyber context have treated the elements of sovereignty as inter-linked, para 37.
[99] Egan (2017), 'International law and stability in cyberspace', p. 13.

entitled to take countermeasures) or because they do not view the activity as a violation of sovereignty in the first place. The notion that all unauthorized exercises of state authority by cyber means constitute violations of sovereignty is not easily reconcilable with the day to day workings of states. Nor does it appear to correspond with current state practice.[100] On the other hand, the position that violation of sovereignty has no legal consequences at all in the cyber domain (below the threshold of the non-intervention principle) is difficult to reconcile with the judgments of international courts on the principle of sovereignty, which seem in principle capable of application to all unauthorized exercises of state authority, cyber or otherwise.[101]

Criteria to delineate violations of sovereignty

64. Perhaps recognizing the difficulties of a 'purist' approach to sovereignty, some commentators favour a kind of half-way house position, under which some state cyber activity violates another state's sovereignty but only if it reaches a certain threshold. The question then becomes what the criteria are for such a threshold – is it a *de minimis* threshold based on quantitative factors such as the scale of the harm in the target state, the number of citizens affected, or the geographic reach of the attack; or is it based on qualitative factors such as the nature of the attack – or both?

65. The international group of experts involved in the Tallinn Manual 2.0 explored whether it is possible to identify criteria for infringements of the target state's 'territorial integrity',[102] whereby remote cyber intrusions will only reach the level of violation of sovereignty where a certain level of harmful effects are caused on the territory of the victim state. They did so by reference to a hierarchy of scenarios, as follows:

- physical damage or injury (e.g. malware that causes the malfunctioning of the cooling elements of equipment, rendering components inoperable, as in the Stuxnet operation);[103]
- loss of functionality of cyber infrastructure (e.g. hacking into a computer and spreading a powerful virus that disables functionality, potentially also resulting in the need to replace computers, as in the 'Shamoon' cyber operation against the Saudi oil company, Aramco);[104] and
- activity below loss of functionality, e.g. the slowing down of a computer; causing the cyber infrastructure or programmes to operate differently; or altering or deleting data without physical or functional consequences.

66. This idea of a violation of sovereignty based on varying levels of harmful effect appears to have been at least partially inspired by discussion of an 'effects doctrine' in the context of the rules on the use of force, which the international group of experts also considered in the context of state-sponsored

[100] Although this may become clearer as more states put their views on record: the French government, in its report of September 2019, stated that *any* unauthorized cyber intrusions into the French system would constitute a violation of sovereignty, which implies a pure sovereigntist approach; see Roguski, P. (2019), 'France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I', *Opinio Juris*, 24 September 2019.
[101] See, for example, paras 29–32.
[102] It is submitted that the term 'territorial sovereignty' may be more appropriate here than violation of a state's 'territorial integrity', as the latter implies part of the territory being taken by another state, which does not fit well with the type of harm caused by state cyberattacks. It was also noted at para 37 that international courts and commentators in the non-cyber context have treated the elements of sovereignty as inter-linked, rather than breaking up sovereignty into separate elements, and there seems no reason not to take the same approach in the cyber context.
[103] The Stuxnet operation, uncovered in 2010, targeted an Iranian uranium enrichment facility, and resulted in physical damage to a significant number of nuclear centrifuges.
[104] The Shamoon virus, uncovered in 2012, overwrote the master boot record of infected computers, rendering the computers unusable thereafter.

cyberattacks.[105] In practice, physical damage to cyber infrastructure as a result of a cyber intrusion is much less common than loss of functionality or some effect below that, so the latter two criteria above will be the most important for the purpose of low-level cyber interventions.[106] But drawing the line for a *de minimis* threshold based on the effects in the target state raises a number of challenges.[107] The international group of experts took differing positions on where the line should be drawn, both in relation to the proposed criterion of 'loss of functionality'[108] and in relation to damage below loss of functionality.[109] The scenarios above mingle effects and the object/nature of the interference. They could be taken to imply a descending scale of severity, but in practice it is not so straightforward. The deletion of one state's critical government data by an outside state does not necessarily cause physical effects or loss of functionality but may be capable of having a more serious effect on the ability of the target state to exercise its state functions.[110] Should 'harm' caused by cyber interference be measured in quantitative or qualitative terms, or both?

> Certain states have posited that as well as severity, the scale of the effects on society may be a factor that they take into account when considering whether the cyberattack could constitute a violation of sovereignty.

67. It is currently unclear what most states think of the idea of an 'effects-based' approach to violations of sovereignty in cyberspace (beyond the UK position of not recognizing a rule of sovereignty in cyberspace) since, as noted above, few states have put their views on record. The French government, in its report of September 2019, as well as stating that any unauthorized cyber intrusions into the French system would constitute a violation of sovereignty, also indicated that sovereignty can be violated by 'any production of effects by cyber means on French territory'.[111] France's national cyber incident classification system is based on a technical and effects-based assessment of the cyber operation, graded according to gravity.[112] There are indications that other states are also seriously considering an effects-based approach. The government of the Netherlands alludes to limits to sovereignty in its recent statement on the application of sovereignty to cyberspace, and notes that 'in general' it endorses Rule 4 of the Tallinn Manual 2.0 'for determining the limits of sovereignty in the cyber domain'.[113] Certain states have posited that as well as severity, the scale of the effects on society may be a factor that they take into account when considering whether the cyberattack could constitute a violation of sovereignty.[114] Others have focused on the practical effects on the victim state's ability to regulate its sovereign functions on its territory.[115]

[105] Commentary to Rule 69 of the Tallinn Manual 2.0. Schmitt has proposed that the criteria used to decide whether a cyberattack constitutes a use of force should be focused predominantly on the consequences of the attack. The first of his seven proposed criteria is severity, i.e. the level of destruction caused by the attack. Under this criterion, the scope, duration and intensity of the attack are taken into consideration.
[106] The Stuxnet operation is a relatively rare example of the causation of physical damage.
[107] See Schmitt, M. N. (2017), 'Grey Zones in the International Law of Cyberspace', *The Yale Journal of International Law*, 42(2): p. 11, referring to a 'confusing melange of views' on this issue. Von Heinegg, W. H. (2012), 'Legal Implications of Territorial Sovereignty in Cyberspace', 2012 4th *International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, p. 5, states that 'if … there is no or merely minor material damage to the cyber infrastructure it is not really settled whether that activity can be considered a violation of sovereignty'.
[108] The international group of experts involved in the Tallinn Manual 2.0 could not agree on the threshold at which cyber intrusions that result in a loss of functionality could qualify as a violation of sovereignty: Tallinn Manual 2.0, pp. 20–21, para 13 of commentary to Rule 4.
[109] Below the threshold of loss of functionality, there was also no agreement among the experts: ibid., para 14 of the commentary to Rule 4.
[110] For example in 2012, Iran's oil production was targeted by the 'Wiper' virus, which systematically scrubbed hard drives clean, deleting the malware's code with it.
[111] Ministère des Armées (2019), 'Droit International Applique Aux Operations Dans Le Cyberspace'.
[112] Roguski (2019), 'France's Declaration on International Law in Cyberspace', notes that the cyber incident in question is assessed on the basis of the actual or intended impact on the fundamental interests of the nation (sovereignty; democracy; territorial integrity); internal and civilian security; the availability of fundamental services to the population (water supplies, electricity, healthcare) and the economy.
[113] 'It should be noted that the precise limits of what is allowed and what is not allowed have not been fully crystallized', Minister of the Netherlands (2019), 'Statement to parliament on 5 July 2019'.
[114] Views given informally by government representatives in workshops held to discuss drafts of this paper.
[115] Ibid. This is an amalgam of the two different bases used for violation of sovereignty in the Tallinn Manual 2.0, i.e. territorial integrity and usurpation of government functions.

68. The idea of an effects-based approach in relation to state cyber activity from outside the territory with harmful effects in another territory is also one that the EU has recently adopted in relation to its newly enacted cyber sanctions regime.[116] The sanctions are aimed at cyberattacks that have a (potentially) 'significant effect', and which constitute an external threat to the EU or its member states. The EU decision lists the following as the factors determining whether a cyberattack has a significant effect:

a. the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety;
b. the number of natural or legal persons, entities or bodies affected;
c. the number of Member States affected;
d. the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;
e. the economic benefit gained by the perpetrator, for himself or for others;
f. the amount or nature of data stolen or the scale of the data breaches; or
g. the nature of commercially sensitive data accessed.[117]

69. While the EU decision does not refer to sovereignty or intervention, it is an interesting example of states creating criteria for the wrongfulness of cyber activity based on a wide-ranging list of factors, both quantitative and qualitative. Note that the reference to 'scope, scale, impact or severity of disruption caused' is linked, in (a) above, to the carrying out by the state of inherently state functions, such as economic and societal activities; essential services; critical state functions; public order; or public safety. This causal link between behaviour that has a certain scope, scale, impact or severity and the carrying out by the state of its exclusive and independent state functions is quite close to the idea of violation of sovereignty (i.e. the unauthorized exercise of authority regarding another state's sovereign functions) being subject to certain effects. However, the EU criteria are clearly broader, going beyond scale and effect to encompass, for example, economic loss and the type of data stolen.

70. An approach based on quantitative and/or qualitative effects in the target state, or some other form of *de minimis* threshold, is attractive from a practical and pragmatic point of view as it enables states to take action in relation to cyber intrusions that may not reach the threshold of intervention but that nevertheless cause harmful effects within the territory. It has the merit of being neither too restrictive (as the pure sovereigntist position arguably is) nor too permissive (in catching activity that does not require the establishment of coercive behaviour as in the non-intervention principle).

71. The difficulty is that as noted above, outside the cyber context it is hard to define parameters or criteria for what constitutes a violation of sovereignty, beyond the general formula of an exercise of authority by one state in another's territory without consent in relation to an area over which the territorial state itself has the exclusive right to exercise state powers independently.[118] A pure sovereigntist would argue that scale and effects may inform norms such as those regarding intervention and use of force but have no place in relation to sovereignty, and that effects are rather a matter related to enforcement and the proportionality of remedies. On the other hand, it has been noted that remote

[116] EU Council (2019), EU Council decision (CFSP) 7299/19 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 14 May 2019, https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf (accessed 6 Oct. 2019).
[117] Ibid., Article 3.
[118] Para 54.

violations are often analysed as a matter of degree.[119] But the matter is not clear or settled, and the lack of agreement on whether there is a *de minimis* threshold for violations of sovereignty in the non-cyber context is just as apparent in the cyber context.

72. As yet, there also appears to be no agreement as to what kinds of effects would be required under a *de minimis* threshold. The Tallinn Manual 2.0 formula, which imports a doctrine based on severity of effects derived from the rules on use of force, is one version; another is the practical effects on the victim state's ability to exercise its independent state powers over society (which is close to how the non-intervention principle operates in practice). The EU's restrictive measures offer a range of other factors to consider in the context of regulating remotely conducted cyberattacks based on significant effect. Even those that argue that breach of sovereignty is subject to some threshold (whom we might term for the purposes of this paper 'relative sovereigntists') concede that agreement on the criteria for delineating violations is currently lacking.[120] Until such agreement is reached between states, determination of when a violation of sovereignty occurs risks becoming a subjective exercise as opposed to one based on a mutually agreed interpretation of the application of sovereignty in cyberspace.

Proving violation of sovereignty in the cyber context

73. Establishing whether sovereignty has been violated in a particular case is complicated by the fact that states have differing views as to what constitutes a violation. Even if an approach based on some kind of threshold is accepted, the analysis is more challenging still because of the peculiar attributes of cyberspace. As the government of the Netherlands has pointed out, it is possible that a single cyber operation is made up of different components or actions that are initiated from different countries or that run through different countries, often simultaneously, in a way that cannot always be traced.[121] There are various options for masking both the identity of the perpetrator and the geographical origin of the cyber activity, especially now that data is often stored in a cloud system in different locations. In practice, it is therefore not always possible to determine whether a cyber operation has a cross-border element, such that it may violate the sovereignty of a particular state.[122]

III. Due diligence

74. International law requires that a state may not knowingly allow its territory to be used for mounting hostile, including terrorist, activities against another state.[123] In the cyber context, it has been argued that this obligation applies so as to require a state to exercise due diligence to prevent harmful cyber activities emanating from that state's territory.[124] The contrary argument is that in the

[119] Para 53.
[120] See, for example, Biller, J. and Schmitt, M. (2018), 'Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences', *EJIL Talk!,* 24 October 2018, https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/ (accessed 23 Oct. 2019).
[121] Minister of the Netherlands (2019), 'Statement to parliament on 5 July 2019'.
[122] Ibid.
[123] In the *Corfu Channel* case, the ICJ affirmed 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States', p. 22. See also the *Trail Smelter* arbitration where the tribunal stated that 'a State owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction', p. 1963. Oppenheim, however, indicates that, 'Such limited international judicial consideration of the issues involved, while affording sound guidance as to the underlying principles, is insufficient to regulate increasingly complex situations' in Oppenheim (1996), *Oppenheim's International Law, Vol. 1: Peace*, p. 409.
[124] Rule 6 of the Tallinn Manual 2.0 provides that 'a State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States'.

cyber context there is no legal obligation but that applying due diligence would be good practice.[125] Since the latter argument is contained in the UN GGE, it is indicative of at least some states' opinion that in the cyber context there is no legally binding obligation.[126] At the same time, there is state support for the *desirability* of its application, and some states are beginning to take the view that it is indeed now a binding principle in the cybersphere.[127]

75. Crucially, though, the difference between 'shall' and 'should' is not yet of great practical importance. This is because it is currently unclear what the application of the due diligence principle to cyberspace would in fact require. For its application to a particular context, the principle in effect must be comprised of a number of smaller duties,[128] and, in relation to cyberspace, states are yet to elucidate what those 'sub-duties' would be.[129] For example, would due diligence involve obligations to undertake investigation or simply to respond to identified activity, to review and secure use of cyberspace from within the state's territory, to share information with other states? It should also be stressed that the principle is one of conduct, not result: it is not a duty to prevent harmful cyber activity, but to take reasonable steps to attempt to do so.

76. Nonetheless, there are potential advantages in the application of due diligence to cyber activities, both in terms of developing a preventive rather a than merely responsive approach, and in lessening the issues associated with the attribution of cyber activity to a state.[130] Due diligence therefore is an area where the development of principles as to what might be expected of a state in applying the principle would be welcome, and further work is needed before the principle can be called in aid.

