Israel Law Review **53**(2) 2020, pp 189–224. © Cambridge University Press and The Faculty of Law, The Hebrew University of Jerusalem, 2020.
doi:10.1017/S0021223720000060

Information Operations and the Question of Illegitimate Interference under International Law

Henning Lahmann[*]

The article examines the legal qualification of state-led information operations that aim to undermine democratic decision-making processes in other states. After a survey of the legal attitudes of states towards such operations during the Cold War, the impact of the digital transformation on the frequency and quality of information operations is explained. The article assesses scholarly responses to the outlined paradigm shift regarding the prohibition of intervention, respect for sovereignty, and the principle of self-determination. The study then inquires whether it is possible to detect a change in how states qualify adversarial information operations by tracking recent state practice and official statements of opinio juris*. The survey concludes that there is insufficient uniformity to allow for an inference that the content of the analysed rules of customary international law has already shifted towards more restrictive treatment of foreign interference. As a possible way forward, the article ends with a proposal to focus on deceptive and manipulative conduct of information operations as the most viable path to outlaw such state behaviour in the future. Instead of attempting to regulate the content of information, this approach is better suited to safeguard freedom of speech and other potentially affected civil rights.*

Keywords: information operations, election interference, principle of non-intervention, sovereignty, self-determination

1. Introduction

Attempting to influence public opinion in another country is not a new phenomenon. In fact, information warfare is probably one of the oldest forms of conflict.[1] However, since the scale of Russian attempts to meddle with decision-making processes in Western states has come to light, there has been growing concern about the stability of liberal-democratic political systems and their vulnerability to digitally enabled, state-led information operations. Public discourse, as one of the foundations of modern democracy,[2] appears increasingly to be under threat. In fact, not just Russia, but a growing number of states have found novel ways to weaponise information with hitherto unforeseen combinations of covert social media campaigns, bots, hacks and leaks.[3] According to a recent study, at least 70 countries were affected by concerted

[*] Senior Researcher, Digital Society Institute, ESMT Berlin; henning.lahmann@esmt.org. The author would like to thank the Israel Public Policy Institute and the Heinrich Böll Stiftung in Tel Aviv for funding the research as part of the 'European-Israeli Dialog on Policies for the Post-Truth Era: Disinformation in the Digital Public Sphere', and the research staff of the Lipkin-Shahak Program at the Institute for National Security Studies at Tel Aviv University, in particular, David Siman-Tov, Pnina Shuker and Itai Brun.

[1] Herbert Lin and Jaclyn Kerr, 'On Cyber-Enabled Information Warfare and Information Operations', May 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680.

[2] Judit Bayer and others, 'Disinformation and Propaganda: Impact on the Functioning of the Rule of Law in the EU and its Member States', European Parliament, 28 February 2019, 52.

[3] Peter Pomerantsev, 'To Unreality – and Beyond' *6 Journal of Design and Science*, 23 October 2019, https://jods.mitpress.mit.edu/pub/ic90uta1?readingCollection=eb8e12ec.

disinformation campaigns in 2018 alone – and not only in the West.[4] Facebook reports that many information operations are ongoing and that there is likely to be a further increase ahead of the 2020 United States presidential election,[5] ready to repeat the troubling events of 2016 when the Saint Petersburg-based Internet Research Agency carried out a months-long disinformation campaign aimed at the American electorate.[6] Indeed, as was prominently evidenced ahead of the 2019 elections for the European Parliament, no vote is now safe from antagonistic, subversive interference, a development that has the potential to severely undermine trust in democratic processes in the long run. Considerable concern surrounded the two parliamentary elections in Israel in 2019, as the country is considered 'particularly sensitive to foreign influence operations' given that, according to an expert, its internal rifts and unique security situation can be exploited for concerted meddling which further divides the electorate.[7] Almost all experts agree that this new problem for liberal democracies will only gain more urgency, and that we have only recently started to grapple slowly with the implications. Viable solutions are still far down the road.

While any answers will require a multifaceted approach which takes into account the various aspects of the issue of adversarial information operations targeting democratic decision-making processes, this article examines the potential contribution of public international law. After a brief explanation of relevant concepts, a survey of state-led information operations in historical perspective will track the evolution of such conduct after the Second World War and assess the significance of changes triggered by the digital transformation over the past two decades. Acknowledging a qualitative difference that was exposed by recent election meddling, the article evaluates approaches in international legal scholarship to tackle the problem before attempting to identify corresponding shifts in recent *opinio juris* and state practice with the aim of determining the existence of international rules against information operations. This in-depth survey is followed by outlining a number of suggestions for a possible way forward to find a sustainable solution under international law.

2. The Contemporary Transnational Information Landscape: Conceptual Explication

Ever since the scale of foreign influence efforts gradually became clear in the aftermath of the 2016 US presidential election, there has been a surge in journalistic coverage and academic literature on the topic of information asymmetries within the democratic sphere. At the same time,

[4] Davey Alba and Adam Satariano, 'At Least 70 Countries Have Had Disinformation Campaigns, Study Finds', *The New York Times*, 26 September 2019.

[5] Mike Isaac, 'Facebook Finds New Disinformation Campaigns and Braces for 2020 Torment', *The New York Times*, 21 October 2019; Donie O'Sullivan, 'Facebook: Russian Trolls Are Back. And They're Here to Meddle with 2020', *CNN.com*, 22 October 2019, https://edition.cnn.com/2019/10/21/tech/russia-instagram-accounts-2020-election/index.html.

[6] Robert S Mueller, 'Report on the Investigation into Russian Interference in the 2016 Presidential Election', Volume I, March 2019, 1.

[7] Ofrir Barel, 'Why Are Israeli Elections Extremely Sensitive to Fake News?', *Council on Foreign Relations*, 9 April 2019, https://www.cfr.org/blog/why-are-israeli-elections-extremely-sensitive-fake-news.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

the ensuing public debate has suffered from a lack of clarity and definitional rigour[8] concerning frequently used terms such as 'fake news', 'disinformation', 'misinformation', 'propaganda', 'cognitive warfare', 'influence operations' and 'information operations'. The resulting ambiguities have been exploited both by authoritarian leaders to delegitimise free public discourse within their own countries, and by states to muddy the waters as regards adversarial behaviour on the international plane. In order to be able to tackle the matter from a legal perspective, it is imperative to clarify the meaning of some of the notions. As there are different understandings in the literature concerning the concepts, the following section limits itself to provide definitions that are useful and appropriate for the legal issues under scrutiny here.

While the term 'fake news' is generally seen as misleading and should be avoided given its overuse in public discourse despite its inherent lack of definitional clarity,[9] 'disinformation' is more expedient even though the concept, too, suffers from an abundance of occasionally incoherent descriptions. It is useful to contrast 'disinformation' with 'misinformation': whereas the latter signifies information that is factually wrong yet not intentionally so, disinformation is 'deliberately false or misleading'.[10] The European Commission defines the concept as 'false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit'.[11] This intended harm comprises 'threats to democratic political processes and values' and is not already covered by statutory restrictions on legitimate speech such as 'defamation, hate speech, incitement to violence'.[12] In other words, the harm manifests not necessarily in the inaccuracy of the piece information itself, but in its context, application and purpose. In this sense, otherwise factually correct information can be used *as disinformation*, such as where the recipient of the information is deceived as to the identity of the speaker. For instance, one of the hallmarks of Russian conduct on social media is the method of posting information in the guise of a citizen of the target audience's country.[13] This aspect of disinformation campaigns is particularly relevant for the following legal analysis.

Conceptually distinct from the notion of 'disinformation' is the term 'propaganda', which is in some ways older and originally had a rather neutral connotation. In its more recent discursive application it is most appropriately described as a deliberate attempt to persuade a target audience, often in the form of a systematic information campaign. Often, though not necessarily, the persuasion is achieved by means of manipulation or deception.[14] Utilising disinformation as explained above may or may not be a part of such efforts, but it is not by definition a necessary element of propaganda. In principle, the objectives can just as easily be achieved in the case

[8] Claire Wardle and Hossein Derakhshan, 'Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making', Council of Europe Report DGI(2017)09, 27 September 2017, 15.
[9] ibid 15.
[10] Caroline Jack, 'Lexicon of Lies: Terms for Problematic Information', *Data & Society Research Institute*, 2017, 2–3, https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf.
[11] European Commission, 'A Multi-Dimensional Approach to Disinformation', 30 April 2018, 10.
[12] ibid.
[13] Scott Shane, 'The Fake Americans Russia Created to Influence the Election', *The New York Times*, 7 September 2017.
[14] Jack (n 10) 6–7.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

where an agent with a verified identity disseminates factually correct information and merely frames it in a way that has a manipulative effect on the target audience. Such course of communicative action often takes the form of putting an *alternative* narrative about a current or historical event in competition against the official or established one. In this way, manipulative information does not require an actual lie or deception of identity. Depending on the method of persuasion, 'propaganda' is sometimes broken down into 'white' (using accurate information with a particular narrative framing or *spin*), 'grey' (combining accurate and false information), and 'black' (using inaccurate information and/or deception of speaker identity).[15]

Closely related to the term 'propaganda' is the notion of 'information operations'. For the purpose of this article 'information operations' – sometimes called 'influence operations'[16] – will be used as an encompassing concept broadly circumscribing the subject under scrutiny. In a 2017 paper, social media company Facebook defined 'information operations'[17] as:

> actions taken by organised actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts aimed at manipulating public opinion.

Although not strictly congruent, there is thus a considerable conceptual overlap between the notions of 'propaganda' and 'information operations'; as the latter is the more contemporary term and arguably bears a more neutral connotation, it will be the preferred term for the subsequent legal assessment.

Once such conduct enters the realm of interstate relations, and information is used strategically and with adversarial aims by or on behalf of a state in conflict with another state, other concepts such as 'information' or 'cognitive warfare' are sometimes used. The Russian Ministry of Defence defines 'information war' as 'a struggle between two or more states … to destabilise a society and a state through massive psychological conditioning of the population, and also to pressure a state to make decisions that are in the interest of the opponent'.[18] Such conduct falls into the broader, emergent strategic category of 'hybrid warfare'.[19] While useful for a comprehensive assessment of contemporary forms of interstate conflict, this article will apply the more general notion of 'information operations'.

---

[15] ibid 7.

[16] Bruce Schneier, '8 Ways to Stay Ahead of Influence Operations', *Foreign Policy*, 12 August 2019, https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations.

[17] Jan Weedon, William Nuland and Alex Stamos, 'Information Operations and Facebook', 27 April 2017, 4, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

[18] See Martin Russell, 'Russia's Information War: Propaganda or Counter-Propaganda', European Parliamentary Research Service, 3 October 2016, 2.

[19] See Patrick J Cullen and Erik Reichborn-Kjennerud, 'Understanding Hybrid Warfare', January 2017, 8 ('the synchronised use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects'), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

3. ADVERSARIAL INFORMATION OPERATIONS AND INTERNATIONAL LAW

As mentioned at the outset, addressing information operations and the problem of disinformation in today's political discourse more generally requires a comprehensive, overarching and multi-faceted approach, which comprises efforts to increase media literacy in the general population, institutions for fact checking, platform regulation, or robust national legislation to calibrate freedom of speech and its boundaries at the domestic level.[20] This is not least vital given the fact that much activity that may fall into the broad rubric of 'disinformation' is conducted by actors on the inside, such as political parties or even the government.[21] However, when foreign actors turn out to be responsible for interfering in democratic decision-making processes in another country by way of orchestrated, strategic information operations – as, for instance, abundantly demonstrated by Russian meddling in elections in Europe and the United States over the past couple of years – affected states will be inclined to resort to additional tools of diplomacy and foreign policy; if they do, questions of international law will almost inevitably come into play.