[125] The 2015 consensus report of the UN GGE show that states agreed that they 'should' exercise due diligence: UN A/70/174, para 13(c). See also 2013 report of the UN GGE, UN A/68/98, para 23. See also EU Council Decision, preambular para 4, concerning restrictive measures against cyberattacks threatening the Union or its member states, which states that '[States] should seek to ensure that their territory is not used by non-State actors to commit such acts'.

[126] In this regard, a distinction should be made between acts conducted on a state's territory that have significant harmful effects on another state(s), of which the territorial state clearly had knowledge and the ability and opportunity to prevent on the one hand, and on the other hand a general duty of vigilance over any act by a non-state actor or individual that might have an effect on another state. See also Chircop, L. (2018), 'A Due Diligence Standard of Attribution in Cyberspace', *ICLQ,* 67(3): pp. 665–668.

[127] For example, France and the Netherlands (as set out in official statements at footnotes 42 and 43). See Schmitt, M. (2019), 'France's Major Statement on International Law and Cyber: An Assessment', *Just Security*, 16 September 2019; Jensen, E. T. and Watts, S. A. (2017), 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', *Texas Law Review*, 95: pp. 1555–1577.

[128] Sklerov, M. J. (2009), 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent', *Military Law Review,* 201: pp. 1–85.

[129] Having said this, as long ago as 2000, the UN General Assembly 'not[ed] the value of' states taking various measures that could be required under a duty of due diligence in the cyber context: GA Res. 55/63 (4 December 2000).

[130] See Green, J. A. (2016), 'Disasters Caused in Cyberspace', in Breau, S. C. and Samuel, K. L. H. (eds) (2016), *Research Handbook on Disasters and International Law,* Edward Elgar, pp. 406–427.

3. The Application of the Non-intervention Principle in Cyberspace

77. The non-intervention principle is the corollary of every state's right to sovereignty, territorial integrity and political independence.[131] It derives from and safeguards the general principle of sovereignty. The members of the UN GGE accepted that the prohibition on non-intervention applies in principle to states' cyber operations in another state below the threshold of use of force. This chapter analyses the principle and considers how it applies to states' cyber operations.

> The members of the UN GGE accepted that the prohibition on non-intervention applies in principle to states' cyber operations in another state below the threshold of use of force.

78. The 1970 Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the UN (Friendly Relations Declaration) provides that:

> No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of another State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.[132]

79. The prohibition on intervention is an inter-state doctrine, and does not apply to intervention by or in relation to the activities of non-state groups unless the activities of the non-state groups can be attributed to a state under the rules of attribution in international law.[133] The principle is set out in many international law sources,[134] and is grounded in Article 2(7) of the Charter, which prohibits the UN from intervening in 'matters which are essentially within the jurisdiction of any state'. The ICJ said in *Nicaragua* that the non-intervention principle is 'part and parcel of customary international law', notwithstanding the fact that 'examples of trespass against this principle are not infrequent'.[135]

80. Despite being codified in various international agreements and documents, the prohibition on non-intervention has been described by scholars as vague and 'elusive'.[136] It applies both to interventions by force and non-forcible interventions, but its content is not clearly defined outside the context of use of force.

---

[131] Oppenheim (1996), *Oppenheim's International Law, Vol. 1: Peace,* p. 428.
[132] Friendly Relations Declaration, UN General Assembly, 1970.
[133] See, in particular, Part One, Chapter II of the ILC's Articles on State Responsibility.
[134] The principle is included in the constituent instruments of regional organizations, as well as in other multilateral and bilateral treaties. It is reflected in the Charter of the Organization of American States (Article 3); the Charter of Organization of African Unity (Article III(2); and the Charter of ASEAN (Article 2(2)(e) and (f)), among others. It has also been reflected in numerous declarations adopted by international organizations and conferences including resolutions of the General Assembly from the mid-1960s to 1980s, during which there was disagreement between states over the scope of the principle. The Final Act of the Conference on Security and Co-operation in Europe (the Helsinki Final Act, 1 August 1975) includes a detailed statement of the principle (Principle VI). The non-intervention principle has been frequently promoted in documents by non-Western states, including the Bandung Principles (agreed between 29 countries from Asia and Africa in 1955 at the Bandung Conference), and China's Five Principles of Peaceful Co-Existence.
[135] *Certain Activities Carried Out By Nicaragua In The Border Area (Costa Rica V. Nicaragua)*, para 202.
[136] Lowe, V. (2007), *International Law*, Oxford University Press, p. 104.

81. Nevertheless, the ICJ in *Nicaragua* provided some useful guidance. The ICJ held that the non-intervention principle (outside the context of use of force) applies to one state's actions in relation to another state where two elements are present:

i. coercion by one state of another state;

ii. in relation to 'matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy'.[137]

82. The ICJ's dicta on the non-intervention prohibition in *Nicaragua* should not be read prescriptively since the ICJ was clear that, 'the Court will only define those aspects of the principle which appear to be relevant to the resolution of the dispute'.[138] Since the dispute in question primarily concerned forcible intervention, the court did not opine in any detail on how intervention and coercion might be defined outside the use of force context. Outside the area of use of force, 'it is often unclear what is, and what is not, prohibited under customary international law. Much depends on context, and even on the state of relations between the states concerned'.[139]

83. The terms 'interference' and 'intervention' are sometimes used interchangeably; for example, China's Five Principles of Peaceful Co-Existence include 'mutual respect for sovereignty and territorial integrity' and 'non-interference in each other's internal affairs'.[140] This paper uses the term 'intervention' in the sense of coercive intervention in the internal or external affairs of another state.[141] The two elements of the non-intervention principle are analyzed below.

I. Coercion

84. Under the non-intervention principle, the coercion must take place in relation to 'matters of an inherently sovereign nature', i.e. those over which the state has exclusive authority, including a state's political, economic, social and cultural systems. The non-intervention principle, insofar as it concerns non-forcible interventions, thus relates to the element of sovereignty under which states are entitled to exercise their state powers independently and free from interference from other states.[142] It follows that the main difference between violation of the non-intervention prohibition and other breaches of sovereignty is the element of coercion. This accords with the judgment of the ICJ in *Nicaragua*, in which the court noted that:

> Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones… the element of coercion… defines, *and indeed forms the very essence of,* prohibited intervention.[143]

[137] *Nicaragua*, para 205.
[138] Ibid.
[139] Jamnejad and Wood (2009), 'The Principle of Non-intervention', p. 367.
[140] Some commentators have also noted that the debates on the non-intervention principle that led up to the approval of the Helsinki Final Act suggest that Russia considered non-intervention to be interchangeable with 'non-interference'. The word used in the Russian-language version of the Final Act – 'невмешательство' – conveys a broader meaning, encompassing both non-intervention and non-interference. By contrast, Western states considered that non-intervention was prohibited but activity below that threshold – mere 'interference' was not. The Helsinki Act represented a compromise between these different concepts of intervention. See Raynova, D. (2017), 'Towards a Common Understanding of the Non-Intervention Principle', *European Leadership Network*, Post Workshop Report, https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/170929-ELN-Workshop-Report-Non-Intervention.pdf (accessed 24 Oct. 2019).
[141] This reflects the definition of intervention in Oppenheim's International Law (Vol. 1: Peace): 'the interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question. Interference pure and simple is not intervention', p. 432.
[142] The Friendly Relations Declaration provides that, 'No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it *the subordination of the exercise of its sovereign rights*' (emphasis added).
[143] *Nicaragua*, para 205 (emphasis added).

85. Coercion regulates the line between minor interference and unfriendly acts on the one hand, and intervention sufficient to breach the prohibition on non-intervention on the other.[144] The line between the two is not always easy to identify, particularly because there is no generally accepted definition of 'coercion' in international law.[145] Nevertheless it is possible to identify certain features of what is meant by 'coercion' from the international law sources.

Coercion involves the application of pressure

86. The requirement of coercion involves an element of pressure or compulsion on the part of the coercing state. Without this requirement for a degree of pressure, the line between coercion and mere attempts to influence would become blurred. The degree of pressure that is required to deprive the target state of control of its state functions will vary in each case according to the facts, and cannot be quantified.[146] But clearly a certain amount of pressure is required, and Jamnejad and Wood note that 'if the pressure is such that it could be reasonably resisted, the sovereign will of the target state has not been subordinated'.[147] As a result, 'Only acts of a certain magnitude are likely to qualify as coercive'.[148]

87. An example of concern that attempts merely to influence should not be regarded as coercion can be seen in the statement made by the UK on adoption of the Friendly Relations Declaration in the UN General Assembly:

> In considering the scope of 'Intervention', it should be recognized that in an interdependent world, it is inevitable and desirable that States will be concerned with and will seek to influence the actions and policies of other States, and that the objective of international law is not to prevent such activity but rather to ensure that it is compatible with the sovereign equality of States and self-determination of their peoples.[149]

88. Coercion is sometimes associated with dictatorial behaviour by one state in relation to another: 'do x or else'. Oppenheim for example states that, '… to constitute intervention the interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question'.[150] Outside the international law context, coercion is often characterized as a threat that is used in order to change the *conscious* behaviour of the target.[151] The power of the threat is predicated on the fact that the target knows that it is being coerced, and will

[144] Jamnejad and Wood note that the requirement of coercion 'removes minor international friction' and 'is a crucial limit in the principle of non-intervention. Without it, any act which had an effect on another state could fall within the prohibition'; Jamnejad and Wood (2009), 'The Principle of Non-intervention', p. 381. Higgins argues that, 'The purpose of the international law doctrine of intervention is… to provide an acceptable balance between the sovereign equality and independence of states on the one hand and the reality of an interdependent world and the international law commitment to human dignity on the other'; Higgins (2009), 'Intervention and International Law', p. 273.

[145] For a survey of coercion as it arises in different contexts in international law, and the problems of defining it, see Tzanakopoulos, A. (2015), 'The Right to be Free from Economic Coercion', *Cambridge Journal of International and Comparative Law,* 4(3): pp. 618–623.

[146] Some commentators have suggested that the pressure needs to be extensive. Ziolkowski for example states that 'scholars assert that illegal coercion implies "massive influence"' but this will depend on the circumstances in each case, Ziolkowski, K. (2013), 'General Principles of International Law as Applicable in Cyberspace', in Ziolkowski, K. (ed) (2013), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, Tallinn, Estonia: NATO CCD COE Publication, p. 165.

[147] Jamnejad and Wood (2009), 'The Principle of Non-intervention', p. 348. Dickinson argues that coercion is present if it 'cannot be terminated at the pleasure of the state that is subject to the intervention': Dickinson, E. D. (1920), *The Equality of States in International Law*, Harvard University Press, p. 260.

[148] Jamnejad and Wood (2009), 'The Principle of Non-intervention', p. 348.

[149] Statement of Sir Ian Sinclair on behalf of the UK government (1966), Official Records of the General Assembly, 25th session, UN Doc A/AC.125/SR.114, Supplement No. 18 (A/8018), 155.

[150] Oppenheim (1996), *Oppenheim's International Law, Vol. 1.* p. 432. See also Jamnejad and Wood, who argue that 'only those that are intended to force a policy change in the target state will contravene the principle', Jamnejad and Wood (2009), 'The Principle of Non-intervention', p. 348.

[151] See, for example, Wertheimer, A. (1987), *Coercion*, Princeton University Press, who advocates that coercion should be understood as a situation in which the coercer's proposal creates a choice situation for the target, such that the target has 'no reasonable alternative but to do X'; p. 172; and Nozick argues that coercion involves a threat by one actor to another that if the target does not do a certain action, then negative consequences will follow, Nozick, R. (1969),'Coercion', in Morgenbesser, W. (ed)(1969), *Philosophy, Science and Method: Essays in Honor of Ernest Nagel*, St Martin's Press, pp. 440–472.

suffer consequences if it does not respond as the coercer wishes, rather like blackmail. But the international law sources discussed above suggest that coercion in the international law context is framed rather differently, in the sense of the application of pressure by one state to influence an outcome in, or conduct with respect to, a matter reserved to the sovereign state. This characterization of coercion is derived from the overarching principle of sovereignty in international law, and the notion of an unauthorized exercise of authority in relation to the target state's exercise of independent and exclusive powers on its territory. Analogies with coercion outside the international law context therefore need to be treated with care.

> In practice, the means and techniques used by a state to coerce another state in relation to the exercise of the latter's state powers can be various and nuanced.

89. In practice, the means and techniques used by a state to coerce another state in relation to the exercise of the latter's state powers can be various and nuanced. Damrosch argues that, 'The traditional formulation of intervention as "dictatorial interference" resulting in the "subordination of the will" of one sovereign to another is … unsatisfactory, because some subtle techniques of political influence may be as effective as cruder forms of domination'.[152] Oppenheim, when referring to intervention as interference that is forcible or dictatorial, adds 'or otherwise coercive', implying that the nature of coercion can in fact take a range of forms.[153]

Coercion is directed at securing a benefit for the perpetrating state

90. The Friendly Relations Declaration provides that 'No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights *and to secure from it advantages of any kind*'.[154] This suggests that the pressure must be directed towards affecting the behaviour of the target state in some way to the benefit of the perpetrating state. There are different formulations of what the coercive behaviour is designed to achieve. Is it the application of pressure:

- simply to usurp or undermine the target state's ability to exercise its exclusive state functions independently?
- or must it, in attempting to deprive the target state of its free will over its sovereign functions, seek to compel an outcome in, or conduct with respect to, the target state's exercise of those functions?
- or must it specifically try to force the target state into a change of government policy in some respect?

[152] Damrosch, L. F. (1989), 'Politics Across Borders: Non-intervention and Non-forcible Influence over Domestic Affairs', *The American Journal of International Law,* 83(1): p. 5.
[153] Tsagourias argues that there are multiple ways in which 'coercion' can be exerted for the purposes of the non-intervention principle, Tsagourias, N. (forthcoming 2020), 'Cyber intervention and international law' in Broeders, D. and Van den Berg, B. (2020), *Governing Cyberspace: Behaviour, Power and Diplomacy*, Rowman & Littlefield, p. 10.
[154] Friendly Relations Declaration.

91. The international law sources on the non-intervention principle do not specifically refer to a requirement for the intervention to be directed towards a change of policy or government. The Friendly Relations Declaration refers to the 'securing of advantages';[155] Oppenheim refers to '…interference in the affairs of another State *for the purpose of maintaining or altering the actual condition of things*',[156] including the right of a state to 'adopt any Constitution it likes, arrange its administration in a way it thinks fit, and make use of legislature as it pleases'.[157] The ICJ in *Nicaragua* stated that intervention is wrongful 'when it uses methods of coercion in regard to such choices… which must remain free ones'.