Therefore, from the perspective of interstate relations it is important to discuss whether adversarial information operations aimed at interfering in another state's internal political affairs violate international law.[22] If they do not, then affected states are barred from resorting to responses such as certain sanctions or offensive cyber operations, as they qualify as countermeasures and thus require an unlawful prior act of the target state in order to be justified. That aside, deeming this kind of conduct as unlawful under international law, of course, sends a strong signal to the community of states, unambiguously communicating which type of behaviour is considered acceptable and which is not. Starting with a survey of the historical development of the issue, the following sections will thus examine how international law deals with the problem of information operations.

3.1. INFORMATION OPERATIONS AND ELECTION INTERFERENCE DURING THE COLD WAR

3.1.1. HISTORICAL EXAMPLES

Information operations for the purpose of manipulating public opinion in adversarial states were a frequent occurrence during the Cold War, often with the aim of interfering in electoral processes. Not surprisingly, it was first and foremost the great powers that employed such strategies in order to exert influence over other states. Former officers from US intelligence services readily admit to

[20] Annina Claesson, 'Coming Together to Fight Fake News: Lessons from the European Approach to Disinformation', *New Perspectives on Foreign Policy*, 8 April 2019, 13.
[21] Samantha Bradshaw and Philip N Howard, 'The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation', *Oxford Internet Institute*, 2019, 9–10, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf; McKay Coppins, 'The Billion-Dollar Disinformation Campaign to Reelect the President', *The Atlantic*, March 2020.
[22] Steven J Barela, 'Zero Shades of Grey: Russian-Ops Violate International Law', *Just Security*, 29 March 2018, https://www.justsecurity.org/54340/shades-grey-russian-ops-violate-international-law.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

having engaged in the practice during the decades after the end of the Second World War.[23] There is little doubt that the Soviet Union consistently acted in the same manner. In fact, since the early 1960s at least, Moscow has employed subversive methods to increase the chances of the preferred candidate in presidential elections in the United States.[24] In a widely quoted paper from 2016, the scholar Dov H Levin estimated that between 1946 and 2000 the US attempted to influence no fewer than 81 elections in other countries, while the Soviet Union/Russia did the same in at least 36 cases, both openly and through covert information operations.[25]

As evidenced by the numbers alone, the United States was particularly active in this field. Certainly such conduct was not limited to information operations as defined above. Occasionally, election 'meddling' amounted to outright violence or the supporting of coups by authoritarian, anti-communist military leaders; the examples of Iran 1953, Guatemala 1954, Congo 1961, and Chile 1973 are the most notorious. More to the point, however, there have also been numerous instances of more subtle interference. In Italy, in 1948, the Central Intelligence Agency heavily funded the Christian Democrats in order to prevent the communists from coming to power and resorted to propaganda efforts that involved false narratives about the communist leaders. Elections in the Philippines in 1953 and the clandestine backing of Christian parties in Lebanon four years later represent two further proven instances of US interference.[26] With the end of the Cold War the practice shifted. While attempts to influence decision-making processes in other states did not come to a halt, the efforts gradually became more overt, relying on the touting of economic aid or open campaigns under State Department leadership as opposed to CIA meddling. The uncertain re-election of Boris Yeltsin in Russia was ensured in this way[27] and, in 2000, growing opposition to Yugoslavia's president Slobodan Milosevic was straightforwardly supported by the United States and other Western states.[28] The practice has continued to this day, although not always successfully: when Washington tried to prevent Afghan president Hamid Karzai from being re-elected in 2009, it failed.[29]

These attempts at influencing political processes in other countries often involved the utilisation of media tactics. During the 1980s the CIA managed to have desired information published through foreign news organisations. In some instances, at least, these operations involved the dissemination of disinformation.[30] One of the longest running influence campaigns orchestrated by

[23] Scott Shane, 'Russia Isn't the Only One Meddling in Elections. We Do It, Too', *The New York Times*, 17 February 2018.
[24] Joseph Nye, 'Protecting Democracy in an Era of Cyber Information War', *Governance in an Emerging New World*, 13 November 2018, https://www.hoover.org/research/protecting-democracy-era-cyber-information-war.
[25] Dov H Levin, 'When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results' (2016) 60 *International Studies Quarterly* 189.
[26] Ishaan Tharoor, 'The Long History of the U.S. Interfering with Elections Elsewhere', *The Washington Post*, 13 October 2016.
[27] Michael N Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19 *Chicago Journal of International Law* 30, 38.
[28] Shane (n 23).
[29] Sabrina Tavernise, Mark Landler and Helene Cooper, 'With New Afghan Vote, Path to Stability Is Unclear', *The New York Times*, 20 October 2009.
[30] Shane (n 23).

the United States was Radio Free Europe, a broadcasting station launched in 1950 aimed at audiences in the countries of the Warsaw Pact. While some maintain that the station, which continues to operate and is today based in Prague, provided 'very real journalism' with a 'transparent' agenda to promote 'democracy and human rights',[31] critics argue that Radio Free Europe's work during the Cold War is more accurately described as the waging of 'a subversive campaign to weaken Communist governments behind the Iron Curtain'.[32]

Cue the Soviets. In 1970 the KGB spread disinformation about politicians in Pakistan. Ahead of federal elections in Western Germany in 1980 the Soviet intelligence service falsely insinuated that the conservative candidate had ties to right-wing groups.[33] Since 1991 Russia has interfered in 27 elections. While initially focusing on post-Soviet states, the strategy shifted in 2014 when Moscow started attempts to influence electoral processes in Western countries. Observers have suggested that the primary goal of meddling with the internal affairs of states in the former communist sphere was to ensure a preference for candidates with policies that were favourable towards Russia.[34] Moscow's interferences in Western democracies relied more heavily on disinformation campaigns, although it is difficult to assess the impact that those information operations actually had on the results.[35]

According to Levin, electoral interference has more chance of succeeding if the adversarial state cooperates with a domestic actor in order to tap knowledge about the local political environment.[36] Information operations require a certain expertise about the specifics of a target country to have the chance to be successful. When these conditions apply, the data shows that the interfering operations can swing the vote by three per cent on average.[37] Interestingly, however, the numbers furthermore suggest that this effect in favour of the intervening power's preferred outcome is much more likely to manifest as a result of overt interference as opposed to a covert operation.[38]

3.1.2. DEVELOPMENT OF LEGAL PRACTICE

Being aware of the contentious and ongoing practice of the great powers and, in particular, the United States, most of the Eastern European and Latin American states, along with the vast majority of post-colonial and newly independent countries in Africa and Asia, became outspoken supporters of international rules against foreign interference.[39] At the same time, the exact

[31] Thomas Kent, 'Radio Free Europe's Mission', *The New York Times*, 20 October 2017.
[32] Kenneth Osgood, 'The C.I.A.'s Fake News Campaign', *The New York Times*, 13 October 2017.
[33] Dov H Levin, 'Sure, the U.S. and Russia Often Meddle in Foreign Elections. Does It Matter?', *The Washington Post*, 7 September 2016.
[34] Lucan A Way and Adam Casey, 'Russia Has Been Meddling in Foreign Elections for Decades. Has It Made a Difference?', *The Washington Post*, 8 January 2018.
[35] ibid.
[36] Levin (n 25) 190.
[37] ibid 193.
[38] ibid 200.
[39] Maziar Jamnejad and Michael Wood, 'The Principle of Non-Intervention' (2009) 22 *Leiden Journal of International Law* 345, 350.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

contours of an international prohibition of such conduct remained uncertain. While the famous Friendly Relations Declaration by the United Nations General Assembly from 1970 stated that 'every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State',[40] it also made clear that such *interference* would be considered an unlawful *intervention* only if conducted by way of *coercive* means.[41] To this day, the precise content of the requirement of coercion has continued to be a point of contention.

Two subsequent UN General Assembly resolutions – the 1976 Declaration on Non-Interference in the Internal Affairs of States and the 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States – attempted to circumscribe prohibited forms of foreign interference more precisely. Strikingly, they explicitly referred to information operations conducted by adversarial states through broadcasting or other media, denouncing 'campaigns of vilification' and 'subversion and defamation',[42] and 'any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States',[43] respectively. The 1981 Declaration even stipulated the 'right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news which can be interpreted as interference in the internal affairs of other States'.[44]

Still, it has been pointed out that neither General Assembly resolution can be considered a reflection of customary international law, as a large majority of Western states objected to their content. The 1981 Declaration was adopted with 102 votes to 22 (and 6 abstentions), only finding support from the states of the Warsaw Pact and the Non-Aligned Movement.[45] Part of the West's discomfort may have had to do with fears that a prohibition of interference by 'defamation' or 'hostile propaganda' would be interpreted too broadly by non-democratic states that were seeking to further restrict civil rights such as freedom of expression or freedom of information. Indeed, the Soviet Union frequently argued that the prohibition of intervention comprised all kinds of news coverage by Western media about the internal political affairs of socialist states, in effect trying to declare the work of Radio Free Europe as contrary to international law.[46] Fears of undue Western influence were also the principal motivation behind the Soviet Union's short-lived attempts to revive the rather obscure 1936 Convention on the Use

[40] UNGA Res 2625(XXV) (24 October 1970), Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, UN Doc A/Res/2625(XXV), Annex, (1) para 26.
[41] ibid, Annex, para 10.
[42] UNGA Res 31/91 (14 December 1976), Non-Interference in the Internal Affairs of States, UN Doc A/Res/31/91, preambular para 6.
[43] UNGA Res 36/103 (9 December 1981), Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of State, UN Doc A/Res/36/103, Annex, para II(j).
[44] ibid para III(d).
[45] Jamnejad and Wood (n 39) 355.
[46] Bruno Simma, 'Grenzüberschreitender Informationsfluß und domaine réservé der Staaten' (1979) 19 *Berichte der Deutschen Gesellschaft für Völkerrecht* 39, 63.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

of Broadcasting in the Cause of Peace,[47] finally ratifying it in 1982; however, the move had little to no effect.[48]

Restricting interference was also front and centre in the Final Act of the Conference on Security and Co-operation in Europe, which was held in Finland's capital Helsinki in 1975 and brought together almost all European states, including the Soviet Union and additionally the United States and Canada. The agreement stated that all participating states will 'refrain from any intervention … in the internal or external affairs falling within the domestic jurisdiction of another participating State'.[49] Like the Friendly Relations Declaration, it stressed that it understood 'intervention' as *coercive interference*, implying that interference without coercive means, such as media broadcasts, would not be proscribed. At least, that is how the participating Western states interpreted the Final Act. It has been pointed out that the Russian-language version of the text uses a word that denotes both 'non-intervention' and 'non-interference' [невмешательство], which can arguably be understood as outlawing interstate conduct that does not resort to coercive means.[50] This lack of clarity has marred the effect of the Final Act, which otherwise remains in force today.

In 1986, in its landmark *Nicaragua* decision, the International Court of Justice weighed in on the question of intervention and confirmed preceding state practice by emphasising that in order to be unlawful under customary international law, foreign interference must include an element of coercion:[51]

> 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. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention is particularly obvious in the case of an intervention which uses force.

Although 'coercion' arguably has never been adequately defined and is still an indistinct concept, the *Nicaragua* dictum remains the leading case on the issue.

As shown by the brief survey of the history of interference and intervention after the Second World War, the legal-political resistance against attempts at influencing by outside powers, including by means of information operations, was led principally by non-Western states. The

[47] International Convention concerning the Use of Broadcasting in the Cause of Peace (entered into force 2 April 1938) 186 LNTS 301, 197 LNTS 394, 200 LNTS 557.
[48] Björnstjern Baade, 'Fake News and International Law' (2019) 29 *European Journal of International Law* 1357, 1366–68.
[49] Conference on Security and Co-operation in Europe: Final Act (1 August 1975) (1975) 14 *International Legal Materials* 1292, s VI.
[50] Denitsa Raynova, 'Post Workshop Report: Towards a Common Understanding of the Non-Intervention Principle', European Leadership Network, October 2017, 2, https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/170929-ELN-Workshop-Report-Non-Intervention.pdf.
[51] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)* Merits, Judgment [1986] ICJ Rep 14, [205] (*Nicaragua*).