92. The language in each of the above sources suggests that the coercive behaviour could extend beyond forcing a change of policy to other aims, such as preventing the target state from implementing a policy or restraining its ability to exercise its state powers in some way. At the same time, as noted above, the attempt to deprive the target state of its free will over its sovereign powers is carried out for the benefit of the perpetrating state in some way: the unauthorized exercise of authority is not incidental. The benefit sought need not relate to a specific policy issue; it may suffice for the target state's control over the underlying policy area to be impaired in a way that adversely affects the target state.[158] In light of this, the coercive behaviour is perhaps best described as pressure applied by one state to deprive the target state of its free will in relation to the exercise of its sovereign rights in an attempt to compel an outcome in, or conduct with respect to, a matter reserved to the target state.

93. The *Nicaragua* case suggests that coercive behaviour can be direct as well as indirect.[159] The ICJ determined that US funding of the contras constituted intervention, notwithstanding that a series of intervening events were required after the US transfer of funds took place and before coercion of the Sandinista regime of Nicaragua occurred. The court adopted a more nuanced approach to understanding both coercive behaviour and intervention than simply direct, dictatorial behaviour.

Coercion in the cyber context

94. Some scholars writing in the cyber context have understood coercion in the sense of dictatorial action by a state to force a change of policy and on the basis of this 'narrow coercion standard' have concluded that the threshold for the non-intervention principle is a high one[160] that needs reformulating in the cyber context.[161] Others have argued that the non-intervention threshold is seldom reached, and advocate that as a result greater reliance should be placed on the sovereignty principle.[162]

[155] Ibid., p. 5. This formula is reiterated in similar form in a number of UN General Assembly resolutions and in the Charter of the Organization of American States (Article 20).
[156] Oppenheim, L. (1920–21), Oppenheim's International Law, Vol. 1: Peace, 3rd edn, Roxburgh, R. F. (ed.), London: Longmans, p. 221; Buchan (2018), *Cyber Espionage and International Law*, similarly argues that coercion 'subordinates the will of the state in order for the entity exercising coercion *to realise certain objectives'* (emphasis added), p. 63.
[157] Ibid., p. 207.
[158] Kunig argues that intervention 'aims to impose certain conduct of consequence on a sovereign state', Kunig, P. (2008), 'Intervention, Prohibition of', *Max Planck Encyclopedia of Public International Law*, p. 5.
[159] *Nicaragua*, para 205.
[160] Kilovaty, I. (2019), 'The Elephant in the Room: Coercion', *AJIL Unbound,* 113: pp. 89–90. Ziolkowski argues that, 'coercion occurs only in drastic cases of overwhelming (direct or indirect) force being put upon a State's free and sovereign decision-making process', Ziolkowski, K. (2013), 'General Principles of International Law as Applicable in Cyberspace'.
[161] Ibid., p. 87; Kilovaty argues that cyber operations are distinct in their effects from their physical counterparts and require a more nuanced definition of non-intervention that departs from the 'narrow coercion standard', Kilovaty, I. (2018), 'Doxfare: Politically motivated leaks and the future of the norm of non-intervention in the era of weaponized information', *Harvard National Security Journal,* 9: p. 168 ff.
[162] Schmitt and Vihul argue that 'the prohibition on intervention and the use of force… contain thresholds that are seldom reached. Thus the vast majority of hostile cyber operations attributable to states implicate only the prohibition of violation of sovereignty': Schmitt and Vihul (2017), 'Sovereignty in Cyberspace: Lex Lata Vel Non?', p. 214.

95. But there seems no reason why a flexible approach to coercion should not apply in the cyber context, as in the non-cyber context. Several scholars writing in the cyber context have supported the idea of coercion as meaning coercive behaviour aimed at seeking an advantage of some kind by depriving the target state of its free will over the exercise of its sovereign powers. Watts, for example, argues that 'actions *merely restricting a state's choice* with respect to a course of action or compelling a course of action may be sufficient to amount to violations of the principle of non-intervention'.[163] Gill defines intervention as '[A]ction aimed at coercing a State to do *or abstain from doing* something it is entitled to do under international law'.[164]

96. The examples of non-intervention in the Tallinn Manual 2.0 involve forcing a particular policy decision on the target state, for example 'the use by one State of non-cyber coercive means to compel another State to adopt particular domestic legislation related to Internet server liability', or using such means to compel another state 'to refrain from becoming Party to a multilateral treaty dealing with cyber disarmament or human rights online'.[165] But the Tallinn Manual 2.0's definition of coercion in fact supports a broader understanding of coercion, which could include restraining a state from exercising its state functions more broadly, as well as forcing it to act in a particular way: 'an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner *or involuntarily refrain from acting* in a particular way'.[166] The majority of the international experts involved in the Tallinn Manual 2.0 were also of the view that 'the coercive effort must be designed to influence outcomes in, or conduct with respect to, a matter reserved to a target state'.[167]

> Coercive behaviour is perhaps best described as pressure applied by one state to deprive the target state of its free will in relation to the exercise of its sovereign rights in an attempt to compel an outcome in, or conduct with respect to, a matter reserved to the target state.

97. The Australian government's position on the application of the non-intervention principle in the cyber context reflects this more nuanced understanding of coercive behaviour, defining a prohibited intervention as:

> …one that interferes by *coercive means (in the sense that they effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature),* either directly or indirectly, in matters that a state is permitted by the principle of state sovereignty to decide freely. Such matters include a state's economic, political and social systems, and foreign policy.[168]

[163] Watts, S. (2015), 'Low-Intensity Cyber Operations and the Principle of Non-Intervention,' in Ohlin, J. D., Govern, K. and Finkelstein, C. (2015), *Cyber War: Law and Ethics for Virtual Conflicts,* Oxford University Press, p. 256, emphasis added.
[164] Gill, T. (2013), 'Non-Intervention in the Cyber Context' in Ziolkowski, K. (ed) (2013), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, Tallinn, Estonia: NATO CCD COE Publication, p. 222.
[165] Para 2 of commentary to Rule 66 of the Tallinn Manual 2.0.
[166] Ibid., para 18 of commentary to Rule 66 (emphasis added). The examples given of coercion in the Tallinn Manual 2.0 are based on forcing a change in policy (e.g. the use by one state of a distributed denial of service operation to coerce a government into reversing a decision about the official language after a referendum) – para 9 of commentary to Rule 66. But a minority of the international group of experts involved in the Tallinn Manual 2.0 considered that the coercion requirement is satisfied when 'an act has the effect of depriving the State of control over the matter in question', para 19 of commentary to Rule 66.
[167] The Tallinn Manual 2.0 states that 'coercion must be distinguished from persuasion, criticism, public diplomacy, propaganda… retribution, mere maliciousness, and the like in the sense that, unlike coercion, such activities merely involve either influencing (as distinct from factually compelling) the voluntary actions of the target State; para 21 of the commentary to Rule 66.
[168] 2019 International Law Supplement to Australia's International Cyber Engagement Strategy, p. 2, emphasis added.

98. Coercive behaviour may thus be understood as pressure applied by one state to deprive the target state of its free will in relation to the exercise of its sovereign rights in an attempt to compel an outcome in, or conduct with respect to, a matter reserved to the target state. This could have quite significant implications when applied in the cyber context. It would capture the use by a state of covert cyber operations with the aim of disrupting or undermining the exercise of another government's sovereign functions. The very inability of the target state to exercise control over its sovereign functions, with the harmful effects that are likely to ensue within the target state as a result, is the outcome that the perpetrating state is seeking to compel. There are many examples where states have used cyber operations in this way, for example attacks on another state's critical infrastructure in order to punish or retaliate against that state.

Intent, motive or purpose

99. The formula for coercion suggested above reflects the fact that states will usually have a reason for applying pressure to another state in relation to the exercise of its sovereign functions. But it does not go so far as to require a specific intent, motive or purpose on the part of the coercing state in seeking to compel an outcome or conduct in the target state. In the *Nicaragua* case, the ICJ noted evidence that the US intended to overthrow the government of Nicaragua and intended to inflict economic damage. But the court declined to make findings with respect to the intentions or motives of the US, observing that:

> in international law, if one State, with a view to the coercion of another State, supports and assists armed bands in that State whose purpose is to overthrow the government of that State, that amounts to an intervention by the one State in the internal affairs of the other, whether or not the political objective of the State giving such support and assistance is equally far-reaching.[169]

100. The court's ruling suggests that the motive of the intervening state is of little relevance. It is the *fact* of coercive behaviour with respect to the victim state's free will over its sovereign functions that establishes a prohibited intervention.[170] The coercive behaviour on the part of the perpetrating state will, by its nature, be intentional, and thus the description of coercion discussed above necessarily involves an intention to compel an outcome or conduct.[171]

Must the coercive behaviour succeed?

101. A violation of sovereignty usually involves actual usurpation of a state's sovereign powers by another state without consent.[172] But under the non-intervention principle, it is the fact of the coercive behaviour itself, in relation to another state's sovereign powers, that matters. This suggests that if the hostile state carries out coercive cyber operations against another state but does not succeed, it would still be caught by the non-intervention principle, just as an act involving a use of force that misses its target would still constitute a use of force. Potential as well as actual effects are therefore relevant

[169] *Nicaragua*, para 241.
[170] Watts (2015), 'Low-Intensity Cyber Operations and the Principle of Non-Intervention', p. 268. See also the *Armed Activities (DRC v Uganda)* case, in which the ICJ held that Ugandan training and military support for rebels operating in the territory of the DRC constituted a violation of the principle of non-intervention but made no determination on Uganda's motive for supporting the rebels, Judgment, ICJ Reports 2005, p. 168, para 163.
[171] Intent, motive and purpose do not generally play a part in the international rules on state responsibility, although it will depend on the content of the primary obligation in question. See para 3 of the Commentary to Article 2 of the ILC's Articles on State Responsibility, and para 10: 'In the absence of any specific requirement of a mental element in terms of the primary obligation, it is only the act of the State that matters, independently of any intention'.
[172] The international group of experts involved in the Tallinn Manual 2.0 considered that in order for there to be a violation of sovereignty, consequences must manifest (para 24 of the commentary to Rule 4).

when assessing the coercion element. Otherwise, a state that was targeted but, being well prepared, was not affected, could not claim a violation of international law, whereas a state that had not invested in such protections could.[173]

102. Since actual harmful effects are not a prerequisite for the non-intervention principle to be engaged, the element of coercion is better understood as the fact of 'coercive behaviour' by a state in relation to another state's sovereign functions, which does not presuppose the success of the behaviour, rather than 'coercion'. Some argue that coercion is essentially about the conduct on the part of the perpetrating state rather than the effects that such behaviour produces.[174] Others, in assessing whether the non-intervention principle has been breached, place greater weight on the effects (actual or potential) of the behaviour on the target state's inherently sovereign functions.[175] In a sense, both conduct and effects are relevant: it is the fact of the coercive behaviour that is important, but (based on the definition at para 92 above) there is a close causal link between the coercive behaviour and its actual or potential effects on the target state's free will to exercise control over its sovereign functions. To the extent that harmful effects do ensue, they may also provide evidence of the coercive behaviour, and will be relevant in assessing the proportionality of any response by the target state under international law. It is also worth noting that although potential rather than actual effects may suffice, it will be harder to evidence intervention where it is not possible to show practical effects on the ability of the target state to carry out its sovereign functions.

103. In the cyber context, the coercive behaviour of the perpetrating state is usually covert. The question arises as to whether the target state needs to know that it is being coerced in order for the coercion element to be established. If it is the fact of the coercive behaviour by the perpetrating state that establishes coercion, and if the coercion does not have to succeed in order to be unlawful, then it is not necessary for the target to know about it. The coercive behaviour is in itself enough.[176]

II. 'Matters in which a state is permitted to decide freely'

104. For the non-intervention principle to be breached, there must be a causal nexus between the coercive behaviour on the one hand and the deprivation, or attempted deprivation, of the victim state's authority in relation to the exercise of its state functions on the other. This connection is reflected in the ICJ's dicta in *Nicaragua* that:

> A prohibited intervention must … be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.[177]

105. The Tallinn Manual 2.0 and some scholars writing in the cyber context have equated the concept of a state's inherently sovereign functions, for the purposes of the non-intervention principle, with what is known as *domaine réservé*,[178] i.e. a state's internal affairs, or a sphere of activity that is 'not,

[173] The international group of experts involved in the Tallinn Manual 2.0 considered that the fact that a coercive cyber operation fails to produce the desired outcome has no bearing on whether the non-intervention principle has been breached (para 29 of the commentary to Rule 66).
[174] The international group of experts involved in the Tallinn Manual 2.0 appear to take this view; ibid.
[175] See, for example, Watts (2015), 'Low-intensity cyber operations and the principle of non-intervention', p. 256.
[176] The majority of the international group of experts involved in the Tallinn Manual 2.0 considered that knowledge of coercion was not required on the part of the target state: para 25 of the commentary to Rule 66.
[177] *Nicaragua*, para 205.
[178] Tallinn Manual 2.0, para 22 of the commentary to Rule 4. See also Schmitt (2017), 'Grey Zones in the International Law of Cyberspace', p. 7; Watts (2015), 'Low intensity cyber operations', pp. 263–5.

in principle, regulated by international law'.[179] The Tallinn Manual 2.0 states that 'usurpation of an inherently government function' (discussed in the context of violation of sovereignty) differs from intervention in that the former deals with inherently governmental functions, whereas the latter (intervention) involves the *domaine réservé*, 'concepts that overlap to a degree but that are not identical'.[180] It has been argued that the scope of a state's *domaine réservé* is increasingly limited because there are hardly any topics or policy areas today that are inherently removed from the international sphere.[181] This has contributed to a perception by some that the non-intervention principle has a relatively narrow application.

106. Even if international law has some bearing on the policy area in which a state exercises its state functions, the state may still retain ultimate authority over the area in question. Thus, international regulation of a subject does not remove it entirely from the *domaine réservé*; states retain independent authority to make choices among various lawful courses of action on a subject regulated by international law. For example, while international human rights law has had an impact on how states must interpret their policies on asylum, this does not mean that the conduct of these activities does not – to some extent – fall within the state's sovereign powers. Even when a state is found to be in breach of its human rights obligations, for example, it retains the prerogative of implementing that adverse decision – the prerogative of responsibility – and thus the initiative in the matter.[182]

107. In any event, since the non-intervention principle derives from and is a reflection of the principle of sovereignty, the better view is that there are not two different standards of matters reserved to a state.[183] The notion of *domaine réservé* is not particularly helpful in the non-intervention context. It concerns a state's domestic jurisdiction, which, as noted above, is to be distinguished from a state's inherently sovereign functions.[184] It also does not include a state's external affairs, which, as the ICJ made clear in *Nicaragua*, form part of the scope of the non-intervention principle.[185] A better understanding of a state's sovereign functions for the purposes of the non-intervention principle can be derived from the *Nicaragua* case and the Friendly Relations Declaration, in which state functions are characterized as including a state's choice of political, economic, social and cultural system, as well as the formulation of foreign policy.[186] The scope of a state's inherently sovereign functions is thus quite broad, extending to the making of state policies in these areas through its organs and agencies of a legislative, executive and judicial kind.