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

West, on the other hand, consistently regarded foreign interference as acceptable as long as it did not reach the blurry coercion threshold. It seems safe to assume that this legal position was informed by a feeling of moral and political superiority in the sense that anti-democratic or anti-liberal interference from non-Western states ultimately could not do much harm. However, the digital transformation that started in the late 1990s has fundamentally shifted this calculus.

3.2. A Paradigm Shift? Information Operations after the Digital Transformation

When asked in 2018 whether Russia had violated any international rules when it interfered in the 2016 presidential election in the United States, a former CIA agent answered staunchly in the negative, referring to his own country's long-standing practice of trying to influence political processes in foreign states[52] – a sentiment that is shared, notably, by US President Trump.[53] The question, however, is whether the digital transformation of the past two decades, with its ascent of social media platforms and the ensuing fundamental alterations of the global media ecosystem, requires a new and different legal assessment.

After a relatively brief period of widespread optimism about the potential of the internet to bring about a new era of a democratised information environment open to everyone,[54] and a new public sphere that no longer drowns the voices of those without the necessary access to participate in political debates,[55] a number of intertwined technological developments have quickly revealed more problematic aspects of the digitisation of society. While it may still be fair to argue that the public sphere today is, thanks to the internet, overall more inclusive than ever,[56] it is undeniable that democracies, in particular, have become more prone to manipulation.

The proliferation of digital media over the last twenty years has had profound effects both on the recipients and on the producers and disseminators of information, two aspects that are deeply interconnected. For the latter, digitisation and the global networks mean that news and other pieces of information can spread at greatly increased speed and considerably lower cost.[57] By default, communication now happens across borders, which enables actors to address audiences in foreign countries directly.[58] Social media platforms have organised this global public discourse horizontally, which means that the traditional media have lost their role as gatekeepers with supervising functions.[59] Everyone is able to communicate directly with everyone else,

[52] Shane (n 23).
[53] Shane Harris, Josh Dawsey and Ellen Nakashima, 'Trump Told Russian Officials in 2017 He Wasn't Concerned about Moscow's Interference in U.S. Election', *The Washington Post*, 27 September 2019.
[54] Nye (n 24).
[55] Michael Meyer-Resende, 'A New Frontier: Social Media/Networks, Disinformation and Public International Law in the Context of Election Observation', *Democracy Reporting International*, 2018, 5, https://democracy-reporting.org/wp-content/uploads/2018/10/A-new-frontier_social-media_election-observation_Briefing-Paper-by-Michael-Meyer-Resende.pdf.
[56] Bayer and others (n 2) 51.
[57] Nye (n 24).
[58] Bayer and others (n 2) 54.
[59] ibid 51.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

strengthening the position of hitherto marginalised voices and points of view; in this way, every person is able to distribute and amplify all political messages that suit them, with no regard for verifying the underlying facts.[60] We live in what has been dubbed a 'hyper-pluralistic information environment'.[61] At the same time, media users constantly leave traces of their online behaviour. The collected data enable interested parties to infer interests and political preferences, tapping a growing pool of intimate personal information that can be exploited for micro-targeting of receptive audiences.[62] As a result of developments in artificial intelligence, so-called bots can amplify political messages, including targeted pieces of disinformation, at a scale not imaginable for human agents.[63] They also make it easier to conceal the identity of the source of the information and the identity of its creator,[64] further muddying the waters of the contemporary information ecosystem.

The digital transformation has furthermore fundamentally altered the way in which information is received. The ease with which communication happens via digital channels has led to an 'information deluge',[65] which causes a constant feeling of being overwhelmed, making the attendance of a target audience the primary scarce resource that needs to be captured.[66] A recent market behaviour analysis of Taiwanese citizens showed that consumers spend no more than 40 to 60 seconds per article they encounter online,[67] which makes it fairly simple for interested actors to inject pieces of false or misleading information. As the large amounts of new information everyone has to process cause disorientation and confusion,[68] one almost natural cognitive defence strategy is to retreat into filter bubbles and echo chambers that reduce the information onslaught to digestible snippets of an ostensible reality, which does not come into conflict with one's own confirmation bias and aligns with one's view of the world.[69] In turn, these isolated islands of opinion can be exploited by outside actors in order to micro-target pliable voters with tailor-made sets of information.[70]

The distorted contemporary information environment leads to an erosion of the shared public sphere of societies and inhibits the ability of citizens to make informed political decisions.[71] What makes the situation entirely different from the Cold War era is that, because of their intrinsic openness, liberal democracies are inherently more vulnerable than authoritarian or totalitarian

[60] Weedon, Nuland and Stamos (n 17) 4.
[61] Bayer and others (n 2) 52.
[62] Nicholas Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace', *EJIL: Talk*, 26 August 2019, https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace.
[63] Meyer-Resende (n 55) 14.
[64] Bayer and others (n 2) 59.
[65] Lin and Kerr (n 1).
[66] Nye (n 24).
[67] Michael Cole, 'The Impact of China's Disinformation Operations Against Taiwan', *The Prospect Foundation Newsletter*, November 2018, http://bit.ly/341XHCq.
[68] Lin and Kerr (n 1).
[69] Bayer and others (n 2) 57 et seq.
[70] See Mostafa El-Bermawy, 'Your Filter Bubble Is Destroying Democracy', *Wired*, 18 November 2016, https://www.wired.com/2016/11/filter-bubble-destroying-democracy; Coppins (n 21).
[71] Bayer and others (n 2) 58.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

systems with tight public structures that can more easily control the streams of information. In this sense, the old asymmetry has been reversed;[72] and the problem is getting worse, with more and more interested actors learning the lessons of the foreign information operations prior to the unexpected results of the Brexit referendum and the 2016 US presidential election. The number of organised campaigns keeps increasing.[73]

3.3. Recent Approaches to Information Operations under International Law

Since the scale and quality of Russian attempts to conduct highly organised sustained information operations have come to the surface, a number of scholars of international law have started to reassess the legal qualification of foreign influencing. Acknowledging the described technological developments and the societal shifts that followed, a growing number of authors regard the previous evaluation, prevalent at least until roughly ten years ago, as no longer sufficient. Asking whether rules of current international law prohibit such conduct, the norms under particular scrutiny are the already mentioned prohibition of intervention, respect for the sovereignty of other states, and the principle of self-determination of peoples. The following section presents and examines the main arguments of the incipient debate.

3.3.1. Information Operations as Prohibited Intervention

Picking up past scholarship[74] and critically re-examining state practice during the Cold War period, a couple of scholars focus on a possible reinterpretation of the principle of non-intervention within the context of information operations and interference in internal decision-making processes. In its traditional scope of application, as shown, the rule is not understood as prohibiting every form of foreign interference.[75] Only if the interfering act intends to subordinate the target state's 'sovereign will'[76] in a coercive manner will the conduct qualify as prohibited intervention. As explained above, to this day it is undetermined what exactly counts as coercion in this sense.[77]

From a doctrinal standpoint the question, therefore, is whether information operations can ever qualify as *coercive*. Coercion within the scope of the prohibition of intervention is commonly understood as implying some form of compulsion,[78] which leads the target state to act

[72] Nye (n 24).
[73] Samantha Bradshaw, Lisa-Maria Neudert and Philip N Howard, 'Government Responses to Malicious Use of Social Media', *NATO Stratcom COE*, November 2018, 3, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/01/Nato-Report.pdf.
[74] See, in particular, Lori Fisler Damrosch, 'Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs' (1989) 83 *American Journal of International Law* 1.
[75] Robert Jennings and Arthur Watts, *Oppenheim's International Law* (9th edn, Oxford University Press 2008) 428.
[76] Jamnejad and Wood (n 39) 348.
[77] Sean Watts, 'International Law and Proposed U.S. Responses to the D.N.C. Hack', *Just Security*, 14 October 2016, https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack; Jamnejad and Wood (n 39) 367.
[78] Tsagourias (n 62).

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

in a way in which it would otherwise not have acted, or to take a decision it would otherwise not have taken,[79] such as when it bends to economic pressure or the threat of armed force.

Largely evading the issue, Barela argues that the value at stake – the 'significance and expanse, both in scale and reach, of the interests targeted'[80] – and not the mode of conduct should be decisive as to whether the act of a state reaches the threshold. As information operations that attempt to distort democratic decision-making processes target 'the legitimacy of the electoral process itself' and thus a '*sine qua non* for the state', this alone should be sufficient to consider the operation a violation of the principle of non-intervention.[81] In Barela's view, the Russian disinformation campaign ahead of the 2016 US presidential election – because of its 'expansive costs, planning and aims' and the fact that it made use of the 'vastly improved mechanisms for cross-border precision targeting of voters' – therefore qualifies.[82] However, while it is certainly expedient to take the value of the target into consideration when making an overall assessment of the conduct,[83] the argument is ultimately not persuasive. Given the explicit emphasis on the requirement of coercion by leading resolutions such as the Friendly Relations Declaration and the landmark *Nicaragua* judgment, the mode of conduct itself cannot simply be ignored entirely.

Acknowledging this, other scholars make an argument for interpreting the coercion criterion as encompassing *deceptive* state conduct. As the International Court of Justice has held that choices concerning a state's own internal affairs 'must remain free ones' and coercion exists when another state's conduct constrains this freedom,[84] a number of authors assert that manipulating state decisions by way of deception does fit within this description of coercion. According to Baade, information operations that utilise disinformation manipulate the 'capacity to reason'[85] and have to be considered coercive, as 'the projection of a different set of facts constrains one's freedom to act by making certain options and conclusions no longer seem viable or making others seem mandatory'.[86] Similarly, Nye argues that 'if the degree of manipulation is so deceptive that it destroys voluntarism, the act becomes coercive'.[87] This is the difference between an open propaganda operation (for example, by a state broadcasting organisation such as Russia's RT or China's Xinhua) and an information operation that deceives the target audience (for example, by concealing the identity of the source of a piece of information).[88] If the true identity of the person communicating the information remains hidden, the addressees are stripped of their ability to evaluate the trustworthiness of the information;[89] in this sense, deceit is merely the employed method that renders the effect – that is, the ultimate outcome of the election –

[79] Schmitt (n 27) 51.
[80] Steven J Barela, 'Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion', *Just Security*, 12 January 2017, https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion.
[81] ibid.
[82] Barela (n 22).
[83] See Raynova (n 50) 6.
[84] *Nicaragua* (n 51) 205.
[85] Baade (n 48) 1363.
[86] ibid 1364.
[87] Nye (n 24).
[88] ibid.
[89] Baade (n 48) 1364.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

coercive.[90] Proponents of this view assert that the threshold of coercion is reached if an information operation is covert, manipulating a democratic decision-making process by deceptively depriving the electorate of the opportunity to make genuinely informed choices[91] and thus of *control* over the choice of government.[92]

Other authors disagree with this wide understanding of 'coercion'. As the term implies compulsion with some degree of *forcible* conduct in the broader sense, deceptive manipulation by way of a disinformation campaign cannot be conceived as coercion.[93] Because the will of the target state is not subordinated, information operations do not amount to a violation of the principle of non-intervention.[94]

3.3.2. Information Operations and Sovereignty

In view of the difficulty in qualifying information operations as coercive conduct, Schmitt has suggested that they could instead be considered violations of the sovereignty of the target state. As a foundational concept of public international law, the principle of sovereignty safeguards each state's independence, which 'in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State', in the famous words of the Permanent Court of Arbitration in 1928.[95] The answer to the question of whether information operations against an adversarial state may violate that state's sovereignty depends principally on the more general question of whether 'respect for sovereignty' is a primary rule of international law alongside the prohibition of intervention.[96] If not, then naturally information operations cannot be in violation of that rule.

Legal opinions of scholarship and states seem undecided up to this point.[97] While the experts who drafted the widely quoted *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[98] and the UN Group of Governmental Experts on Developments in the Field of

[90] Dominik Steiger, 'International Law and New Challenges to Democracy in the Digital Age: Big Data, Privacy and Interferences with the Political Process' in Norman Witzleb, Janice Richardson and Moira Peterson (eds), *Big Data, Political Campaigning and the Law: Privacy and Democracy in the Age of Micro-Targeting* (2019) 22, https://ssrn.com/abstract=3430035.
[91] Schmitt (n 27) 51.
[92] Nicholas Tsagourias, 'Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behaviour, Power and Diplomacy* (Rowman & Littlefield 2020 forthcoming) 14, https://ssrn.com/abstract=3438567; see also Harriet Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention', *Chatham House Research Paper*, December 2019, 41–42.
[93] Jens D Ohlin, 'Election Interference: The Real Harm and the Only Solution', *Cornell Law School Research Paper* 18–50, 2018, 7.
[94] Tsagourias (n 62).
[95] *Island of Palmas* (*Netherlands v US*) 2 RIAA 829, 838 (1928).
[96] Schmitt (n 27) 40.
[97] For a good overview see Moynihan (n 92) 9.
[98] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) rr 1–4.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

Information and Telecommunications[99] have both come out in favour of assuming the existence of respect for sovereignty as a primary rule of international law, opinion among leading scholars remains divided.[100] More significantly, even likeminded states have not found common ground. In 2018 the UK Attorney General, Jeremy Wright, famously held that it is the 'UK Government's position that there is no such rule as a matter of current international law',[101] whereas France recently asserted that it assumes its existence.[102]

If sovereignty in itself can be violated by interfering with state conduct without regard to the threshold of coercion, then it might be put forward that information operations are in breach of the rule when they target and distort electoral processes, which belong to the 'inherently governmental functions'.[103] As a qualifying requirement, Schmitt refers to covert and thus deceptive methods: while overt propaganda by an adversarial state, though manipulative, is to be tolerated, the line towards a prohibited violation of sovereignty is crossed when activities conceal the source of the information or the identity of the communicator.[104]

3.3.3. INFORMATION OPERATIONS AND THE RIGHT TO SELF-DETERMINATION

Finally, two scholars more recently have suggested focusing not on the state-centred principles of sovereignty and non-intervention when it comes to legally qualifying information operations, but on the principle of self-determination of peoples.[105] Conceived as 'government for and by the people'[106] and considered a *conditio sine qua non* for the existence and validity of human rights,[107] the principle finds its origins in enlightenment philosophy and was first spelled out in the Declaration of Independence of the United States of America of 4 July 1776, which asserted that it is the 'consent of the governed' that gives a government its legitimacy.[108] Today, it finds its positive embodiment in international law in Article 1 of the International

[99] UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), UN Doc A/70/174, para 15.
[100] Michael N Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 *Texas Law Review* 1639 (in favour of respect for sovereignty as a primary rule); Gary P Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 *AJIL Unbound* 208 (against).
[101] Jeremy Wright, 'Cyber and International Law in the 21st Century', 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
[102] Ministère des Armées de la République Française, 'Droit International Appliqué aux Opérations dans le Cyberspace', 2019, 6–7.
[103] Schmitt (n 27) 45; see also Moynihan (n 92) 42–43.
[104] Schmitt (n 27) 46–47.
[105] Tsagourias (n 62); Jens D Ohlin, 'Did Russian Cyber-Interference in the 2016 Election Violate International Law?' (2017) 95 *Texas Law Review* 1579; Ohlin (n 93).
[106] Jan Klabbers, 'The Right To Be Taken Seriously: Self-Determination in International Law' (2006) 28 *Human Rights Quarterly* 186, 187.
[107] UN Human Rights Committee, General Comment 12, Article 1 (21st Session, 1984), Compilation of General Comments and General Recommendations; adopted by Human Rights Treaty Bodies (1994), UN Doc HRI/GEN/1/Rev.1, para 12.
[108] See Daniel Thürer and Thomas Burri, 'Self-Determination' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2012) 1.

Covenant on Civil and Political Rights (ICCPR):[109] 'All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development'.

Applied to the context of foreign interference by means of information operations, Tsagourias and Ohlin both hold that it is this right that is actually at stake. The premise of the argument is a somewhat idealised construction of the democratically constituted body politic that takes its cues from Habermas' *Theory of Communicative Action*:[110] if the principle of self-determination protects the right of a people to freely choose their political status without interference – in other words, the right to democratic decision-making – and this participatory and deliberative process requires the provision of factually accurate information about relevant political issues in order to be meaningful,[111] then information operations violate this fundamental, collective right of a state's citizens.

Taking this interpretation of the principle as their starting point, the two scholars attempt to separate legitimate information operations by foreign states from those of an illegitimate nature. Although their approaches differ, they arrive at similar conclusions. Tsagourias links the principle of self-determination to the prohibition of intervention, essentially arguing that because there is an inextricable connection between a state's sovereign authority and its people's right to self-government, the principle of non-intervention necessarily not only protects sovereignty *as such* against outside interference but also self-determination as its foundational element.[112] It follows that it must again be determined at what point such interference crosses the line into coercion and thus prohibited intervention. Similar to Baade and Nye, the decisive factor is supposedly the manipulative effect of the information operation: according to Tsagourias, the threshold of coercion is reached when the operation aims to curtail the free formation of the political will of the people by resorting to 'subterfuge', such as the spreading of 'false, fabricated, misleading, or generally manipulated information' with 'a certain degree of severity'.[113]

By contrast, Ohlin does not contend that the principle of self-determination mainly informs the prohibition of intervention in the context of information operations. Instead, he claims that such conduct may violate a people's right to self-determination in itself.[114] Crucially, in his opinion, what distinguishes legitimate from illegitimate communicative acts within the context of democratic decision-making processes is not so much the content of a piece of information but the identity of the speaker or author. Because the electorate's *self*-determination is at stake, only the political views and pieces of information disseminated by members of the collective count as significant. Discursive participation by outsiders – in other words, foreigners – is, from this perspective, inherently irrelevant. As soon as an outsider gains access to the political debate by *pretending to be an insider*, thus assuming relevance by deceiving the recipients of

[109] International Covenant on Civil and Political Rights (entered into force 23 March 1976) 999 UNTS 171.
[110] Jürgen Habermas, *The Theory of Communicative Action* (Beacon Press 1981).
[111] Bayer and others (n 2) 61–62.
[112] Tsagourias (n 62).
[113] ibid.
[114] Ohlin (n 93) 10.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

the information, the principle of self-determination is violated.[115] In other words, according to Ohlin, overt foreign attempts at influencing the outcome of an electoral process – for example, through broadcasting organisations such as RT – are supposedly *illegitimate*[116] yet ultimately harmless, as no member of the targeted body politic cares about the opinions of outsiders. On the other hand, this attitude changes once the same piece of information purportedly stems from an *inside* source: 'the work of the Russian troll farms only worked because the operators impersonated Americans'.[117] Covert participation in a foreign democratic decision-making process by means of an information operation is thus unlawful, while overt participation does not induce any considerable damage and is therefore to be tolerated.

Arguably, Ohlin's point is premised on an overly idealised representation of opinion formation within today's liberal-democratic societies. Faced with an ever-increasing information deluge that causes a continuously deepening fragmentation and polarisation of audiences[118] and decreasing trust in so-called 'mainstream media' and other traditional sources of information,[119] it overstretches confidence in the rationality of citizens concerning political decisions to assume that a propaganda outlet like RT, despite operating out in the open, does not hold any influence over the shaping of public opinion at all.[120] Furthermore, it is unclear how his construction can account for scenarios in which a foreign actor enlists domestic agents to execute the information operation within their own community, either by way of funding or by providing the tools necessary for a concerted disinformation campaign. Still, in line with the other scholars, Ohlin, of course, has a point when claiming that the danger of contemporary information operations that attempt to meddle with electoral processes lies in their covertness.

Schmitt counters that the principle of self-determination is not applicable to a people that has already successfully constituted its own state, as the right supposedly concerns itself only with situations in which a group is denied the right to self-governance – that is, with cases of colonialism, apartheid, alien subjugation, or occupation.[121] However, this limited understanding of self-determination arguably does not properly take into account the origins of the concept in enlightenment thought. Other contemporary scholars therefore argue more persuasively that the formation of an independent polity does not at all exhaust the constituent people's right to self-determination; the 'right subsists and continues to be vested in the people',[122] safeguarding the freedom to determine its political destiny without interference, if need be even against its own

[115] ibid 12–13.
[116] ibid 11.
[117] ibid 12.
[118] David Tewksbury and Jason Rittenberg, *News on the Internet: Information and Citizenship in the 21st Century* (Oxford University Press 2012) 119–43.
[119] Michael Schudson, 'The Fall, Rise, and Fall of Media Trust', *Columbia Journalism Review*, Winter 2019, https://www.cjr.org/special_report/the-fall-rise-and-fall-of-media-trust.php.
[120] Steven Erlanger, 'Russia's RT Network: Is It More BBC or K.G.B.?', *The New York Times*, 8 March 2017; Robert Elliot, 'How Russia Spreads Disinformation via RT Is More Nuanced Than We Realise', *The Guardian*, 26 July 2019.
[121] Schmitt (n 27) 55–57; similarly Steiger (n 90).
[122] Thürer and Burri (n 108) 22.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

government in the event that it turns away from democratic principles.[123] In this sense, after forming a state the constituent people transfers its inherent right to self-determination to a government which then exercises this right in relation to outside actors at the behest of the people.[124] Therefore, the state's sovereignty acts as a mediator of the people's self-determination and must be interpreted accordingly.[125] It functions as a shield against certain forms of outside interference – deceptive, manipulative conduct – and thus safeguards both the state itself and its people's right to free decision making. Although this position might not be considered a majority opinion within scholarship for the moment, the argument is able to explain convincingly why democratic processes within states should enjoy the protection of international law.

3.3.4. Conclusion

The digital transformation and the subsequent rise of information operations have prompted a growing number of international legal scholars to reappraise the legal qualification of foreign interference. While some authors seek to establish a new interpretation of 'coercion' that encompasses manipulative and deceptive conduct, others argue for a novel understanding of the concept of sovereignty. Instead of simply formulating a foundational principle of public international law, they submit that it should be read as creating a right that offers states legal protection beyond the more restrictive principle of non-intervention. This view draws on recent trends in legal works dealing with state conduct in cyberspace more generally. The theoretically most intriguing strand of scholarship applies a liberal understanding of the principle of self-determination of peoples and utilises it to reinterpret either the notion of 'coercion' or the sovereignty of states. Although the approaches differ in terms of their legal argumentation, it is noteworthy that all try to capture the scale and quality of deceptive and manipulative conduct as the crucial development of information operations since the dawn of the digital society.

3.4. Emerging State Practice: Shifting Attitudes towards an Emerging Prohibition of Information Operations?

3.4.1. Formation of Customary International Law and Determination of the Content of Existing Rules

While the exercise of assessing scholarly approaches is worthwhile, given the long history of attempts to interfere in the domestic political affairs of other countries, it will ultimately be up to states to react – both legally and factually – to the new reality after the digital transformation. It therefore must be examined what kind of information operations are considered legitimate

[123] See Hua Fan, 'The Missing Link between Self-Determination and Democracy: The Case of East Timor' (2008) 6 *Northwestern Journal of International Human Rights* 176.
[124] Samantha Besson, 'Sovereignty' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2012) 67.
[125] Tsagourias (n 92).

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

today, and what conduct, although antagonistic, is still tolerated within the international community. Despite past conduct to the contrary, have states' legal attitudes started to shift towards a more restrictive approach to adversarial political influence operations over the past few years? Of course, a potential change of legal opinion would be likely to signal not simply a necessary adaptation to the technological developments of the digital revolution. Since the end of the Cold War a greater emphasis on values such as democratic principles or human rights has emerged among a considerable number of states.[126] Nevertheless, the revelations concerning the impact of Facebook and other social media platforms on the formation of public opinion, and their susceptibility to manipulation by foreign actors, arguably count as the most important factors.