108. While the scope of a state's sovereign powers may be quite broad, state-sponsored cyber operations with effects on individuals or companies will not (without more) engage the non-intervention principle; it is only if the attack in question has an effect on the state's exclusive exercise of its independent sovereign functions. This approach corresponds with the public statements issued by states to date in

[179] *Nationality Decrees Issued in Tunis and Morocco (French Zone) on November 8th, 1921 (Great Britain v France)* Advisory Opinion, (1923) PCIJ Series B no 4, 7th February 1923, in which the PCIJ held that the scope of *domaine réservé* depends on the state of international relations, and whether or not a certain matter is or is not solely within the jurisdiction of a state is essentially a relative question (para 24).
[180] Tallinn Manual 2.0, para 22 of commentary to Rule 4. No further explanation is given.
[181] Ziegler, K. S. (2013), 'Domaine Réservé', *Max Planck Encyclopedia of Public International Law*, Section C: 'The Reduction of the Domaine Réservé'.
[182] Crawford, J. (2012), 'Sovereignty as a legal value', in Crawford, J. and Koskenniemi, M. (eds) (2012), *The Cambridge Companion to International Law*, Cambridge University Press, p. 122, doi:10.1017/CCO9781139035651.009. The PCIJ, in its 1923 *Wimbledon* decision, stated that rather than being an abandonment of sovereignty, 'the right of entering into international agreements is an attribute of State sovereignty': The *Wimbledon (Government of his Britannic Majesty v German Empire)* PCIJ Series A No 1 at para 25; see also *Lotus* at para 18. On the relationship between sovereignty and human rights, see also Besson, S. (2011), 'Sovereignty', *Max Planck Encyclopedia of Public International Law*, paras 130–140.
[183] The international group of experts involved in the Tallinn Manual 2.0 elsewhere appear to agree that there is only one standard. See para 8 of the commentary to the rule on intervention (Rule 66), which notes that they 'thought that the range of protection offered by Rule 66 on non-intervention is broadly coextensive with the range of issues reserved to states by the international law principle of sovereignty'.
[184] Paras 44 above.
[185] *Nicaragua*, para 205.
[186] There is also an analogy with the international rules on state immunity; see para 45 above.

relation to unauthorized state cyber activity in another state's territory. States have so far only invoked a violation of international law where there are practical effects on the ability of the victim state to exercise its inherently sovereign powers. A GRU campaign of indiscriminate and reckless cyberattacks above disrupted (among other targets) transport systems in Ukraine and was described by the UK as being 'in flagrant violation of international law'.[187] Likewise, in relation to the NotPetya attack, attributed by multiple states to Russia in February 2018,[188] the UK said that it 'showed a … disregard for Ukrainian sovereignty' in targeting the Ukrainian government, financial and energy sectors.[189] By contrast, the UK and US did not mention violation of international law in relation to the spear phishing[190] campaign aimed at private universities, private companies and NGOs, which they attributed to Iran in March 2018.[191] In relation to the WannaCry ransomware attack attributed to North Korean actors in December 2017, the UK, US and Australia stated this to be a 'criminal use of cyber space' rather than a violation of international law.[192]

> States have so far only invoked a violation of international law where there are practical effects on the ability of the victim state to exercise its inherently sovereign powers.

109. These recent statements suggest a developing distinction between activities that affect a state's ability to run its core state 'systems' generally (e.g. parliament; financial sector; energy; transport) and those activities that target individuals or private companies. This distinction is also reflected in the EU's recent issue of restrictive measures against cyberattacks threatening the EU or its member states. In describing which cyberattacks fall within the scope of the measures, the EU refers to 'financial market infrastructure'; 'digital infrastructure'; 'critical infrastructure' and 'any other sector', as well as 'critical State functions',[193] all of which suggest that the measures are directed at cyber operations that affect whole sectors, as opposed to cyberattacks on private individuals and private companies.

Proving intervention

110. In order to determine whether the non-intervention principle has been breached, the target state will need to assess whether it has been the victim of an attempt by another state to deprive it of its free will in relation to the exercise of its sovereign rights with a view to compelling an outcome in, or conduct with respect to, an inherently sovereign matter. In doing so, the target state will need to consider whether there is evidence of the application of pressure by the hostile state.

[187] National Cyber Security Centre (2018), 'Reckless Campaign of Cyber Attacks by Russian Military Intelligence Exposed', 3 October 2018, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed (accessed 24 Oct. 2019). The attribution was made by the UK, US, Australia, Canada, New Zealand, the Netherlands and Germany, and supported by Czech Republic, Denmark, Estonia, Finland, France, Latvia, Japan, Norway, Poland, Romania, Slovakia, Sweden, Ukraine, the EU and NATO.
[188] The attribution was made by the UK, US, Australia, Canada and Denmark, and supported by New Zealand, Estonia, Finland, Latvia, Lithuania, Netherlands, Norway and Sweden.
[189] Statement of Foreign Office Minister, Lord Ahmad (2018), 'Foreign Office Minister condemns Russia for NotPetya attacks', https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (accessed 5 Oct. 2019).
[190] 'Spear phishing' is a targeted attempt to steal sensitive information.
[191] Statement of Foreign Office Minister, Lord Ahmad (2018), 'Foreign Office Minister condemns criminal actors based in Iran for cyber-attacks against UK universities', https://www.gov.uk/government/news/foreign-office-minister-condemns-criminal-actors-based-in-iran-for-cyber-attacks-against-uk-universities (accessed 5 Oct. 2019). The US issued indictments of the alleged perpetrators, United States Department of Justice (2018), 'Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps', https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic (accessed 5 Oct. 2019). Both governments treated the cyber intrusion as criminal activity under their domestic law.
[192] Statement of Foreign Office Minister, Lord Ahmad (2017), 'Foreign Office Minister condemns North Korean actor for WannaCry attacks', https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks (accessed 5 Oct. 2019). New Zealand, Denmark and Japan supported this attribution.
[193] Council Decision (CFSP) 2019/7299/19 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Article 4.

111. As with violation of sovereignty, the particular features of cyberspace make it challenging to make these assessments as the activity is usually covert, with the perpetrator hiding their identity, and conducted remotely from outside the territory. The evidence of who is carrying out the attack (non-state actor or state agent; and if the former, whether the non-state actor is acting on behalf of a state), for what purpose, and the relationship if any between the perpetrating state's activity and the affected state's government's functions may not at first be evident. It will require careful investigation and, if the activity is conducted outside the target state, may require cooperation with international partners. In assessing whether a state is applying pressure in order to compel an outcome or conduct, the circumstances, including the political context, the history and relationship between the target state and alleged perpetrating state, and the wider circumstances are all likely to be relevant.

112. Certain other factors may also assist in identifying whether coercive behaviour is present, including the intensity of the attack and nature of the state interests affected by the cyber intrusion. The scale and severity of the effects of the cyber intrusion may also be relevant, including the reach in terms of the number of actors involuntarily affected by the cyber operation at issue.[194] If the cyber intrusion concerns the disabling of critical state infrastructure for example, it may be more likely to be coercive because such an attack would necessarily have a practical effect on the free will of the target state to exercise its sovereign functions exclusively and effectively over that infrastructure. Given the link between coercion and sovereign powers, arguably the more 'inherently sovereign' the area under attack, the easier it will be to establish intervention overall.

113. While the non-intervention principle is well established in international law, and clearly applicable to cyber activities as it is to other state activities, there does not appear to be complete agreement, as we have seen, on the criteria for its application. Case studies, which are increasingly prevalent now that states are becoming more vocal about state-sponsored cyber intrusions, are useful in discussing the application of the principle.[195] The next chapter considers specific scenarios in order to explore how the law discussed in chapters 2 and 3 can be applied to state-sponsored cyber intrusions in practice.

[194] Watts (2015), 'Low-Intensity Cyber Operations and the Principle of Non-Intervention', p. 257, quoting McDougal, M. S., and Feliciano, F. P. (1958), 'International Coercion and World Public Order: The General Principles of the Law of War', *The Yale Law Journal*, 67(5): p. 771. McDougal and Feliciano argued that coercion determinations should account for 'consequentiality', and proposed three dimensions of consequentiality, including 'the importance and number of values affected, the extent to which such values are affected, and the number of participants whose values are so affected', p. 782.

[195] Some scholarly initiatives also provide case studies of state-sponsored cyber intrusions into another state, to which international law can be applied: Efrony and Shany (2018), 'A Rule Book on the Shelf?'; NATO cyber toolkit, NATO CCDCOE (n.d.), 'Cyber Law Toolkit'.

4. Application of the Law to Case Studies

114. This section considers where the boundaries of an internationally wrongful act might lie with reference to practical examples, whether on the basis of a violation of sovereignty, breach of the principle of non-intervention, or both. Whether or not there is an unlawful act will inevitably depend heavily on the facts in question, and this section does not purport to provide concrete answers in each case. Rather, it uses examples to assist in the analysis and to explore the extent to which there may be an overlap between violation of sovereignty and violation of the non-intervention principle in practice.

I. Examples to explore the scope of a state's 'inherently sovereign functions'

115. The following examples explore the boundaries of where a state's 'inherently sovereign functions' might lie, in the context of states' cyber activities in another state. This issue arises in the context of both violation of sovereignty and the non-intervention principle.

Do a state's inherently sovereign powers extend to the activities of private citizens?

i. A state agent hacks into a computer belonging to a private company in another state in order to extract a ransom. The control and authority over the computer are with the private company that owns the computer. The computer and its contents have no relationship with the state's exercise of its powers save for such purposes as criminal law enforcement. It was noted in chapters 2 and 3 above[196] that a state's inherently sovereign powers relate to areas over which a state has exclusive control, including state infrastructure, rather than the activities of private citizens. If this is correct, such cyber activity would not violate the independent powers of the state in which the computer is located and neither could the activity be construed as intervention, regardless of whether it is coercive.

ii. A state agent remotely shuts down the operation of a dominant internet platform provider (such as Facebook) in another state, such that the entire population of the latter state is unable to access the platform for three days. It is an isolated incident without effects on the host state beyond inconvenience to its citizens. On the basis of the above, only if the shutting down of the company in question had a direct effect on the territorial state's exercise of its inherently sovereign functions would the state-sponsored cyber activities constitute a violation of the territorial state's sovereignty and (if the activity is coercive) also the non-intervention rule.[197] If, for example, the platform provider operated a portal on which a significant proportion of the population were exclusively dependent to submit welfare claims, that could be regarded as constituting a violation of sovereignty and the non-intervention principle.

[196] Paras 45 and 107.
[197] The international group of experts involved in the Tallinn Manual 2.0 discussed whether precluding or impeding citizens' access to some or all of the internet could violate sovereignty. They concluded that it would only do so to the extent that it usurped or interfered with inherently governmental functions, para 21 of commentary to Rule 4.

116. As noted in Chapter 2, states that adopt a wide approach to the existence of their powers over all aspects of citizens' behaviour are more likely to invoke violation of sovereignty in relation to incursions of any kind by other states.[198] Such states may take the view that the non-consensual shutting down of an internet company's activities on its territory constitutes a violation of their sovereignty – or 'cyber sovereignty'.[199] But if the activity targeted is that of a private citizen or company, it will not fall within a state's 'inherently sovereign functions', as that is established in international law.[200] This is one of the difficulties of analysing these issues through the prism of sovereignty, particularly if violation of sovereignty is conceived as open-ended, without limitative criteria.

Cyber intrusion in relation to a single commercial entity or attacks directed at a financial system as a whole

117. The ICJ stated in *Nicaragua* that a state's choice of its economic system is a matter in which each state is permitted to decide freely. But it was also noted above that the activities of individuals and companies within a state – including in those states that control almost all aspects of their economy – do not fall within the remit of a state's 'inherently governmental functions' for the purposes of international law.[201]

118. Thus, if a state-sponsored cyberattack is directed at a single commercial entity such as a private bank, on the analysis in chapters 2 and 3 this would not engage the state's inherently sovereign functions because it is a private entity rather than a whole sector falling exclusively within the government's powers.[202] Government statements regarding cyber intrusions on the financial sector (albeit by only a few Western states) support this approach, treating such intrusions as private and as a breach of criminal law rather than international law. For example, in 2014, the Sands Casino in the US suffered a cyberattack, which is suspected to have been carried out by Iran.[203] Notwithstanding the extensive damage done to the operation of the company concerned (including the wiping of hard drives and the permanent erasure of a vast quantity of essential data), the US did not frame the operation as a violation of international law; the FBI investigated it in conjunction with local state police, but no further action was taken.[204] This kind of activity would be a criminal act under the domestic law of almost any country, and would be subject to lawful measures of law enforcement, which might include seizure of criminally gained assets, arrest or a request for extradition. It would not constitute either a violation of sovereignty or an act of prohibited intervention because it lacks the requisite state-to-state relationship.

119. A less clear-cut case is the cyberattack in November 2014 on Sony Pictures. Sony's US affiliate was hacked and confidential data extracted from its servers, followed by the release of a huge quantity of personal data about the company's executives and new productions that had yet to be released. More than 70 per cent of Sony's computers were rendered inoperable by the malware and the company had to invest tens of millions of dollars in IT infrastructure repairs. Evidence suggests that the motive for the attack was to persuade Sony not to release a film ('The Interview') about North

[198] Para 44.
[199] States' views of what is meant by sovereignty – in the context of their powers over the internet and its content within their territory – are increasingly divergent; Wright, K. (2019), 'The 'splinternet' is already here', *TechCrunch*, http://social.techcrunch.com/2019/03/13/the-splinternet-is-already-here/ (accessed 7 Oct. 2019).
[200] Para 45.
[201] This is reflected in the 'relative approach' to state immunity rules applied by international courts and tribunals.
[202] Para 45.
[203] Efrony and Shany (2018), 'A Rule Book on the Shelf?', p. 605.
[204] Ibid.