International rules emerge either through treaties or other formal agreements between states, or as customary international law. A rule of customary law is identified with the method of induction,[127] by inferring 'a general rule from a pattern of empirically observable individual instances of State practice and *opinio juris*'.[128] The latter, subjective element pertains to the question of whether a certain state accepts its behaviour in question 'as law' – that is, whether it considers acting in this way to be an obligation or a right.[129] Both elements must be present for a rule of customary international law to exist, and their presence in a given case must each be assessed separately, even though evidence for each might at times be derived from the same fact; *opinio juris* can itself not simply be inferred from certain state practice.[130] For this reason, when it comes to the legality of contemporary information operations under international law the starting point should be an examination of both the legal attitudes and actions of states towards conduct to that effect, and the relationship of the two factors in each case. However, the scholars cited above would claim, though not always explicitly, that the pertinent rules already exist – prohibition of intervention, respect for sovereignty, and the principle of self-determination – and that the appropriate method for determining the current state of law is to interpret the content of these standing rules and to apply them to the novel factual circumstances surrounding information operations after the digital transformation.[131]

The assertion that once a general rule of customary international law is established *as law*, it is subsequently capable of being applied to various unforeseen situations by way of deductive reasoning finds some support in both literature and the practice of international jurisprudence. For one, it makes methodological sense to open up customary rules for interpretation, as the alternative would effectively amount to a need to inductively re-identify the customary rule in each single instance of application, which would hardly make sense.[132] In line with this argument, it has

[126] Jamnejad and Wood (n 39) 349.
[127] *North Sea Continental Shelf (Germany v Denmark and the Netherlands)*, Judgment [1969] ICJ Rep 1, [44].
[128] Stefan Talmon, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion' (2015) 26 *European Journal of International Law* 417, 420.
[129] See, in general, International Law Commission (ILC), Report of the 70th Session (30 April–1 June and 2 July–10 August 2018), UN Doc A/73/10, 124–25.
[130] ibid 126–27.
[131] In this sense explicitly Ohlin (n 93) 24–26.
[132] Panos Merkouris, 'Interpreting the Customary Rules on Interpretation' (2017) 19 *International Community Law Review* 126, 134 et seq.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

been observed that none other than the International Court of Justice itself has in the past engaged in interpreting the content of rules of customary international law without inductively invoking state practice.[133] This would indeed imply that the content of a customary rule can be modified after its inception by way of reinterpretation.[134]

At the same time, however, state practice can hardly be disregarded when it comes to the operation of deductive reasoning itself. If interpretation of customary international law indeed bears a family resemblance to the corresponding method of interpreting the content of treaty law so that the 'method of logical and teleological interpretation can be applied in the case of customary law as in the case of written law',[135] then it should equally follow that, for the sake of consistency, the interpretative tool of 'any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation' (Article 31(3)(b) of the Vienna Convention on the Law of Treaties)[136] must find a counterpart in the appropriate interpretation of a customary rule as well.

If state practice is undisputedly relevant both for the formation of a rule of customary international law and for the interpretation of a treaty provision,[137] then it cannot be irrelevant for the interpretation of a customary rule. Despite the apparent practice of the International Court of Justice to the contrary, declarations of state representatives substantiate this argument. A case in point is France's recent official position paper on the applicability of international law to cyber operations, in which it explicitly acknowledges the significant contribution on the matter provided by the international group of experts who drafted the *Tallinn Manual 2.0*, while at the same time implying that such scholarly work is ultimately outweighed by the opinions of the states themselves.[138] Accordingly, France deviates from the experts' legal interpretation on a number of issues. The former Legal Adviser to the US State Department echoed this sentiment. In his view, when it comes to customary international law, it is the states themselves that have the 'primary responsibility for identifying how existing legal frameworks apply' and to 'publicly articulate applicable standards'. 'Interpretations or applications of international law proposed by non-governmental groups', on the other hand, 'may not reflect the practice or legal views of many or most States'.[139] Thus, while the content of existing rules of customary international law to a certain extent may be determined by way of deductive reasoning 'as an aid, to be

[133] A Mark Weisburd, 'The International Court of Justice and the Concept of State Practice' (2009) 31 *University of Pennsylvania Journal of International Law* 295, 327.
[134] Christian Delev, 'Throw Custom to the Wind: Examining the Life Cycle of Customary International Law in the Absence of a Custom-Making Moment', *Cambridge Journal of International Law Online*, 17 October 2019, http://cilj.co.uk/2019/10/17/throw-custom-to-the-wind-examining-the-life-cycle-of-customary-international-law-in-the-absence-of-a-custom-making-moment.
[135] *North Sea Continental Shelf* (n 127) dissenting opinion of Judge Tanaka, [181].
[136] Vienna Convention on the Law of Treaties (entered into force 27 January 1980) 1155 UNTS 331 (VCLT).
[137] Weisburd (n 133) 295.
[138] Ministère des Armées (n 102) 5.
[139] Brian J Egan, 'International Law and Stability in Cyberspace' (2017) 35 *Berkeley Journal of International Law* 169, 171–73.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

employed with caution',[140] the primary pieces of evidence for interpretation must remain the practice and public opinions of states in relation to the content of the rule in question.[141]

3.4.2. EVIDENCE OF STATE PRACTICE AND *OPINIO JURIS* IN RELATION TO INFORMATION OPERATIONS

On this basis, the following section examines current attitudes and behaviour towards information operations. In doing so, the present study will attempt to derive general conclusions concerning the lawfulness and legitimacy of information operations according to the legal opinions and practice of states. While this survey can hardly be exhaustive, a specific focus on official statements and domestic measures – such as national legislation – may allow for inferences concerning a possible nascent rule against information operations.

Strikingly, if perhaps not at all surprisingly, the clearest qualification of foreign influence as generally being in conflict with international law has come from some of the countries that are most frequently accused of engaging in adversarial information operations themselves. In January 2015 the six member states of the Shanghai Cooperation Organization (SCO) – China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan – submitted the second version of their 'International Code of Conduct of Information Security' to the Secretary-General of the United Nations.[142] Originally drafted in 2011, the non-binding Code of Conduct is explicitly 'open to all States' and has the 'purpose … to identify the rights and responsibilities of States in the information space'.[143] Of the acts that are deemed to be in contradiction to these rights and responsibilities the document includes the 'use of information and communications technologies and information and communications networks' in order 'to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability'.[144] Constituting an application of the principle of strict 'digital sovereignty' as promoted by these states,[145] this legal standpoint is, of course, in line with their more general anxiety towards a purportedly overbearing and intrusive influence of 'Western universal values'. As shown earlier, such vocal rejection of foreign influence by way of modern communication technologies was already directed against the activities of Radio Free Europe during the Cold War[146] and continues to this day, the latest evidence being Russia's assertion that YouTube's hosting of protest announcement videos amounted to 'interference in its sovereign affairs' and 'hostile influence (over) and obstruction of democratic elections in Russia' in August 2019.[147] China, too, has

[140] ILC (n 129) 126.
[141] ibid 124 onwards.
[142] 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 (13 January 2015), UN Doc A/69/723.
[143] ibid.
[144] ibid para 2(3).
[145] Sarah McKune, 'An Analysis of the International Code of Conduct for Information Security', *The Citizen Lab*, 28 September 2015, https://citizenlab.ca/2015/09/international-code-of-conduct.
[146] Osgood (n 32).
[147] 'Russia Tells Google Not To Advertise "Illegal" Events after Election Protests', *Reuters*, 11 August 2019, https://reut.rs/2pBdVDy.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

repeatedly connected vocal support for the democratic movement in Hong Kong over the summer of 2019 to prohibited outside interference by Western actors.[148]

In comparison, official statements and measures by liberal-democratic states have been much more restrained. Despite general acknowledgement that Russia did indeed run an expansive and intrusive adversarial information operation ahead of the 2016 presidential election in order to manipulate its outcome, to date there has been no government-level assertion that the United States considers such conduct to be a violation of its sovereignty[149] or otherwise a violation of a standing rule of international law.[150] After Russia's conduct had first come to light, President Barack Obama merely stated that Moscow had attempted to 'undermine established norms of behaviour' and to 'interfere with democratic governance'.[151] Given its reluctance to assert itself more emphatically, there have even been doubts as to whether the United States currently views such operations as a proper national security concern.[152] Indeed, in the words of a former CIA operative: 'If you ask an intelligence officer, did the Russians break the rules or do something bizarre, the answer is no, not at all'.[153] According to a former Legal Adviser to the US State Department, this assessment would shift only if another state's conduct interfered with the ability to even hold an election or directly manipulated the results of an election, which would amount to a violation of the principle of non-intervention.[154]

Other states have shown similar restraint. While Japan has implied that it would be interested in developing international rules on the matter, it has not taken the initiative, and the scope of its own legal standpoint is unclear.[155] With two much-noted legal briefs, both France and the Netherlands have recently clarified their opinions on the application of rules of international law to cyber operations.[156] Although they affirmed the emergent legal view that respect for sovereignty is indeed a standalone rule under international law, in opposition to the UK,[157] neither spelled out what that would mean in practice, especially with regard to an information operation

[148] Steven Lee Myers, 'In Hong Kong Protests, China Angrily Connects Dots Back to U.S.', *The New York Times*, 5 September 2019.
[149] Robert Morgus and Justin Sherman, 'When to Use the "Nuclear Option"? Why Knocking Russia Offline Is a Bad Idea', *Just Security*, 17 May 2019, https://www.justsecurity.org/64094/when-to-use-the-nuclear-option-why-knocking-russia-offline-is-a-bad-idea.
[150] Jack Goldsmith, 'Uncomfortable Questions in the Wake of Russia Indictment 2.0 and Trump's Press Conference with Putin', *Lawfare*, 16 July 2018, https://www.lawfareblog.com/uncomfortable-questions-wake-russia-indictment-20-and-trumps-press-conference-putin.
[151] Schmitt (n 27) 39.
[152] Jessica Brandt and Joshua Rudolph, 'A New National Security Framework for Foreign Interference', *Just Security*, 27 September 2019, https://www.justsecurity.org/66357/a-new-national-security-framework-for-foreign-interference.
[153] See Shane (n 23).
[154] Egan (n 139).
[155] 'Japan Plans To Take Steps against "Fake News" by June', *The Japan Times*, 14 January 2019, http://bit.ly/2PImnvf.
[156] Ministère des Armées (n 102); Government of the Netherlands, 'Letter to the Parliament on the International Legal Order in Cyberspace', 5 July 2019, 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.
[157] Wright (n 101).

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

aimed at influencing a democratic decision-making process. For their part, European Union officials, worried that foreign disinformation campaigns might interfere in the May 2019 European parliamentary elections, implemented a number of countervailing measures[158] but otherwise remained equally ambiguous as to their legal views on the matter. While stating that the 'risk of … targeted disinformation campaigns by foreign actors to influence public support or to undermine our democracies is growing',[159] a clear framing in legal language has been missing. In his State of the Union address in 2018, President of the European Commission Jean-Claude Juncker went as far as declaring illegal the 'use of personal data in order to deliberately influence the outcome of the European elections',[160] yet the appropriate framework for that would arguably be the Union's General Data Protection Regulation[161] rather than international law. When outlining her forthcoming political agenda, his successor, Ursula von der Leyen, flagged 'the threats of external intervention in our European elections' as one of the most pressing concerns for the coming years,[162] but the use of the word 'intervention' in itself can hardly count as an assertion of a legal standpoint.

The G7, on the other hand, arguably has been a little more forthright. The 2018 summit in Canada was concluded with the adoption of the 'Charlevoix Commitment on Defending Democracy from Threats', in which the member states declared[163] that:

> democracy and the rules-based international order are increasingly being challenged by authoritarianism and the defiance of international norms. In particular, foreign actors seek to undermine our democratic societies and institutions, our electoral processes, our sovereignty and our security.