Korea, to which North Korea objected.[205] The US attributed the cyberattack to North Korea. It may be argued that the incident constitutes an exercise of law enforcement power on the part of North Korea (assuming that criticizing North Korea's leader, Kim Jong-un, is a criminal offence there) on another state's territory with far-reaching effects. That would fit the definition of violation of sovereignty used above.[206] The attack would arguably also constitute an act of intervention if the purpose was to coerce the US to force Sony from engaging in criticism of North Korea or its leader in the future. Certainly the US government considered the incident significant enough to respond with sanctions and possibly covert cyberattacks in response.[207] One US official was reported as stating that the intrusion crossed a threshold from 'website defacement and digital graffiti' to an attack on computer infrastructure.[208] Secretary of State John Kerry, in discussing the attack, did not refer to a specific aspect of international law, but did say that the hack 'violated international norms'.

120. There are certain factors that may indicate when a state's malicious cyber activity is more likely to be treated as falling within the target state's inherently sovereign functions rather than being merely criminal activity. When a state refers to another state hacking into 'systems' or 'infrastructure', as opposed to referring to the target as a single private bank or company, this suggests behaviour that goes to the heart of a state's exclusive and independent state powers rather than simply a criminal attack.

> The harm sustained by US financial institutions targeted by the [2011–13 distributed denial of service] operation ran into tens of millions of dollars as a result of severe interruptions to their business activities.

121. Where the cyber intrusion is directed at disrupting the national bank or federal reserve of another state, over which the target state exerts sovereign authority, the target state's authority will be directly engaged, and thus the principle of sovereignty or non-intervention will be potentially violated.[209] An example of state cyber intrusion that targeted an entire financial sector rather than merely an individual financial institution was the 2011–13 distributed denial of service[210] campaign that Iran conducted against the US financial sector. This involved a sophisticated, globally distributed network of compromised computer systems (a botnet), reaching a cumulative total of 176 days of attacks. The harm sustained by US financial institutions targeted by the operation ran into tens of millions of dollars as a result of severe interruptions to their business activities. The attacks were attributed to Iran by the US, and certain individuals involved were indicted by the US government in 2016 for attacking critical infrastructure.[211] In this case, there was evidence to suggest coercive behaviour that reaches the threshold of an intervention, i.e. the application of pressure to deprive the US of its free will over its economy with a view to compelling an outcome in the target state. As a result, there is a case to be made that the

[205] For details of this incident, see Efrony and Shany (2018), 'A Rule Book on the Shelf?', pp. 604–605.
[206] Para 48.
[207] Efrony and Shany note that in December 2014, North Korea's internet network was shut down for nine hours and connectivity became intermittent for the next two days. The disruption has been assumed to constitute an unofficial response to the Sony hack, p. 608.
[208] Ibid., p. 607.
[209] The UK's attorney general stated that in the UK's view, cyber operations to intervene in the stability of the UK's financial system 'must surely be a breach of the prohibition on intervention in the domestic affairs of states', Wright (2018), 'Cyber and International Law in the 21st Century'.
[210] A Distributed Denial of Service attack is a malicious attempt to disrupt normal traffic to a web server.
[211] United States Department of Justice (2019), 'Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector', https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged (accessed 7 Oct. 2019). The suspected motive was a response to US and Israel's Stuxnet attack on Iran in 2010 to disable Iran's nuclear centrifuges. Eventually the series of attacks ended in the last months of 2013, as a result of a decision of the Iranian authorities 'probably due to progress in multilateral nuclear talks and the prospect of lifting economic sanctions against Iran'; Efrony and Shany (2018), 'A Rule Book on the Shelf?', p. 600.

cyber activity could have reached the threshold of intervention. In terms of violation of sovereignty, even if an effects-based approach is adopted (as opposed to the maximally protective position under which any cyber intrusion into another state's territory can violate sovereignty), the extensive effects on the US financial sector as a whole suggest that it could also be argued to be a violation of the US's sovereignty.

122. A cyber intrusion directed at a single commercial entity could potentially cause the host state to lose its ability to control its economy as a whole, for example if it were to lead to a run on the banks that requires the government to intervene with corrective measures to balance the economy in response. In this case, too, violation of sovereignty may be implicated, because the practical effect of the unauthorized exercise of authority (by cyber means) by the perpetrating state is to usurp the target state's sovereign functions (control of the economy), regardless of whether the activity was coercive. Increasingly, states link the maintenance of their economic security with their national security, which may increase the likelihood that state-sponsored cyber intrusions on a state's financial sector could be perceived by victim states as an intrusion on their sovereign power to maintain public order.

II. Examples exploring the boundaries of coercive behaviour

123. This section looks at examples where the state cyberattack is directed at functions in another state that are generally accepted to fall within the scope of a state's 'inherently sovereign functions'. It therefore focuses primarily on whether or not such activity is coercive for the purposes of that principle.

Cyber operations to manipulate another state's elections

124. The administration of free and fair elections falls within the inherently sovereign functions of a democratic state.[212] State-sponsored election interference by cyber means can broadly be divided into two categories: (i) cyber interference with election infrastructure; and (ii) cyber operations to manipulate voting behaviour. Each is examined below.

Cyber interference with election infrastructure

125. There are a number of ways in which a state could use cyber operations to manipulate another country's electoral infrastructure: for example, a hacking operation that tampers with the election results; changing the status of voters on the roll so that their vote is listed only as provisional; or deleting voters' names from the electoral roll. There are many examples of such activity: in 2014 cyberattackers accessed the computer of Ukraine's Central Election Commission and changed the result of the presidential election to show the winner as a far-right candidate; in 2016, the website of Ghana's Central Election Commission was hacked and false results announced from the Commission's Twitter account while votes were still being counted.

126. If the perpetrating state attempts to alter the results in order to put pressure on the target state to compel an outcome (such as the election result, or fall-out from that result) this would appear to be coercive and thus to meet the criteria for breach of the non-intervention principle. Brian Egan, then legal adviser to the US government, highlighted an example of a clear violation of international law as 'a cyber operation by a State that interferes with another country's ability to hold an election

[212] The ICJ stated in *Nicaragua* that one of the matters in which a sovereign state may decide freely is 'the choice of political system', para 205.

or that manipulates another country's election results'.[213] The UK's then attorney general stated that an example of the practical application of the non-intervention principle would be 'the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state',[214] and Australia had adopted the same position.[215] Others consider that an operation rendering election-related cyber infrastructure incapable of performing its functions would qualify as a violation of sovereignty.[216]

127. In response to cyberattacks on their election infrastructure, some states have designated their electoral infrastructure as critical national infrastructure.[217] This brings electoral infrastructure within the scope of the consensus report of the 2015 UN GGE,[218] which states that nations should not conduct or support cyber-activity that intentionally damages or impairs the operation of critical infrastructure in providing services to the public.

Cyber operations to manipulate voting behaviour

128. States have peddled propaganda in other states for centuries. The advent of the internet has made this easier, for example through the use of bots operated from outside the territory to circulate posts on social media about a particular electoral candidate without the consent of the target state.[219] In the non-cyber context, if the information circulated as propaganda is factual and neutral, such activity has not usually been considered to be a breach of the non-intervention principle.[220]

129. However, if the information spread is not factually accurate but rather disinformation (i.e. false or manipulated information, which is knowingly shared to cause harm), for example through the covert use of 'deep fakes'[221] or the micro-targeting and trolling[222] of voters using bots and fake Twitter accounts, then the likelihood that such activity could interfere with a democratic state's inherent right to run free and fair elections increases. International human rights law provides one framework for addressing the micro-targeting of individuals with propaganda, including the right to freedom of expression, the right to privacy, the right to freedom of thought and opinion, and the right to a free and fair election, as well as domestic regulation of social media in elections.[223] The right to self-determination, which refers to the right of peoples to determine freely and without external interference their political status and to pursue freely their economic, social and cultural development, is also relevant, and some have noted the link between that right and the principle of non-intervention.[224]

---

[213] Egan, B. (2016), 'Remarks on International Law and Stability in Cyberspace', https://2009-2017.state.gov/s/l/releases/remarks/264303.htm (accessed 4 Mar. 2019).
[214] Wright (2018), 'Cyber and International Law in the 21st Century'. The then Foreign Secretary Jeremy Hunt echoed this view in May 2019: 'We must be crystal clear that any cyber operations designed to manipulate another country's electoral system and alter the result would breach international law – and justify a proportionate response', Hunt, J. (2019), 'NATO Cyber Defence Pledge conference: Foreign Secretary's speech', https://www.gov.uk/government/speeches/foreign-secretary-speech-at-the-nato-cyber-pledge-conference (accessed 7 Oct. 2019).
[215] Australian Government Department of Foreign Affairs and Trade (2019), 'Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace'.
[216] Schmitt, M. (2018), "Virtual' disenfranchisement: cyber election meddling in the grey zones of election law', *Chicago Journal of International Law*, 19(1): p. 11.
[217] For example, the US: Congressional Research Service (2019), 'The Designation of Election Systems as Critical Infrastructure', 18 September 2019, https://fas.org/sgp/crs/misc/IF10677.pdf (accessed 14 Oct. 2019).
[218] UN Doc A/70/174.
[219] See, for example, New Knowledge (2018), 'The Disinformation Report', https://www.yonder.co/articles/the-disinformation-report/ (accessed 25 Oct. 2019). This report was prepared for the US Senate Select Committee on Intelligence on the use of cyber operations by Russia's Internet Research Agency to interfere in the 2016 US Presidential election.
[220] See Jamnejad and Wood (2009), 'The Principle of Non-intervention', p. 374.
[221] A technique for creating fake videos or audio clips using human image synthesis based on artificial intelligence.
[222] 'Trolling' involves intentionally antagonizing others online by posting inflammatory, irrelevant or offensive comments, or other disruptive content.
[223] See Jones, K. (2019), *Online Disinformation and Political Discourse: Applying a Human Rights Framework*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/publication/online-disinformation-and-political-discourse-applying-human-rights-framework.
[224] Tsagourias, N. (forthcoming 2020), 'Electoral Cyber Interference', p. 14, quoting Crawford ('the principle of self-determination is represented by the rule against intervention in the internal affairs of that state'); Ohlin, J. (2016), 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *Texas Law Review*, 95(7).

130. Coercive efforts to manipulate voting behaviour could also amount to intervention in another state's affairs, on the basis that the attempt to manipulate the will of the people also amounts to an attempt to undermine the target state's sovereign will over its choice of political system, which, as the ICJ in *Nicaragua* observed, is a sovereign right.[225] The covert element of disinformation contributes to the fact that the target state is unable to hold elections that are 'free and fair', because rather than there being a free marketplace of ideas, voters are being specifically targeted with information without necessarily being aware of this, nor that the targeting is based on personal data held by the targeting state. The deceptive nature of the cyber activity distinguishes it from a mere influence operation.[226] By contrast, official statements that seek to steer another government's population on a matter may be perceived as propaganda but if they are open and factually correct then they would be less likely to violate the principle of non-intervention because the target state would still have the free will to respond.

Coercive efforts to manipulate voting behaviour could also amount to intervention in another state's affairs, on the basis that the attempt to manipulate the will of the people also amounts to an attempt to undermine the target state's sovereign will over its own political system.

131. The cyber intrusions into the 2016 US presidential campaign involved a state hacking into the computer system of the Democratic National Committee (DNC) and publishing large quantities of written material about Hillary Clinton on Wikileaks, including almost 20,000 emails and 8,000 attachments written by key staff members of the DNC dated 2015–16.[227] The US Director of National Intelligence published a report finding that Russia's President Putin ordered the activity in order to 'undermine faith in the US democratic process, denigrate Secretary Clinton and harm her electability and potential presidency'.[228] If the definition of coercion in this paper is adopted, there is no need for the coercive behaviour to be successful – i.e. for the information actually to have changed people's minds as to whom they voted for, which is difficult to prove either way. It is the fact of coercive behaviour in relation to another state's sovereign functions that is required, rather than the ultimate result. Where a state uses covert cyber operations to influence what the target population thinks about certain candidates, it could also be argued that the perpetrating state by implication is seeking to compel an outcome – the inability of the target state to maintain an open democratic space in which to conduct free and fair elections. On this basis, it is possible that such state behaviour may reach the threshold of coercion.[229]

132. If the cyber intrusion does not reach the level of coercion, the issue arises as to whether it could nevertheless violate the affected state's sovereignty. A pure sovereigntist may argue that it could, on the basis that it is an unauthorized intrusion into another state's territory by cyber means. A relative

[225] Tsagourias (forthcoming 2020), 'Electoral Cyber Interference', p. 17, 'the intervening State controls not only the attitudes, will and choices of the people, but also the will of the government that emerges'; Koh, H. H. (2017), 'The Trump Administration and International Law', *Washburn Law Journal,* 56(3): pp. 413–469, p. 450; Barela, S. (2017), 'Cross Border Cyber Operations to Erode Cyber Legitimacy: An Act of Coercion', *Just Security*, 12 January 2017; Efrony and Shany (2018), 'A Rule Book on the Shelf?', p. 641.
[226] Schmitt (2017), 'Grey Zones in the International Law of Cyberspace', p. 16.
[227] State-sponsored intrusions into foreign computer systems and networks to collect bulk, non-public data that are then leaked to the public are sometimes known as 'doxfare'.
[228] US Office of the Director of National Intelligence (2017), *Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution*, in NIC (2017) *Assessing Russian Activities and Intentions in Recent US Elections,* Intelligence Community Assessment, https://www.dni.gov/files/documents/ICA_2017_01.pdf (accessed 25 Oct. 2019).
[229] Opinions vary as to whether the alleged Russian hacks of the DNC were coercive in the intervention sense. Schmitt (2017), 'Grey Zones in the International Law of Cyberspace', p. 8, argues that the 'slightly sounder' view is that cyber operations manipulating the election process were coercive; Tsagourias (forthcoming 2020), 'Electoral Cyber Interference', p. 17.

sovereigntist would argue that a violation would occur only if there were sufficient scale or severity of effects, but the point at which the line is drawn remains unclear.[230] In the case of the 2016 US presidential election, the highly intrusive nature of the Russian operation, and its extensive reach in terms of numbers of the population,[231] suggests that it could constitute a violation of sovereignty. But the lack of agreement of criteria for violation of sovereignty, including what, if any, effects should be taken into account, makes the assessment difficult.

Cyber intrusion into the fundamental operation of parliament

133. The operation of parliament falls within the sovereign functions of a democratic state. If it can be established that the hostile state is conducting a cyber operation coercively in relation to the operation of another state's parliament, for example disrupting online voting mechanisms during a key parliamentary vote, then such activity could meet the criteria for breach of the non-intervention principle.[232]

134. In the cyberattacks against Estonia in 2007, the websites of Estonia's prime minister, president, and parliament were made to crash, resulting in significant disruption to the country's political system. The attack lasted for three weeks and was of severe intensity, preventing government officials and citizens from updating or accessing information on these websites and maintaining email contact. While the attack has not formally been attributed to another state, it has been suggested that it was caused by Russia in response to Estonia's moving of the Bronze Soldier.[233] The attack's severity and sustained nature suggest the application of pressure by another state to deprive Estonia of its free will over the exercise of its sovereign functions. If the cyberattack was designed in order to compel a certain outcome or conduct in Estonia – even if purely to punish or exact retribution – then the activity could meet the threshold of coercive behaviour and thus intervention.