Two preparatory documents, agreed by the foreign and security ministers of the G7 states, explicitly address 'disinformation' and speak of 'acts or measures by foreign actors with the malicious intent to undermine the confidence in, and the legitimacy of, democratic institutions and processes'[164] that constitute 'interference'.[165] The accompanying commitment was re-emphasised

[158] See below.
[159] European Commission, 'Communication from the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions, Europe in May 2019: Preparing for a More United, Stronger and More Democratic Union in an Increasingly Uncertain World', 30 April 2019, 22, http://bit.ly/2pCaGf8.
[160] European Commission, 'A Europe that Protects: The EU Steps Up Action Against Disinformation', Press Release, 5 December 2018, https://europa.eu/rapid/press-release_IP-18-6647_en.htm.
[161] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
[162] Ursula von der Leyen, 'A Union that Strives for More: My Agenda for Europe', 2019, 21, http://bit.ly/2NBaNzv.
[163] G7, 'Charlevoix Commitment on Defending Democracy from Foreign Threats', 9 June 2018, https://www.mofa.go.jp/files/000373846.pdf.
[164] G7, 'Defending Democracy: Addressing Foreign Threats', 23 April 2018, http://www.g8.utoronto.ca/foreign/180423-democracy.html.
[165] G7, 'Foreign Ministers Joint Communiqué', 23 April 2018, http://www.g8.utoronto.ca/foreign/180423-communique.html.

at the most recent G7 foreign ministers meeting in St Malo in France.[166] Although the use of the term 'interference' could signal the gradual shift towards a *legal* condemnation of information operations, thus constituting an expression of *opinio juris*, it bears noting that the avoidance of 'intervention' is arguably significant.

Ahead of the elections in Israel in April 2019, the head of the Israeli Security Agency alluded vaguely to a foreign state's intention to 'intervene in Israel's election via hackers and cyber technology'.[167] A former senior intelligence official considers the distortion of information 'the greatest threat of recent years' that 'threatens the basic values that we share – democracy and the world order created since World War Two'.[168] The remarks can, however, hardly count as expressions of legal opinion and it is unclear how members of the Israeli government have positioned themselves towards the problem. Probably the most straightforward legal language to date, as far as liberal-democratic countries are concerned, has come from Australia. After former prime minister Turnbull asserted that 'foreign powers are making unprecedented and increasingly sophisticated attempts to influence the political process, both here and abroad',[169] the Attorney General at the time elaborated that 'covert foreign influence can cause immense harm to our national sovereignty, to the safety of our people, to our economic prosperity, and to the very integrity of Australian democracy'.[170]

Given that official statements as expressions of *opinio juris* have been ambiguous or non-committal at best, a deeper look at domestic measures against foreign influence operations as instances of state practice might be pertinent in order to assess states' attitudes towards the issue. In this regard it has been suggested that national legislation or other countervailing means 'do not resolve the independent question of whether the activity violates international law'.[171] A frequently cited case in point is that of peacetime espionage. Although intelligence gathering by foreign agents is criminalised in virtually all domestic legal systems, it is commonly not perceived as a violation of a rule of international law in and of itself.[172] By implication, the fact that espionage is prohibited domestically has no bearing on its legal status under international law, not least because of the observation that all states engage in some sort of intelligence collection on other countries. On the other hand, it has long been recognised that domestic acts, including legislation, may under certain circumstances indeed count as state

[166] G7, 'Foreign Ministers Communiqué', 6 April 2019, http://www.g7.utoronto.ca/foreign/190406-communique.html.
[167] '"Foreign Country" Intends to Intervene in Israeli Elections, Shin Bet Chief Says', *Ha'aretz*, 8 January 2019, http://bit.ly/2C8lZhN.
[168] See Ruth Levush, 'Initiatives to Counter Fake News in Selected Countries: Israel', The Law Library of Congress, April 2019, 41, 44.
[169] 'Australia Passes Foreign Interference Laws amid China Tension', *BBC News*, 28 June 2018, https://www.bbc.com/news/world-australia-44624270.
[170] Gareth Hutchens, 'Brandis Reveals Plans to Curb "Unprecedented" Foreign Influence on Politics', *The Guardian*, 14 November 2017.
[171] Egan (n 139).
[172] A John Radsan, 'The Unresolved Equation of Espionage and International Law' (2007) 28 *Michigan Journal of International Law* 595, 601 et seq; but see critically Jared Beim, 'Enforcing a Prohibition on International Espionage' (2018) 18 *Chicago Journal of International Law* 647.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

practice that informs the formation of international law.[173] This must at least hold true if an internal act communicates a legally significant value judgment on an issue that concerns the transnational realm, as in the case of human rights matters.[174] That is the principal difference from the question of the legality of espionage. Whereas the latter practice at most concerns another state's territorial integrity,[175] domestic measures with the aim of safeguarding a human right as an internationally protected value should be considered expressions of legal views towards the existence of a rule of customary international law. As there are good reasons in favour of arguing that information operations that intend to influence the political will of another country's population infringe the latter's (collective) right to self-determination, as shown above, countervailing measures at the domestic level should, under certain circumstances, be considered state practice.

However, an important distinction should be made between such internal measures against information operations that explicitly address outside threats, on the one hand, and such measures that constitute blanket prohibitions or restrictions of 'fake news' or the dissemination of 'misleading' information, on the other. Aside from the observation that the latter are in fact often enacted by authoritarian regimes that exploit the language surrounding the problem of disinformation for the sole purpose of targeting opposition groups and to generally stifle freedom of speech,[176] such acts also do not convey a legal standpoint specifically about the conduct of foreign actors. For instance, an abuse of legal frameworks ostensibly directed against disinformation in order to persecute political dissidents has already been observed in Iran, Malaysia, Russia, Saudi Arabia and Tanzania.[177] In early 2018 Vietnam announced the establishment of a military cyber unit tasked to act against 'wrong views'.[178] Other countries – such as Egypt, Indonesia and Kuwait – also focus on criminalising the dissemination of disinformation online without distinguishing between external and internal threats.[179] Although Singapore's senior minister of state for law invoked language that alluded to international relations when he spoke of 'asymmetric information warfare' that no country is immune from,[180] the city state went on to enact one of 'the most comprehensive

[173] ILC (n 129) 132.
[174] For this see, eg, Rebecca J Cook and Lisa M Kelly, 'Polygyny and Canada's Obligations under International Human Rights Law', *Department of Justice Canada*, 2006 (analysing national attitudes towards polygyny in order to derive a rule of customary human rights law).
[175] Beim (n 172) 653.
[176] See Rachel Blundy, 'Tactics to Fight Disinformation in Thailand, Indonesia, Japan, The Philippines and India', *Global Ground Media*, 23 April 2019, https://www.globalgroundmedia.com/2019/04/23/tactics-to-fight-disinformation-in-thailand-indonesia-japan-the-philippines-and-india; Emma Goodman, 'The Online Harms White Paper: Its Approach to Disinformation, and the Challenges of Regulation', *LSE Media Policy Project Blog*, 10 April 2019, https://blogs.lse.ac.uk/medialse/2019/04/10/the-online-harms-white-paper-its-approach-to-disinformation-and-the-challenges-of-regulation; Peter Roudik, 'Initiatives to Counter Fake News in Selected Countries: Comparative Summary', The Law Library of Congress, April 2019, https://www.loc.gov/law/help/fake-news/index.php.
[177] Bradshaw, Neudert and Howard (n 73) 8.
[178] 'Vietnam Unveils 10,000-Strong Cyber Unit to Combat "Wrong Views"', *Reuters*, 4 January 2018, http://bit.ly/2C9LTS6.
[179] Bradshaw, Neudert and Howard (n 73) 8.
[180] Nick Bonyhady, 'Australian Anti-Foreign Interference Laws a Model for Singapore', *The Sydney Morning Herald*, 5 March 2019.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

anti-misinformation laws in the world' in May 2019,[181] with terms of imprisonment of up to ten years for spreading false information.[182] The law has been criticised as severely suppressing free speech.[183] At the same time some liberal-democratic countries are among those whose response to the emerging problem of the distortion of the digital information ecosystem has focused on the threats in more non-specific terms as well. Ahead of the recent presidential election, Argentina launched the Commission for the Verification of Fake News (*Comisíon de Verificación de Noticias Falsas*) as part of the *Cámara Nacional Electoral* (CNE) with a mandate to carry out neutral fact-checking of news publications, to report false information to the CNE, and to appeal to service providers to curb the spreading of disinformation.[184] In neighbouring Brazil the police announced that it would 'identify and punish the authors of "fake news"' in the run-up to the 2018 presidential election.[185]

To date, only a relatively small number of states have set up domestic measures with the explicit aim of countervailing information operations carried out by foreign actors. As argued, these examples may count as legally significant in the search for an emergent customary international norm against such conduct. Within this context it is remarkable that despite the reluctance of its leaders to unambiguously call out Russia's interfering campaigns as unlawful, the United States has implemented various steps to counteract foreign interference. It explicitly declares foreign influence operations 'illegal' and promises to 'investigate, disrupt, and prosecute perpetrators'.[186] In late 2017 the US Federal Bureau of Investigations established the Foreign Influence Task Force (FITF) to counter foreign information operations.[187] The National Defense Autorization Act (NDAA) of 2019 included provisions that emphasise that acting against information operations is a national security concern.[188] In the aftermath of the 2016 election the US Department of the Treasury imposed sanctions on Russian entities and actors connected with the extensive efforts to interfere on behalf of Donald Trump.[189]

[181] Daniel Funke and Daniela Flamini, 'A Guide to Anti-Misinformation Actions Around the World', *Poynter*, 2019, https://www.poynter.org/ifcn/anti-misinformation-actions.
[182] 'Singapore "Fake News" Law Set to Come into Force on Wednesday, *Reuters*, 1 October 2019, https://reut.rs/2WDWzC8.
[183] Salil Tripathi, 'Singapore: Laboratory of Digital Censorship', *NYR Daily*, 19 July 2019, https://www.nybooks.com/daily/2019/07/19/singapore-laboratory-of-digital-censorship.
[184] Lucas Robinson, 'Fake News Persists in Argentina as Election Draws Near', *Buenos Aires Times*, 14 September 2019, https://www.batimes.com.ar/news/argentina/fake-news-persists-in-argentina-as-election-draws-near.phtml.
[185] Melanie Ehrenkranz, 'Brazil's Federal Police Says It Will "Punish" Creators of "Fake News" Ahead of Elections', *Gizmodo*, 10 January 2018, https://gizmodo.com/brazil-s-federal-police-says-it-will-punish-creators-of-1821945912.
[186] US Department of Justice, *Justice Manual*, Title 9: Criminal, 9-90.730 – Disclosure of Foreign Influence Operations, September 2018, https://www.justice.gov/jm/jm-9-90000-national-security#9-90.730.
[187] FBI, 'What We Investigate' (undated), https://www.fbi.gov/investigate/counterintelligence/foreign-influence.
[188] US Government Publication Office, 'National Defense Authorization Act for Fiscal Year 2019', 13 August 2018, https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
[189] Alina Polyakova and Daniel Fried, 'Democratic Defense Against Disinformation 2.0', *Atlantic Council*, 2019, 9, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic_Defense_Against_Disinformation_2.0.pdf.