135. If the behaviour did not reach the level of coercion, could it nevertheless have been a violation of Estonia's sovereignty? A pure sovereigntist would argue that it could, as an unauthorized cyber incursion into the cyber infrastructure on Estonia's territory. Relative sovereigntists would argue that it would depend on whether the effects of the intrusion reached a certain scale or severity. In this case, the effects on Estonia's sovereign powers, including the inability to run its political system independently for a material period of time, were significant.

Cyber operations in relation to another state's critical infrastructure

136. 'Critical infrastructure' is a term used by governments to describe assets that are essential for the functioning of a society and economy. In recent years there have been a number of examples of actual or alleged cyberattacks carried out by one state in order to disrupt another state's critical infrastructure. For example, in December 2015, a cyberattack on Ukraine's energy grid caused a blackout that

[230] Schmitt (2017), 'Grey Zones in the International Law of Cyberspace', points out the differing views on violation of sovereignty in this context.
[231] According to New Knowledge's Disinformation Report (above at footnote 218), the scale was significant, reaching 126 million people on Facebook, posting 10.4 million tweets on Twitter, uploading more than 1,000 videos to YouTube, and reaching over 20 million users on Instagram.
[232] The UK's then attorney general stated that in the UK's view, 'intervention in the fundamental operation of Parliament' would be a breach of the prohibition on intervention: Wright (2018), 'Cyber and International Law in the 21st Century'.
[233] The attack occurred after the Estonian government decided to move the statue of the Bronze Soldier from the centre of Tallinn to the outskirts, which had been subject to vocal opposition by Russia, including Foreign Minister Sergey Lavrov, who condemned the move as a 'blasphemous attitude towards the memory of those who struggled against fascism'. See Socor, V. (2007), 'Moscow stung by Estonian ban on totalitarianism's symbols', *Eurasia Daily Monitor*, 4(19), The Jamestown Foundation, 26 January 2007, https://jamestown.org/program/moscow-stung-by-estonian-ban-on-totalitarianisms-symbols/ (accessed 25 Oct. 2019).

affected 225,000 people. Some state-sponsored cyberattacks have disrupted broadcasts from TV, radio or internet platforms that are thought to be serving as government propaganda. In March 2019, the Venezuelan President Maduro accused the US of a cyberattack on the country's power grid in a plot to force him from power.[234]

137. In each of the cases cited above, the aim of the alleged state cyber activity appears to have been to force an outcome or conduct with respect to a matter reserved to the target state, and thus the activity could potentially be regarded as coercive. If the infrastructure targeted is 'critical infrastructure' (i.e. assets that are essential for the functioning of a society and economy, such as public health, transport, energy, telecommunications and financial services) then the cyberattack is likely to concern the target state's sovereign functions because critical infrastructure is something over which the state has exclusive authority, even if – as is commonly the case – the infrastructure is owned and/or run by the private sector.

138. In its 2015 report, the UN GGE agreed that '[a] State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public'.[235] While this does not represent a binding obligation on states,[236] it shows their concern to protect critical infrastructure from cyberattacks.

Targeting of essential medical facilities

139. The provision of essential medical facilities to the population are an aspect of a state's critical infrastructure and as such fall within a state's inherently sovereign functions. The UK's attorney general specifically referred to the targeting of essential medical services by cyber means as an example of a prohibited intervention.[237] But the concept raises a number of questions that have yet to be resolved, including how 'essential medical facilities' should be defined. Countries have different ways of handling the provision of medical facilities within their territory; from state-operated systems that are provided free of charge such as the UK's National Health Service (NHS), to private systems where each individual must pay. Arguably, the provision of essential medical facilities such as emergency treatment for the state's citizens falls within a state's sovereign functions regardless of whether the system is public or private.

140. In order for cyber activity against another state's essential medical facilities to constitute intervention, the activity would need to be coercive. The WannaCry ransomware cyberattack of May 2017 caused certain NHS trusts in the UK to suffer damage, with many GP, hospital and ambulance services affected. The attack was attributed to North Korea by a number of states.[238] As the NHS is part of the UK's public service, there is a strong case to be made that its activities falls within the scope of the UK's sovereign functions. However, as noted above,[239] the intention of the perpetrating state in this case appears to have been to extract hard currency from the individual users affected rather than specifically to influence an outcome or conduct in the UK, which was not the original target of the attack. This would not therefore appear to be coercive and thus would not reach the

[234] Gunia, A. (2019), 'Venezuela Blames US for Record Blackout and Orders American Diplomats to Leave', *Time Magazine*, 13 March 2019.
[235] UN GGE (2015), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security report*, 22 July 2015, UN Doc A/70/174, para 13(f).
[236] For discussion of this point, see CCDCOE Interactive Cyber Toolkit (2019), 'Scenario 03: Cyber operation against a power grid', https://cyberlaw.ccdcoe.org/wiki/Scenario_03:_Cyber_operation_against_the_power_grid (accessed 25 Oct. 2019).
[237] Wright (2018), 'Cyber and International Law in the 21st Century'.
[238] Statement of Foreign Office Minister, Lord Ahmad (2017), 'Foreign Office Minister condemns North Korean actor for WannaCry attacks'.
[239] Para 108.

threshold of intervention. Whether the attack could be considered a violation of sovereignty depends on one's position on sovereignty. A pure sovereigntist might argue that it would, as an unauthorized cyber incursion into the health sector of another state's territory. A relative sovereigntist would argue that it would depend on the scale and severity of the effects involved.

III. Examples relating to espionage

141. Much state-sponsored cyber activity involves the activities of intelligence services. Indeed, cyber operations have enabled a dramatic increase in such intelligence activity. Cyber capable states regularly gather intelligence by gaining access to the foreign computer networks of multiple other states without consent. The intelligence gathered may then be used in a range of different ways.

> Saying that espionage is not prohibited by international law is not the same as saying that it is lawful. That question will depend on the means, method and effects of the intelligence operations, and therefore blanket assertions cannot be made.

142. In terms of the prohibition on intervention, it looks as though states regard the principle to apply to the activities of intelligence agencies as much as to other activities. With regard to other aspects of sovereignty, the issue is perhaps more difficult. As noted in the non-cyber context, the majority position among commentators is that with the exception of certain rules, espionage is largely left unregulated by international law and as such is not prohibited by international law per se.[240] Many commentators argue that this approach also applies in the cyber context.[241] On the other hand, it has been argued that acts of political and economic cyber espionage transgress the rule of territorial sovereignty by intruding into a domain protected by state sovereignty.[242] This approach would render unlawful even the lowest level of cyber activities by intelligence agencies, including information gathering.

143. There are a number of difficulties in assessing the relationship between states' cyber intelligence activities and sovereignty. State intelligence activity has unique features: it is conducted in secret, so it is hard to discern either state practice or state reactions to that practice. Nevertheless, in recent years there has been increasing state practice on the existence and scope of intelligence activity (including cyber activity) in the form of domestic legislation regulating the collection of intelligence, parliamentary

[240] See, for example, Deeks, A. (2015), 'An International Legal Framework for Surveillance', *Virginia Journal of International Law*, 55(2): pp. 291–368, p. 300.
[241] See, for example, para 5 of commentary to Rule 32 of Tallinn Manual 2.0; Huang and Mačák (2017), 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches', p. 303.
[242] Buchan (2018), *Cyber Espionage and International Law*, pp. 54–55. Buchan cites the fact that in the wake of the Snowden revelations that certain state institutions, including the National Security Agency in the US, were spying on other states through cyber means, some states accused the Western intelligence agents involved of violating international law. Buchan also cites some national case law, in particular *Re Canadian Security Intelligence Service Act* [2008]. See also Wrange, P. (2014), 'Intervention in National and Private Cyberspace and International Law', *Stockholm Faculty of Law Research Paper Series* 23, p. 322.

comment and oversight reports.[243] Further, the activities of some intelligence organizations have been extensively litigated in recent years before domestic courts and European courts[244] without any suggestion by the courts that espionage itself is a violation of sovereignty or any other rule of international law.

144. But saying that espionage is not prohibited by international law is not the same as saying that it is lawful. That question will depend on the means, method and effects of the intelligence operations, and therefore blanket assertions cannot be made. A few examples are illustrative.

- Cyber espionage can involve states taking active defence measures, including sitting on networks in many different states to extract information from the internet or to prevent threats to their territory.[245] States are often aware that other states are conducting these activities but do not formally object (whether based on perceptions of legality or otherwise). The assessment of the legality of such activity under international law may depend on the ultimate purpose for which the information gathered is subsequently to be used, and whether that ultimate activity will usurp the authority of the state in the exercise of its independent state powers in some way.
- Cyber espionage may also involve a state going into private servers located in a failed state to take out malware spread by a terrorist group. Such activity may take place without the consent of the host state, which may not be aware that the activity is taking place. The activity is not coercive towards the state on whose territory the servers are located, so this kind of activity would not meet the threshold of intervention. The extent to which the activity violates the sovereignty of the host state by usurping the authority of that state is debateable: the servers and computers affected are private property, and the perpetrating state is not exercising law enforcement powers, but under a pure sovereigntist approach this would constitute a violation of international law.
- States may also use cyber means to engage in economic espionage (for example, theft of IP), which is capable of causing significant economic damage to the target state and the companies within it. The extent to which this could violate sovereignty will again depend on whether sovereignty is perceived as open-ended or delineated by some kind of threshold, for example the quantitative effects of the economic loss caused to the target state's economy.[246] Whether or not it could constitute intervention will depend on whether such activity amounts to coercive behaviour. This is likely to be harder to establish, as it would require such activity to be carried out in order to deprive the target state of its free will in relation to one of its sovereign functions, for example the economy.

145. Increasing concern over economic espionage and the significant effects that it can cause in the target state has led to the conclusion of certain agreements between states on this issue, for example an agreement between the US and China in 2015, in which both states agreed to refrain from

[243] For a survey of legislation regulating the collection of intelligence in the EU; Belgium; France; Germany; Netherlands; Portugal; Romania; Sweden and the UK, see The Law Library of Congress (n.d.), 'Foreign Intelligence Gathering Laws', https://www.loc.gov/law/help/intelligence-activities/index.php (accessed 11 Oct. 2019); EU Agency for Fundamental Rights (2017), *Surveillance by Intelligence Services – Volume I: Member States' Legal Frameworks*, Luxembourg: Publications Office of the European Union https://fra.europa.eu/en/publication/2015/surveillance-intelligence-services (accessed 25 Oct. 2019).

[244] For example, the case of *Big Brother Watch & Others v UK*, App No 58170/13, 62322/14 and 24960/15, 13 September 2018, currently on appeal to the Grand Chamber of the European Court of Human Rights.

[245] For example, the US has adopted a position of 'defend forward', which describes the conduct of operations inside an adversary's networks to prevent threats before they reach their target. See US Department of Defense (2018), *Cyber Strategy*, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed 16 Oct. 2019).

[246] For discussion of sovereignty and economic cyber intrusions, see Djabatey, E. (2019), 'U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis – Part I', *Just Security*, 11 July 2019, https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/ (accessed 25 Oct. 2019).

conducting or knowingly supporting cyber-enabled theft of IP;[247] and a 2015 communiqué issued by world leaders attending the G20 Antalya Summit, which stated that 'no country should conduct or support ICT-enabled theft of intellectual property…' and that 'all states should abide by norms of responsible state behaviour' in using ICT.[248] This practice may in time crystallize into a norm constraining the exercise of state-sponsored economic espionage.[249] In the meantime, the default position would appear to be that while there is no overall prohibition on states' intelligence activities under customary international law, those activities need to be assessed on a case by case basis as to whether they breach a particular rule of international law.

[247] This agreement was reached following a meeting between President Obama and President Xi Jinping in 2015: Rollins, J. (2015), 'US-China Cyber Agreement', *CRS Insight*, 16 October 2015, https://fas.org/sgp/crs/row/IN10376.pdf (accessed 25 Oct. 2019). The UK and China also issued a joint statement that mentions an agreement not to 'conduct or support cyber-enabled theft of intellectual property', FCO (2015), 'UK-China Joint Statement 2015', 22 October 2015, https://www.gov.uk/government/news/uk-china-joint-statement-2015 (accessed 4 Oct. 2019).
[248] Paltiel, D. (2015), 'G20 Communiqué Agrees on Language to Not Conduct Cyber Economic Espionage', *Technology Policy Blog*, Center for Strategic and International Studies, 16 November 2015, https://www.csis.org/blogs/strategic-technologies-blog/g20-communiqué-agrees-language-not-conduct-cyber-economic (accessed 4 Oct. 2019).
[249] Huang and Mačák (2017), 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches', p. 308.

5. Reflections on the Relationship between Sovereignty and the Non-intervention Principle

146. The discussion of specific scenarios in Chapter 4 suggests that, in practice, activities that contravene the non-intervention principle and activities that violate sovereignty will often overlap in terms of the outcome. Just as the ICJ in *Nicaragua* noted that a single act may violate more than one of the prescriptive norms, so states' cyber actions will sometimes do the same.[250] Those that view sovereignty as a self-standing rule, violation of which can give rise to legal consequences, and those that view the non-intervention principle as the main tool for addressing states' cyber actions, are therefore not as far apart as might at first appear. Both view much of states' cyber activity below the use of force as a breach of international law, with the target state entitled to respond. But they reach this conclusion through different routes.

147. This paper argues that a violation of sovereignty occurs when one state exercises authority in another state's territory without consent in relation to an area over which the territorial state has the exclusive right to exercise its state powers independently.[251] The non-intervention principle is breached when a state uses coercive behaviour to deprive another state of its free will in relation to the exercise of its sovereign functions in order to compel an outcome or conduct with respect to a matter reserved to the target state.[252] The main difference between the two principles is that coercive behaviour is required in relation to the non-intervention principle, which is not necessary in relation to a violation of sovereignty.[253]

148. How much overlap (or gap) exists between the two positions discussed in this chapter depends both on how coercive behaviour is interpreted, and on whether some form of *de minimis* threshold applies in relation to violations of sovereignty:

- If some form of *de minimis* threshold applies, the bar for violation of sovereignty is higher and thus closer to the non-intervention principle.
- Coercion is interpreted in this paper as 'pressure on the victim state to deprive the target of its free will in relation to the exercise of its sovereign powers in order to compel conduct or an outcome with respect to a matter reserved to the target state'. The conduct or outcome could include simply hampering the target state in relation to the exercise of its sovereign functions in some way. This is not dissimilar to the conception of violation of sovereignty as one state's exercise of unauthorized power that usurps the target state's own independent authority; on the definition above, this too would often be likely to amount to coercive behaviour in practice.