Although the existing legislation has been criticised as too broad and vague, Canada explicitly considers foreign interference in its elections unlawful.[190] So does Australia, with laws that provide for the punishment of anyone accountable for communicating false or distorted content directed against the 'national interest', and an Election Integrity Task Force was established to thwart malicious information operations from abroad.[191] Adhering to its commitment made during the 2018 G7 summit, Canada has also set up a dedicated Rapid Response Mechanism with the task of analysing ongoing disinformation campaigns.[192] The British government has created the National Security Communications Unit, 'tasked with combating disinformation by state actors and others' in order to 'systematically deter our adversaries and help us deliver on national security priorities'.[193] A similar task force has been installed in Denmark, responsible for countering systematic information operations, in particular, but not limited to coming from foreign entities.[194] Sweden's response has been even more unambiguously aimed at external actors. The country's new 'psychological defence' authority is supposed to identify, analyse and confront foreign influence operations.[195] Sweden clearly considers adversarial information operations by foreign powers a threat to public safety potentially on a par with acts of armed force, counting them as 'attacks directed against our country' that the populace must be prepared to 'resist'.[196] Finally, the European Union has established the EastStratCom unit, which is based in Brussels with the explicit mandate to identify and expose antagonistic Russian behaviour against the European information space. Ahead of the 2019 European Parliament elections, a new Rapid Alert System was established, tasked with exposing ongoing disinformation campaigns. It is linked to governmental agencies of all member states and is intended to exchange real-time information with authorities of NATO and G7 states.[197]

As the survey shows, it is not that the growing problem of false and misleading information has not been acknowledged globally by now. However, the differences between the measures imposed by states to confront the issue are striking. Other than the degree of domestic adherence to human rights standards, the main distinction may come down to threat perception. The more that societies feel at risk of being targeted by outside actors, the more domestic means such as legislation or task forces are outward-looking. To be sure, perception in itself does not necessarily reflect reality. Some states that have imposed strong rules to hamper foreign interference in fact might not be on the radar of any antagonistic actor. On the other hand, there now appear to be states that are targeted without being fully aware of the circumstances: *The New York*

[190] Standing Senate Committee on Legal and Constitutional Affairs, 'Controlling Foreign Influence in Canadian Elections', June 2017, 2, http://publications.gc.ca/collections/collection_2017/sen/yc24-0/YC24-0-421-17-eng.pdf.
[191] Funke and Flamini (n 181).
[192] Polyakova and Fried (n 189) 7.
[193] 'Government Announces Anti-Fake News Unit', *BBC News*, 23 January 2018.
[194] Funke and Flamini (n 181).
[195] ibid.
[196] Swedish Civil Contingencies Agency, 'If Crisis or War Comes: Important Information for the Population of Sweden', May 2018, 12.
[197] Polyakova and Fried (n 189) 5.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

Times reported in October 2019 that a number of African countries had recently been affected by Russian information operations.[198] Still, countervailing measures on the continent have focused largely on domestic issues or the problem of online disinformation more generally. Sudan, which was allegedly among the targeted countries, enacted a bill against 'fake news' in 2018, which was criticised for stifling freedom of expression.[199] Nevertheless, those – mostly Western – countries that have implemented means explicitly aimed at outside threats at least implicitly express a viewpoint against the lawfulness of foreign information operations targeting their body politic.

3.5. Assessment: Current State of the Law

The foregoing analysis of recent scholarship and state practice allows for a number of conclusions.

The cited authors make a persuasive case for a reappraisal of the existing rules of international law, most significantly the prohibition of intervention and respect for state sovereignty. If the principle of non-intervention aims principally to protect a state's freedom to make its own political decisions, then it is reasonable to conclude that in the age of globalised digital media and means of communication, the strict focus on 'coercion' as the only way to conceive of severe constraints on that freedom is overly limited. Although not coercive in the traditional understanding of the concept, covert manipulation via digital media is just as capable of forcing another state's political will, so it might be high time to broaden the notion.

The conceptual connection made by some authors between a modern understanding of state sovereignty and the principle of self-determination of peoples as a collective human right might prove even more fruitful. It is not a completely new thought to consider sovereignty in the modern age without a meaningful interrelationship with self-determination an outdated and empty concept.[200] Yet the potential harm caused by information operations that interfere with democratic decision-making processes as the most significant manifestation of the self-determination of a sovereign populace exposes the connection between the two concepts more clearly than ever, and is certainly a subject that is worth exploring further.

At the same time, the survey of current state practice reveals that it is presently in a state of flux at most. So far, even states that are directly affected by adversarial information operations have shown remarkable reluctance to express unambiguously a legal opinion concerning the qualification of such conduct. Therefore, while scholarly views on the topic are well defendable, neither the practice of states nor their expressions of *opinio juris* are sufficiently uniform and consistent to support such far-reaching conclusions.[201]

[198] Davey Alba and Sheera Frenkel, 'Russia Tests New Disinformation Tactics in Africa to Expand Influence', *The New York Times*, 30 October 2019.
[199] Abed Kataya, 'Do New Sudanese Laws Regulate Digital Space or Limit Freedom of Expression?', *SMEX*, 23 July 2018, https://smex.org/do-new-sudanese-laws-regulate-digitalspace-or-limit-freedom-of-expression.
[200] Besson (n 124) 121.
[201] ILC (n 129) 136.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

The reluctance of states to come out more straightforwardly against information operations stems presumably from two main, interconnected reasons. First, Western states are well aware of their own conduct, both in the past and in the present. Important global players such as the United States and the European Union routinely continue to engage in influencing other states and societies, either directly or through intermediaries like state-funded non-governmental organisations (NGOs) or media such as the aforementioned Radio Liberty. Overly outspoken rhetoric against foreign interference may threaten to further blur the line between open and transparent conduct on the one hand, and covert and manipulative conduct on the other. As evidenced by the Shanghai Cooperation Organization's International Code of Conduct, authoritarian states like Russia or China would agree to a complete international ban on the free global flow of information. This leads directly to the second consideration: the reasonable fear that any hard push-back against disinformation campaigns will end up further diminishing the already sorry global state of fundamental civil rights like freedom of speech and freedom of the media. Both considerations, taken together, explain why no liberal-democratic states aligned themselves with the Code of Conduct, ostensibly neutral and harmless language notwithstanding.

4. THE WAY FORWARD: PROSPECTS FOR INTERNATIONAL NORM BUILDING

To some extent, the preoccupation with the threat of foreign information operations targeting democratic decision-making processes is a replacement activity. As the past few years have shown very clearly, Western societies themselves bear a fair amount of anti-liberal elements that strive to undermine the post-war democratic consensus by challenging and manipulating common narratives via social media or other means of communication.[202] This does not mean that tackling foreign interference – which often attempts to exploit existing rifts within target societies by co-opting radical local actors[203] – is unnecessary or unproductive. On the contrary, internationally applicable rules can provide long-term solutions to our emerging post-truth realities that not least threaten the rules-based international order.[204] The preceding analysis has established that existing legal frameworks are so far insufficient.[205]

However, from the outset, all actors involved should acknowledge that *international* rules addressing the issue are most likely not to mean *universal* rules. As shown by the collapse of the 2017 UN Group of Government Experts process to establish common ground regarding

[202] eg, for the US, Coppins (n 21).
[203] See Casey Michel, 'The Kremlin's California Dream', *Slate*, 4 May 2017, https://slate.com/news-and-politics/2017/05/why-russia-cultivates-fringe-groups-on-the-far-right-and-far-left.html; Michael Carpenter, 'Russia Is Co-opting Angry Young Men', *The Atlantic*, 29 August 2018, https://www.theatlantic.com/ideas/archive/2018/08/russia-is-co-opting-angry-young-men/568741.
[204] Alex Pascal and Tim Hwang, 'War Is as War Does: World Order and the Future of Conflict', *Just Security*, 26 August 2019, https://www.justsecurity.org/65959/war-is-as-war-does-world-order-and-the-future-of-conflict; on this concept more generally see Malcolm Chalmers, 'Which Rules? Why There Is No Single "Rules-Based International System"', *Royal United Services Institute*, April 2019, https://rusi.org/sites/default/files/201905_op_which_rules_why_there_is_no_single_rules_based_international_system_web.pdf.
[205] Raynova (n 50) 7.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

the application of international law to state cyber operations,[206] it is increasingly difficult to engage in truly far-reaching and comprehensive norm-finding mechanisms against the backdrop of the state of current great power relations on the international stage.[207] The widely shared observation concerning rules for cyber conduct – that 'governments haven't been willing to sign on to cyberwar limitation agreements because they don't want to limit their own freedom to launch cyberattacks at their enemies'[208] – arguably also holds true with regard to information operations. What is more, it plainly seems unrealistic to ever reach a shared understanding between liberal-democratic and authoritarian states on notions such as 'facts-based reporting' or 'objective journalistic standards', let alone 'the truth'.[209]

Fundamental disagreement on how to deal with disinformation is not at all limited to a gap between Western states and the rest of the international community. A second rift runs through the liberal-democratic community, more precisely between conceptions of free speech in the United States, on the one hand, and European states, on the other. Whereas the latter are quite comfortable and familiar with restricting certain manifestations of speech for the purpose of protecting other constitutionally protected values, the right to freedom of expression is understood much more expansively in the US;[210] some have dubbed this approach 'First Amendment fundamentalism'.[211] Adherents consider limitations on free speech to be a much greater threat to democratic principles than the manipulation of information by malicious actors.[212] Indeed, some even argue that the erosion of trust in freedom of speech and freedom of information in itself might be one of the ultimate goals of adversarial conduct by illiberal foreign actors:[213]

> By launching its information operations, the Kremlin is putting in place a logic that pushes the West into reversing the gains of the Cold War, particularly in the area of ending censorship and improving freedom of expression. The growth of information operations increases the sense that we can't trust anything we see online, strengthening a view that manipulation is all around us and leading to policies that do damage to the very democratic values that information operations were created to subvert.

In light of the above, any viable and realistic path forward must navigate the narrow space between, on the one hand, an informational order that allows for unrestrained meddling by

[206] Adam Segal, 'The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?', Council on Foreign Relations, 29 June 2017, https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.
[207] Moynihan (n 92) 55.
[208] Andy Greenberg, 'The Wired Guide to Cyberwar', *Wired*, 23 August 2019, https://www.wired.com/story/cyberwar-guide.
[209] Raynova (n 50) 7.
[210] Noah Feldman, 'Free Speech in Europe Isn't What Americans Think', *Bloomberg*, 19 March 2017, https://www.bloomberg.com/opinion/articles/2017-03-19/free-speech-in-europe-isn-t-what-americans-think; Michael Chertoff, 'Fake News and the First Amendment', *Harvard Law Review Blog*, 10 November 2017, https://blog.harvardlawreview.org/156-2.
[211] Quinn Mulholland, 'Fighting Words: The Free Speech Fundamentalists', *Harvard Political Review*, 6 April 2018, https://harvardpolitics.com/columns-old/fightwords1.
[212] Chertoff (n 210).
[213] Pomerantsev (n 3).

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

malicious actors in the democratic affairs of other countries by exploiting the possibilities of modern digital technologies, and an increasing fragmentation of the global information ecosystem, on the other – with more and more states asserting 'digital sovereignty', a concept that is often little more than a euphemism for restricting the civil rights of their citizens online.[214]

If a universal process involving all states is not feasible, the question is which actors should join in order to move ahead, and with what goal in mind. One obvious option is to invite only 'like-minded' liberal-democratic states to launch a norm-finding mechanism, which might then influence the emergence of rules on information operations that gradually develop a broader scope by consecutively binding more and more states. With regard to cyber norms, such a 'digital Alliance of Democracies' was recently proposed by former Danish Prime Minister and NATO Secretary-General Anders Fogh Rasmussen.[215] A clear downside is the risk that the agreed rules do not end up convincing any actor outside the initial alliance. The initiative would not necessarily be completely without merit, but its long-term impact is likely to be of quite limited value. A more open approach could, from the start, involve a greater number of states and not only liberal democracies in the strict sense. Such a 'coalition of the willing'[216] might face more difficulties in finding common ground concerning the substance of possible rules, but any tangible outcome is likely to benefit from greater acceptance globally. In this respect the most ambitious proposal might be the one presented by the German foreign minister in Tokyo in July 2018. In a speech he outlined the idea of an 'alliance of multilateralists' that 'defends existing rules together and continues to develop them where this is necessary' and in that way acts as an agent to 'shape' the rules of the international order.[217] Crucially, his vision does not seem to imply the exclusion of states with political systems that deviate from the Western liberal-democratic model. All that is necessary for participation would be a commitment to the rules-based international order and a willingness to work for its progressive development. Whether any of these models prove to be feasible or even desired by the states remains to be seen. In any case, despite laudable intentions and efforts, forums such as the G7 are arguably not sufficiently inclusive to make a considerable impact in terms of rule formation, the setting up of workable modes of collaboration to tackle the problem on an operational level notwithstanding.

The involvement of actors other than states should also be considered. Large platform providers and other online media companies like Facebook, Google and Twitter have an obvious stake in the development of norms for responsible behaviour vis-à-vis the dissemination of information

[214] See Sally Adee, 'The Global Internet Is Disintegrating. What Comes Next?', *BBC Future*, 15 May 2019, https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.

[215] Anders Fogh Rasmussen, 'The West's Dangerous Lack of Tech Strategy', *Politico*, 11 March 2019, https://www.politico.eu/article/opinion-the-wests-dangerous-lack-of-tech-strategy.

[216] Annegret Bendiek and Eva Pander Maat, 'The EU's Regulatory Approach to Cybersecurity', SWP Working Paper, October 2019, 24, https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf; Patryk Pawlak, 'The EU's Role on Shaping the Cyber Regime Complex' (2019) 24 *European Foreign Affairs Review* 167.

[217] Heiko Maas, 'Speech by Minister for Foreign Affairs, Heiko Maas at the National Graduate Institute for Policy Studies in Tokyo, Japan', 25 July 2018, https://www.auswaertiges-amt.de/en/newsroom/news/maas-japan/2121846.

via the internet as one of the core elements of contemporary information operations. The question is to what degree and in what way an institutionalised cooperation with such private business entities can be beneficial in the search for sustainable normative solutions at the international level. In the field of transnational cybersecurity, more generally, some companies, such as Microsoft, have recently started to move ahead and publish detailed proposals for legal frameworks for cyberspace.[218] However, proper coordination with states has often been lacking, an aspect that seems crucial for the context in hand. Nonetheless, the development of workable rules for the problem of the post-truth information ecosystem online can hardly be successful without taking into account the positions of private media companies as natural stakeholders.

As for the substance of possible international rules on information operations, outlining a few essential components will suffice for the purpose of this article. The association of norm-developing actors should clarify that they consider information operations targeting the integrity of democratic decision-making processes to be a violation of international law along the doctrinal lines spelled out by the above-cited scholars: as either a violation of sovereignty or a prohibited intervention under the assumption that manipulative cognitive warfare does indeed amount to 'coercion'. For either option the interpretative impact of the principle of self-determination as a collective and democratic human right should be emphasised. On the basis of this premise, the process of norm clarification or development should lay out workable and unambiguous criteria as to the distinction between legitimate and illegitimate influencing of other states and societies. It should be obvious that under the conditions of a globalised world society and global network infrastructures, there will be no going back to a state of complete non-interference (as if that had ever existed in the first place); nor should that be the goal: just like international trade, mutual exchange of information and cultural values across borders is beneficial for all actors and ultimately contributes to a more peaceful and secure international community.

For this reason, it is submitted that the international legal qualification of information operations targeting populations in other states should disregard the content of the information itself and the (political) values communicated – liberal-democratic or illiberal-authoritarian. Instead, as suggested by some authors,[219] the line should be drawn between information operations that employ communicative means that are open and transparent, on the one hand, and those that are covert, subversive, deceptive and manipulative, on the other. From an international legal standpoint the problem is not – and should not be – the truth-value of a certain disseminated piece of information; not least, this would imply the need for an impartial instance *at the international level* that authoritatively decides which communicative acts are 'true' and which are 'false' – indeed a troubling proposition from the perspective of liberalism and the right to free speech. The dissemination of information becomes manipulative when the identity of the speaker or its origin is obfuscated, depriving the addressees of their ability to investigate the speaker's possible aims and intentions. As correctly pointed out by Ohlin, this is where the right to self-

[218] See Louise Marie Hurel and Luisa Cruz Lobato, 'Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs' (2018) 3 *Journal of Cyber Policy* 61.
[219] Especially Ohlin (n 93).

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

determination is affected.[220] Recent legislative initiatives and judicial decisions in the United States (at both state[221] and federal levels[222]), Germany[223] and Israel[224] have highlighted this crucial aspect of transparency, which shows that there already exists some tangible support in state practice for this proposal. As recent electoral campaigns in democratic states have shown, authoritarian actors have figured out how to exploit existing vulnerabilities of open societies for information operations. More than attempting to regulate content, a number of experts suggest that increasing transparency can reduce the threat of manipulation.[225] Therefore, subversive and deceptive information operations, such as those carried out by the Russian Internet Research Agency, should be qualified as crossing the line into prohibited interference.[226] This argument finds further support in international human rights practice with regard to the right of political participation pursuant to Article 25 of the ICCPR. In its General Comment 25, the UN Human Rights Committee states that the right provides that 'voters should be able to form opinions independently, free of violence or threat of violence, compulsion, inducement *or manipulative interference of any kind*'.[227] Political participation of the individual citizen forms the foundation of the actualisation of a people's political self-determination; stifling the former by way of a manipulative use of information thus necessarily obstructs the latter and violates the state's sovereignty as the point of reference of the self-determination.[228] In light of this, it is submitted that liberal-democratic states should more prominently and jointly promote this reconfigured understanding of the international rules in question.

At the same time, it follows from this approach that Western liberal democracies must be ready to tolerate broadcasting activities by state outlets such as Russia Today or Xinhua in their own countries even if they evidentially spread disinformation,[229] just as much as

[220] ibid.
[221] See Noam Cohen, 'Will California's New Bot Law Strengthen Democracy?', *The New Yorker*, 2 July 2019, https://www.newyorker.com/tech/annals-of-technology/will-californias-new-bot-law-strengthen-democracy.
[222] Bradley Hanlon and Laura Rosenberger, 'Countering Information Operations Demands a Common Democratic Strategy', *Alliance for Securing Democracy*, 14 October 2019, https://securingdemocracy.gmfus.org/countering-information-operations-demands-a-common-democratic-strategy.
[223] Markus Reuter, 'Was nicht erkannt werden kann, sollte nicht reguliert werden', *netzpolitik.org*, 9 May 2019, https://netzpolitik.org/2019/social-bots-was-nicht-erkannt-werden-kann-sollte-nicht-reguliert-werden.
[224] Toi Staff, 'Election Judge Bars Anonymous Internet Ads Despite Likud Objection', *The Times of Israel*, 23 February 2019, https://www.timesofisrael.com/election-judge-bars-anonymous-internet-adds-despite-likud-objection.
[225] Hanlon and Rosenberger (n 222); Robert D Blackwill and Philip H Gordon, 'Containing Russia: How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge', Council on Foreign Relations, January 2018, 21, https://backend-live.cfr.org/sites/default/files/report_pdf/CSR80_BlackwillGordon_ContainingRussia.pdf; Elizabeth Bodine-Baron and others, 'Countering Russian Social Media Influence', RAND Corporation, 2018, 32–36, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2740/RAND_RR2740.pdf.
[226] See tentatively likewise Moynihan (n 92) 43.
[227] UN Human Rights Committee, General Comment 25 to the ICCPR (12 July 1996), UN DOC CCPR/C/21/Rev.1/Add.7 (emphasis added).
[228] See similarly Bayer and others (n 2) 61–63.
[229] Similarly, Nye (n 24).

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

authoritarian states cannot claim a violation of their sovereignty in the face of the operation of Radio Liberty or other public Western broadcasters, YouTube hosting inconvenient videos by oppositional activists, or the presence of publicly funded civil rights NGOs on their territories.

Any attempt to regulate the growing problem of disinformation, information operations and cognitive warfare – at both the international and domestic levels – potentially puts democratically essential civil rights at risk. As clarified by the 2017 Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda,[230] 'the human right to impart information and ideas is not limited to "correct" statements'. For this reason, human rights experts stress that 'general prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression'.[231] By focusing on the mode of conduct of information operations – deceptive, manipulative – while avoiding any regulation of the content of the information itself, the proposed future legal framework puts careful emphasis on the safeguarding of freedom of speech and related rights. However, it bears noting that linking the question of lawfulness to transparency is not without pitfalls for civil rights either: compelling involved actors, such as social media platforms, to expose the source of a piece of information or the identity of the speaker is potentially in conflict with the right to privacy and therefore also freedom of speech. As noted by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, the right to communicate anonymously is a necessary precondition for the ability to freely express one's opinion online.[232] As a consequence, efforts to establish the source of an information operation should be limited and not disclose the identity of individuals unless absolutely necessary.

Finally, the historical survey shows the complicity of Western liberal democracies when it comes to subversive meddling in the sovereign political affairs of other states. This practice has seen a sharp decline since the end of the Cold War, and one may argue that recent influence operations by Western states have consistently promoted democratic values,[233] thus constituting attempts at assisting target populations in authoritarian states to realise their right to self-determination rather than undermine it. In a way, the tables have turned: because of the internet, and social media in particular, the open societies of Western-style liberal democracies now seem to be the most vulnerable, whereas states with tightly controlled online environments have an easier time in preventing foreign interference. Still, considering the history of information operations, if Western liberal-democratic states intend to address the problem within a legal framework

[230] UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda', 3 March 2017.
[231] ibid.
[232] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (22 May 2015), UN Doc A/HRC/29/32, 7.
[233] Shane (n 23).

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

they must be prepared to persuasively counter inevitable allegations of hypocrisy; it is certainly not sufficient to argue that past transgressions should be deemed irrelevant for the contemporary context.[234] Instead, there should be a clearly voiced and unambiguous commitment to abstain from engaging in interference in the internal affairs of other states by way of deceptive or otherwise manipulative information operations in the future.[235] Without such commitment, any endeavour to identify or create international rules against adversarial information operations will be doomed from the start.[236] Of course, this is a question of the political will of the West, and it is not at all clear that this understanding is yet shared by every relevant Western actor.[237]

5. CONCLUDING REMARKS

International law can only be one piece of the puzzle when it comes to addressing the rising threat of information operations and disinformation in the public-democratic discourse more generally; and it is an inherently limited one at that. Despite this caveat, the article has made an attempt to outline the contours of a possible way forward for developing an international legal framework for the problem. As the works of an increasing number of scholars argue persuasively, the existing rules of customary international law – the prohibition of intervention, the principle of sovereignty, and the principle of self-determination – are capable of an interpretation that makes them suitable candidates. This could be accomplished either by an expanded understanding of the requirement of 'coercion' that includes manipulative conduct, or by recognising respect for sovereignty as a standalone rule of customary international law and the acknowledgment that it protects internal democratic decision-making processes by way of the principle of self-determination of a state's constituent people.

To date, however, such an interpretation of existing rules is not sufficiently reflected in current state practice and expressions of *opinio juris*. In the absence of necessary uniformity the present state of customary international law is indeterminate. The reasons are multifaceted. On the one hand, both liberal-democratic and authoritarian powers have a long history of interfering with internal political processes in other states, and this practice has been continuing to the present. On the other hand, in particular, Western states are concerned that increased protection for the sovereignty of states could come at the cost of the universal application of civil rights such as freedom of speech and freedom of information. These concerns must be taken seriously. Still, the survey of recent state practice reveals that the paradigm shift of the digital transformation, with its emergence of a revolutionised global media ecosystem, have prompted more and more states to reconsider their legal attitudes towards information operations.

[234] In this sense, however, Ohlin (n 93) 24.
[235] See likewise Nye (n 24).
[236] Goldsmith (n 150).
[237] ibid.

https://doi.org/10.1017/S0021223720000060 Published online by Cambridge University Press

Assuming the political will to protect their constituent people from illegitimate outside interference, it is up to the states to move ahead. As a prudent way forward the article proposes a focus on deceptive and manipulative modes of conduct without advocating the regulation of the content of information itself. Such an approach tackles the growing problem of information operations that threaten to undermine the legitimacy of liberal-democratic systems while taking seriously potential pitfalls for civil rights posed by overly broad approaches.