[250] The examples of 'usurpation of government functions' provided in the Tallinn Manual 2.0, which are used to demonstrate situations in which violations of sovereignty would take place, could equally amount to a violation of the non-intervention principle in some cases, as the commentary itself points out: 'Although the International Group of Experts could not define "inherently governmental functions" definitively, it agreed that a cyber operation that interferes with data or services that are necessary for the exercise of inherently governmental functions is prohibited as a violation of sovereignty (*and in some cases the prohibition of intervention*, Rule 66). Examples include changing or deleting data such that it interferes with the delivery of social services, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, and the performance of key national defence activities' (para 16 of commentary to Rule 4, emphasis added).
[251] Para 46.
[252] Para 98.
[253] Para 84.

149. If we can set on one side the position of the 'pure sovereigntist', which does not sit easily with the reality of states' day to day interactions (especially in the intelligence context), there is indeed a significant overlap between those using the language of sovereignty and those referring only to non-intervention. It is not surprising that there is a good deal of overlap, as the principle of non-intervention protects sovereignty, and intervention violates sovereignty.

150. The difference of views between states on what constitutes a violation of sovereignty point to the value of states trying to first reach agreement on what kind of cyber activity they consider to constitute an internationally wrongful act, rather than focusing too much at the outset on the meaning of abstract terms.

Indiscriminate effects

151. Consideration should nevertheless be given to possible examples where the cyber activity in question is better viewed through the prism of general sovereignty than the specific non-intervention principle. These may include where the unauthorized exercise of authority by the state carrying out the cyber activity gives rise to indiscriminate knock-on effects in other states from a cyberattack directed elsewhere. These knock-on effects are unintended, without the perpetrating state caring about the consequences for other states, rather than as a result of deliberately coercive behaviour.

> In the case of the WannaCry ransomware cyberattack, which affected 300,000 computers in 150 countries, the perpetrating state attempted to extract hard currency from users, rather than to deprive the state(s) on whose territory users were affected of free will in relation to the exercise of sovereign functions.

152. For example, in the case of the WannaCry ransomware cyberattack mentioned above,[254] which affected 300,000 computers in 150 countries, the perpetrating state attempted to extract hard currency from users, rather than to deprive the state(s) on whose territory users were affected of free will in relation to the exercise of sovereign functions. The attack on individual users had ripple effects in other states, including on critical infrastructure in the UK, where GP surgeries and hospitals linked to NHS Trusts that had not updated their software were affected.[255] But the facts suggest that the disruption to the services affected was a side effect of the original criminal enterprise, rather than coercive behaviour specifically directed at subordinating the UK's sovereign will in relation to the exercise of its government functions. If so, then the intervention threshold would not have been met. Could the cyberattack still be considered an unauthorized exercise of authority in relation to the sovereign functions of another state? The Tallinn Manual 2.0 suggests that in certain circumstances it could.[256]

[254] Para 140.
[255] National Audit Office (2018), *Investigation: WannaCry cyber attack and the NHS*, Department of Health, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (accessed 25 Oct. 2019).
[256] The international group of experts involved in the Tallinn Manual 2.0 were of the view that intent is not a constitutive element of breach of sovereignty. 'So a cyber operation by or attributable to a state that is not intended to result in consequences that violate the sovereignty of another State, but that nevertheless generates them, is a violation of sovereignty', para 25 of commentary to Rule 4. See further at para 25: If a State conducts a cyber operation against another State, but that operation unexpectedly bleeds over into third States and causes harm at the level necessary to qualify as a violation of sovereignty, this Rule has been breached vis-à-vis those States despite the unintentional and unforeseeable nature of the harm.

153. But if this were the case, the scope of application of the sovereignty principle in the cyber context would expand quite significantly. The nature of the internet is such that malware and viruses can easily proliferate beyond borders with indiscriminate effect. In the WannaCry example, it could mean that the sovereignty of each of the 150 states affected was violated (in the case of relative sovereigntists, this would of course depend on the scale of the effects in the state concerned). Note that the joint statement by the UK, US and Australia attributing the attack to North Korea suggests that they did not consider sovereignty to be violated in this case; the attack was referred to as a 'criminal use of cyber space' rather than a violation of international law.[257] Similarly, in relation to the NotPetya attack (attributed to Russia by a number of states),[258] which targeted the Ukrainian government, but also generated indiscriminate damage in countries across Europe,[259] the UK government stated that the attack showed 'continued disregard for Ukrainian sovereignty' but did not refer to the sovereignty of other states affected by the virus.[260]

154. There is a need for caution when drawing insights from government statements (collective or individual) given that thus far there have been relatively few. There may be reasons other than the law for states to choose not to frame state-sponsored cyber activity as a violation of sovereignty, for example political caution; fear of retaliation; operational tactics;[261] or lack of certainty about how international law applies. The state concerned may prefer to handle the activity as an unfriendly act with diplomatic consequences; through covert counter cyber operations of their own;[262] prosecutions under domestic law,[263] or sanctions.[264] But nevertheless, it is clear from the public statements available that states have not thus far characterized knock-on effects in other countries as violations of sovereignty.

Non-intervention principle or sovereignty?

155. If the significant overlap identified above is accepted, one might ask: what is the point of the non-intervention principle? The value of the principle, as with the rules on the use of force, is that it provides an established customary rule for dealing with these issues. It has a firm existential foundation, content that is reasonably well understood, and is an emanation of the principle of sovereignty.

[257] Statement of Foreign Office Minister, Lord Ahmad (2017), 'Foreign Office Minister condemns North Korean actor for WannaCry attacks'. New Zealand, Denmark and Japan supported this attribution.
[258] Attribution made jointly by the UK, US, Australia, Canada, Denmark, and supported by New Zealand, Estonia, Finland, Latvia, Lithuania, Netherlands, Norway and Sweden.
[259] For example, Danish transport company Maersk spent $300 million to fix the damage caused to its worldwide operations, Osborne, C. (2018), 'NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs', *ZDNet,* 26 January 2018, https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/ (accessed 7 Oct. 2019).
[260] UK Government (2018), 'Foreign Office Minister condemns Russia for NotPetya attacks', https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (accessed 5 Oct. 2019).
[261] Efrony and Shany argue that some states are deliberately silent about the application of international law to give them greater operational leeway, Efrony and Shany (2018), 'A Rule Book on the Shelf?', p. 588.
[262] For example, US Cyber Command disrupted Russian hackers in the US midterm elections by signalling to them that they had been identified, and by using 'defend forward' measures to disrupt the internet access of Russia's Internet Research Agency on the day of the elections, Nakashima, E. (2019), 'U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms', *The Washington Post*, 27 February 2019, www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html (accessed 12 Sep. 2019).
[263] For example, in February 2018, the US Justice Department charged 13 Russian individuals and three Russian companies, including the Internet Research Agency, with carrying out a campaign designed to interfere in the conduct of the 2016 US Presidential election: *United States of America v. Internet Research Agency LLC*, District Court of Columbia, 18 U.S.C. §§ 2, 371, 1349, 1028A.
[264] For example, in March 2018, the US administration imposed sanctions on Russia's FSB and GRU and six of its senior officials in response to the NotPetya attack. As noted in para 68 above, the EU also recently agreed a cyber sanctions regime, which targets both state-linked groups and individual hackers with restrictive measures such as asset-freezing.

Just as the use of force has its own set of rules even though it is also a derivative of the sovereignty principle, so the non-intervention principle is a clearly established part of international law with its own constituent elements.

156. The lack of clarity as to when a violation of sovereignty has been committed in the cyber context may be one of the reasons that the UK government and some academic experts have argued that there is no cyber-specific rule on sovereignty. This paper has argued that there is a (perhaps small) gap between violation of the non-intervention principle and violation of sovereignty, but that it is not clear where the limits are in relation to sovereignty. There are two potential approaches to sovereignty that may avoid capturing all unauthorized intrusions in another state including mere trespass (whether physical or remote). One relates to the interpretation of the notion of inherently sovereign powers. The other encompasses a threshold based on scale and/or effects in the victim state. As we have seen, both issues are currently disputed.

157. On the issue of independent state powers, given that some states appear to conceive their inherently sovereign powers to include sovereignty over their citizen's data, placing greater reliance on sovereignty in the cyber context risks bolstering a position ('cyber sovereignty') in which individuals' freedoms online are undermined, contrary to international human rights law. As the definition of inherently sovereign functions in international law concerns the regulation of a state's political, economic, social and cultural systems, it does not seem credible to categorize any kind of state-sponsored interference in the matters of private companies or citizens as an internationally wrongful act. In the absence of agreement on how sovereignty applies in the cyber context, the non-intervention principle provides a more objective basis for assessing international wrongfulness than the sovereignty principle.

158. On the second issue, some suggest that where there is interference by one state in another state's affairs but no coercion, this should be considered to be a violation of sovereignty only in circumstances where there are certain quantitative or qualitative effects. This position has the virtue of striking a middle ground between those that consider sovereignty to be an unauthorized exercise of authority, whether physical or remote, which does not sit with reality of states' daily interactions, and those that deny that sovereignty has any legal consequences at all in the cyber context. But this position is *lex ferenda* rather than established international law. In due course, as further state practice and *opinio iuris* emerge, a cyber-specific understanding of sovereignty may develop, much like that developed for other domains of international law. In the meantime, because it is unclear whether there is a limit or threshold to violations of sovereignty, states may prefer to use the more clearly established framework of non-intervention where that is possible.

159. Ultimately, it may be that what matters is the substance of the rights and obligations and not how they are labelled (whether a violation of sovereignty or the prohibition on intervention). Nevertheless, it is important to be able to reach common understandings on these issues, especially when there is so much else in the cyber context on which states fundamentally disagree.

6. Processes for Reaching Agreement on the Application of International Law to Cyberspace

160. A number of multilateral, regional and bilateral initiatives have developed in recent years in attempts by states to reach agreement on how international law applies to states' cyber activities.[265] These initiatives have taken various forms including strategic dialogue; political statements; and proposals for the agreement of principles. These state-to-state initiatives, together with a number of multi-stakeholder initiatives, have often been directed at a wide range of aspects of regulating cyberspace, many of which go beyond the issues discussed in this paper. Where the initiatives concerned have addressed the application of international law to state-sponsored cyber intrusions below the use of force, they have not yet gone into much detail as to how international law principles such as sovereignty and non-intervention apply in practice.

UN initiatives

161. In terms of rule-making, the most significant initiative to date has been the UN GGE. As noted above,[266] the UN GGE of 2013 and 2015 reached some important conclusions on the law, including that international law and the principles of sovereignty and non-intervention apply to cyberspace. It also reached agreement on 11 voluntary non-binding norms on responsible state behaviour,[267] confidence-building measures, and coordinated cybersecurity capacity-building, which have since been endorsed by other states and regional groupings.[268] Together, these measures are often referred to as a Framework for Responsible State Behaviour in Cyberspace. But the 2016–17 UN GGE failed to agree a consensus report, amid concerns by some states about the militarization of cyberspace, in particular the application of the rules on use of force and international humanitarian law to states' activities in cyberspace.

162. In June 2019, a new Open-Ended Working Group (OEWG) of the UN General Assembly started work, as a result of a resolution sponsored by Russia,[269] and will report to the General Assembly in September 2020.[270] The OEWG has been tasked with studying the existing norms contained in the previous UN GGE reports. The resolution also includes the possibility of 'introducing changes to the rules, norms and principles of responsible behaviour of States' agreed in the 2013 and 2015 UN

[265] The Carnegie Endowment's Cyber Norms Index provides a useful overview of multilateral dialogue and initiative on cyber norms, Carnegie Endowment for International Peace (n.d.), 'Cyber Norms Index', https://carnegieendowment.org/publications/interactive/cybernorms (accessed 7 Oct. 2019).
[266] Paras 15; 18–19.
[267] For a commentary on the voluntary, non-binding norms of responsible state behaviour from the 2015 report of the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security, see United Nations Office for Disarmament Affairs (2017), *Voluntary Non-binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary*, https://www.un.org/disarmament/wp-content/uploads/2018/04/Civil-Society-2017.pdf (accessed 7 Oct. 2019).
[268] See, for example, Noor, E. (2018), 'ASEAN Takes a Bold Cybersecurity Step', *The Diplomat*, 4 October 2018, https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/ (accessed 28 Oct. 2019), which notes that at its third Ministerial Conference on Cybersecurity, the ASEAN conference endorsed in principle the 11 voluntary, non-binding norms recommended by the 2015 UN GGE.
[269] UN General Assembly (2018), 'Developments in the Field of Information and Telecommunications in the context of International Security', UN Doc A/C.1/73/L.27/rev.1, https://undocs.org/A/C.1/73/L.27/Rev.1 (accessed 28 Oct. 2019).
[270] For details of the work and timetable for both UN groups, see Geneva Internet Platform (n.d.), 'UN GGE and OEWG', Digital Watch Observatory for Internet Governance and Digital Policy, https://dig.watch/processes/un-gge (accessed 28 Oct. 2019).

GGE reports.[271] It was clear from the OEWG's first session in September 2019 that most states wish to use the existing recommendations in the 2015 UN GGE report as the starting point for the basis of discussions, but there remains a risk that certain states will push for elements of the existing agreement reached on international law to be undone.

163. The UN General Assembly also agreed to the formation of a new UN GGE, further to a resolution sponsored by the US. The new UN GGE will hold its first meeting in December 2019 and report to the General Assembly in 2021.[272] This group of 25 selected UN member states has also been mandated to study how international law applies to state action in cyberspace and to identify ways to promote compliance with existing cyber norms. The results will be submitted in a report to the General Assembly in 2021; the resolution also requests 'an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications'.[273] It is hoped that the discussions in both the OEWG and UN GGE will encourage more states to indicate publicly their position on the legal principles and thresholds that they consider to apply in cyberspace. This will promote transparency and predictability, and help to further common understandings.

> The new UN GGE has been mandated to study how international law applies to state action in cyberspace and to identify ways to promote compliance with existing cyber norms.

164. The twin-track approach in the UN offers an opportunity for further dialogue among states on these issues. The OEWG, open to all interested UN member states, enables a larger and more diverse number of states to participate. But the overlapping mandates of the two groups reflect the fact that cyber norm-making and enforcement have become a site of geopolitical rivalry, with the risk that the parallel processes will operate in competition or contradiction with one another rather than constructively. There is also a risk that the process and institutionalization of dialogue over 'norms' in the cybersecurity area trumps the difficult discussion of how existing international law applies. Given the differences between states in their approaches to how sovereignty applies in cyberspace, including whether it applies as a principle or a legally consequential rule in this area, statements issued by the OEWG and UN GGE with reference to principles will need to be studied carefully. They may not so much clarify the law as paper over important legal differences, each side agreeing with the language but understanding that language to mean something fundamentally different.

Regional state-led initiatives

165. Regional and bilateral initiatives may offer a helpful means of identifying common areas of agreement, as a supplement or complement to the UN processes. During 2019, the UN GGE held consultations with regional groups (the African Union, EU, Organization of American States, OSCE

[271] Ibid., operative para 5.
[272] UN General Assembly (2018), 'Resolution adopted by the UN General Assembly on 22 December 2018 on "Advancing responsible State behaviour in the context of international security"', UN Doc A/Res/73/266, https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266.
[273] Ibid., operative para 3.

and ASEAN Regional Forum) in advance of the GGE's first meeting. States have been discussing the application of international law to cyber in a number of other regional forums, including the Shanghai Cooperation Organisation[274] and Asian-African Legal Consultative Organization.[275]

166. Other organizations such as the G7 and G20, OSCE,[276] EU,[277] OAS and African Union have been debating cyber norms more broadly, including the development of confidence-building measures. Such measures focus on the exchange of information between states; greater transparency in order to deter cyber conflict and reduce the risk of escalation in the event of a cyberattack; capacity-building to strengthen cyber resilience in states; and cybersecurity.

Initiatives involving non-state actors

167. Over the last few years, there has been a proliferation of multi-stakeholder initiatives focused on furthering understanding on what rules should apply to states' interactions in cyberspace. These initiatives, which involve a range of actors drawn from various sectors including civil society, think-tanks, the tech sector and international institutions, have sought to fill the void left by the silence or ambiguity of most states in this area. They include the work of the Global Commission on the Stability of Cyberspace, a multi-stakeholder body that has proposed principles, norms and recommendations to guide responsible behaviour by all parties in cyberspace;[278] the Cybersecurity Tech Accord, which aims to promote collaboration between tech companies on stability and resilience in cyberspace;[279] and Digital Peace Now, a campaign to stop cyberwarfare.[280] They also include the Tallinn Manual 2.0 and the writings of a number of legal practitioners and academics in this area.

168. Some states have spearheaded multi-stakeholder initiatives, for example President Macron's 'Paris Call for Trust and Security in Cyberspace', which to date has received the backing of 67 states, 139 international and civil society organizations, and 358 private-sector organizations.[281] There are also opportunities for non-state actors to contribute to state-led processes, for example at the intercessional meetings of the OEWG and GGE at the UN.[282]

[274] In January 2015, the member states of the Shanghai Cooperation Organisation submitted to the UN General Assembly a revised version of the International Code of Conduct for Information Security, which it had originally submitted to the UN General Assembly in 2011: Letter dated 9 January 2015 from the permanent representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the secretary-general, UNGA A/69/723. The original version was the first international paper dedicated to norms of behaviour in cyberspace, but has not enjoyed support from Western states due to concerns about the lack of reference to international human rights law, in particular in the context of the 'duty to cooperate in combating terrorism, separatism and extremism'.
[275] The Asian-African Legal Consultative Organization, the only inter-governmental international organization of Asia and Africa in the field of international law, currently has a work stream on international law in cyberspace.
[276] The OSCE has launched 16 voluntary confidence-building measures, which would allow states to 'read' another state's posturing in cyberspace, with the aim of making cyberspace more predictable; provide opportunities for timely communication and cooperation between states, including to defuse potential tensions; and promote due diligence to address cyber challenges.
[277] In June 2017, the EU Council adopted conclusions on a framework for a joint diplomatic response to malicious cyber activities, known as 'The Cyber Diplomacy Toolbox'.
[278] Global Commission on the Stability of Cyberspace (2019), *Advancing Cyberstability*, Final Report, November 2019, https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf (accessed 13 Nov. 2019).
[279] Cybersecurity Tech Accord (2018), 'About the Cybersecurity Tech Accord', https://cybertechaccord.org/about/ (accessed 7 Oct. 2019).
[280] Microsoft (2018), 'Digital Peace Now', https://digitalpeace.microsoft.com (accessed 16 Oct. 2019).
[281] The Ministry for Europe and Foreign Affairs (2018), 'Paris Call for Trust and Security in Cyberspace', https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf (accessed 7 Oct. 2019).
[282] In practice, access for non-state actors may be difficult as some states favour a multilateral as opposed to multi-stakeholder approach. At the OEWG meeting in September 2019, non-governmental organizations without UN Economic and Social Council (ECOSOC) status were unable to obtain accreditation to participate in the meeting.

169. Initiatives by non-state actors benefit from broader understanding of the issues from a range of interested parties without the geopolitics involved in multilateral meetings.[283] They also recognize the important role that the private sector can play in detecting or preventing cyber incidents, and the fact that the private sector often owns and manages the critical infrastructure that is frequently the target of state-sponsored cyber operations.

Prospects of reaching agreement in this area

170. In practice, there are a number of obstacles to states reaching agreement on how the principles of non-intervention and sovereignty apply in the cyber context. The first is geopolitics, which is likely to hamper the new OEWG and GGE processes in the UN. In light of this, there is perhaps some value in separate groups of states, academics and civil society coming together to contribute to the processes in a less politically fraught environment. But whatever the modalities of discussion, it has to be recognized that because states' positions on sovereignty are so different, it is likely to be difficult in practice for states to reach agreement on how sovereignty applies in cyberspace. Apart from the differing position on the law, there is also a practical impediment: because cyber activity is in the toolkit of governments, they will wish to safeguard their ability to use it, rather than setting the bar for unlawful activity too low. There is perhaps likely to be more commonality between states about whether particular state behaviour constitutes an internationally wrongful act, and why, than there is about whether sovereignty is a rule or a principle, and how it relates to intervention.

171. The prospect of states reaching agreement in the form of a treaty on these issues is a long way off, despite calls from many quarters for greater legal certainty.[284] Above all the process would take political will, which is currently lacking in this area. It may be easier to reach agreement on specific applications of the law than on abstract principles.[285] In the cyber context, the agreements between certain states not to conduct commercial cyber espionage against each other suggest that where there are pressing issues of mutual concern, there may be scope for states to reach agreements on specific issues. In due course, such agreements could potentially pave the way for the development of specific agreements, for example a prohibition on attacking another state's critical infrastructure.

[283] For discussion of the role of non-state actors in the debate on cyber norms see Mačák, K. (2019), 'On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law', *AJIL Unbound,* 113: pp. 81–86.
[284] See, for example, Robert Hannigan, ex Director of GCHQ, in an interview with Wired, February 2018, Burgess, M. (2018), 'We need a global cyberwar treaty, says the former head of GCHQ', *Wired UK*, https://www.wired.co.uk/article/gchq-uk-robert-hannigan-cyberwar-definition (accessed 7 Oct. 2019); Microsoft has called for a 'Digital Geneva Convention', Smith, B. (2017), 'The Need for a Digital Geneva Convention', keynote speech, https://1gew6o3qn6vx9kp3s42ge0y1-wpengine.netdna-ssl.com/wp-content/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf (accessed 3 Feb. 2019).
[285] Just as it was possible for states to reach agreement in 1868 on the St Petersburg Declaration on 'dum dum' bullets, long before agreement on general principles of international humanitarian law was possible.

7. Conclusions and Recommendations

172. Until governments are more transparent about their views on how international law applies to their cyber activities, and explain their practices, the conclusions below about the application of international law to states' cyber operations are necessarily cautious. The following conclusions and recommendations are a result of extensive research and discussions, including at roundtables attended by states' representatives.

I. Conclusions on the law

i. International law is applicable to states' activities in cyberspace.

ii. In the absence of relevant treaties other than the UN Charter, existing customary international law must be looked to as a basis for the law applicable in cyberspace. Publicly available state practice relating specifically to cyberspace is currently sparse. But as with any other state activity, existing principles and rules of international law are applicable to state activities in cyberspace, unless there is state practice with *opinio iuris* to indicate that a relevant principle or rule is not applicable.

iii. The principle of sovereignty applies in relation to states' cyber activities, as it applies in the non-cyber context. The principle has legal consequences.

iv. A state's authority and jurisdiction apply in relation to cyber infrastructure and operations within its territory, as they do to other matters. Territorial sovereignty and the independence of a state's powers vis-à-vis other states are therefore applicable.

Violation of sovereignty

v. A state with an agent physically present in another state's territory who is exercising state powers within the territory of that other state without consent may be committing a violation of the latter state's sovereignty. Similarly, the remote carrying out of such an act by a state agent without consent, which has a harmful effect on another state's territory may also be a violation of sovereignty in certain circumstances. This rule applies equally in relation to activities in cyber operations as it does in relation to other state activities.

vi. The precise limits of the application of this rule are not established in international law. It is not clear, for example, whether there is some form of *de minimis* rule in action, as evidenced by the way that states treat the activities of other states in practice. While some would like to set limits by reference to the scale or severity of effects of the cyber activity, at this time there is not enough state practice or *opinio iuris* to say that such limits are reflected in customary international law. The assessment of whether sovereignty has been violated therefore has to be made on a case by case basis, if no other more specific rules of international law apply.

vii. Before a principle of due diligence can be invoked in the cyber context, further work is needed to agree upon rules as to what might be expected of a state in this context. This should be discussed and agreed upon by states.

The non-intervention principle

viii. The principle of non-intervention is the corollary of the principle of sovereignty, by prohibiting a state from intervening by coercive means in matters within another state's sovereign powers. This principle applies to a state's cyber operations as it does to other state activities.

ix. The coercive behaviour is carried out by a state or by a non-state actor whose actions are attributable to a state under the rules on state responsibility.

x. The element of coercion in the non-intervention principle describes pressure on the victim state to deprive the target of its free will in relation to the exercise of its sovereign powers in order to compel an outcome in, or conduct with respect to, a matter reserved to the target state.

xi. The coercive behaviour can consist of a range of techniques: direct and indirect; overt and covert.

xii. It is the fact of the coercive behaviour applied in relation to the sovereign functions of another state that is the key to the non-intervention principle. The coercive behaviour does not need to succeed in depriving the target state of its free will in relation to its sovereign functions. Nor does the state need to know of the interference at the time it takes place.

xiii. Where there are state cyber operations affecting another state's powers, but there is no coercion, the principle of non-intervention does not apply. In such circumstances it will be necessary to ascertain whether a cyber operation has violated the target state's sovereignty in another way.

Overlap between non-intervention and sovereignty

xiv. In practice, activities that contravene the non-intervention principle and activities that violate sovereignty will often overlap. How much overlap or gap exists between the two depends both on the interpretation of coercion and on whether or not a form of *de minimis* threshold applies in relation to violations of sovereignty.

xv. In view of the overlap, it is perhaps not surprising that states refer to violations of international law in general rather than specifying a particular branch of the law.

xvi. Because it is unclear whether there is a limit or threshold to violations of sovereignty, states may prefer to use the more clearly established framework of non-intervention, where that is possible.

xvii. In due course, further state practice and *opinio iuris* may give rise to an emerging cyber-specific understanding of sovereignty, just as specific rules deriving from the sovereignty principle have crystallized in other areas of international law.

II. Recommendations to governments

i. States need to make an informed decision as to where their own position lies on the application of international law to cyber activity. Intelligence agencies and foreign services within a state need to speak with one voice.

ii. Once they have decided on their legal position, states should indicate publicly what it is, where possible giving examples of when an obligation may be breached, as states such as the UK, the Netherlands and France have done.

iii. States that disagree on how the law applies must discuss these issues in a more open way.

iv. The UN offers one forum for discussion. Further dialogue between separate groups of states, academics, private-sector organizations and civil society on these issues would also be valuable, building on the work in the Tallinn Manual 2.0 and other initiatives.

v. Discussion of sovereignty and non-intervention in the cyber context should be divorced from consideration of the law on use of force and armed conflict.

vi. States should not seek to undo the valuable consensus on the application of international law to cyberspace that has been reached at past UN GGEs.

vii. Instead, further discussion should focus on how the rules apply to practical examples of state-sponsored cyber operations. There may be more commonality about specific applications of the law ('is this behaviour an internationally wrongful act, and why?') than there is about abstract principles ('is sovereignty a rule or a principle and how does it relate to intervention?').

viii. The prospects of a general treaty in this area are far off. There may be benefit in looking for agreement on limited rules, for example on due diligence and a prohibition on attacking critical infrastructure, before tackling broad principles.

Acknowledgments

The author would like to express her sincere thanks to Elizabeth Wilmshurst, Distinguished Fellow, Chatham House, for her invaluable comments, guidance and support in writing this paper.

The analysis in this paper draws upon a number of roundtable meetings held under the Chatham House Rule in 2019 to encourage open and constructive discussion. I would like to thank the participants at those meetings, who gave generously of their time and provided valuable insights. Many thanks also to James Green, Sean Watts, Nicholas Tsagourias, Douglas Wilson, Russell Buchan, Pål Wrange, Joyce Hakmeh, Ruma Mandal and the anonymous peer reviewer for their helpful comments on or relating to the paper. I am also grateful to Jack Kenny for research assistance, to Mike Tsang for editing, and to Chanu Peiris for coordinating the paper.

The views expressed in this publication are the sole responsibility of the author.

About the Author

Harriet Moynihan is an associate fellow in the International Law Programme at Chatham House, a research visitor at the Bonavero Institute of Human Rights at the University of Oxford, and a visiting fellow of Mansfield College, Oxford. Before joining Chatham House, Harriet was a legal adviser at the Foreign & Commonwealth Office, where she advised on a wide range of international law issues. Prior to that, Harriet was an associate solicitor in the antitrust department of Clifford Chance LLP, where she worked in the firm's London and Singapore offices.

Independent thinking since 1920

Cover image: A computer hacked by a virus known as Petya. The Petya ransomware cyberattack hit computers of Russian and Ukrainian companies on 27 June 2017.

Photo credit: Copyright © Donat Sorokin/TASS/Getty

ISBN 978 1 78413 378 8

This publication is printed on FSC-certified paper.

FSC

Typeset by Soapbox, www.soapbox.co.uk

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223