Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber Operations Targeting Democracy

Presented at Conference on 'New Technologies: New Challenges for Democracy and International Law', University of Cambridge, March 2019.

Steven Wheatley[*]

Introduction

International lawyers have long accepted the need to respond to the challenges created by the Internet and other information and communications technologies. The primary focus, thus far, has been on the rules that apply to cyber warfare, specifically whether the laws of war can be stretched to the cyber domain. Increasingly, though, it is recognized that there is a need to be clear about the rules that apply to cyber operations falling below the use of force threshold, especially as few, if any, cyber operations have crossed that line, whilst malicious cyber operations below the use of force borderline are commonplace.

This paper examines the legality of foreign state cyber operations targeting the practices of democracy, specifically attempts to 'hack' elections and change the result of the vote, and efforts to influence political campaigns through new social media (Facebook, Twitter, etc.), including by the promulgation of 'fake news'. The subject has become an issue of controversy following complaints that the Russian Federation interfered in the 2016 US presidential election, and there have also been allegations that Russia attempted to affect the 2017 French presidential election, the 2017 German general election, and as well as the 2016 UK Brexit referendum, and 2017 Catalan independence vote.

Security analysists explain the alleged Russian behaviour in terms of a wider practice of hybrid warfare, sometimes referred to as information or political warfare, with the approach outlined by Valery Gerasimov, chief of the general staff of the Russian military, in his now famous 2013 article, in which he concluded that the 'rules of war have changed… in the direction of the broad use of political, economic, informational, humanitarian and other non-military measures'.[1] Hybrid warfare relies, inter alia, on the launching of cyber operations with the objective of changing the regime in the target state, or changing the way the Russian Federation is perceived in the target state, or undermining the population's trust in the legitimacy of the target state's democratic system.[2] Thus, the US Office of the Director of National Intelligence concluded that Russian cyber and propaganda operations during the 2016 US Presidential election were motivated by a desire to support the candidacy of Donald Trump over Hilary Clinton and to undermine the faith of the American public in the democratic process.[3]

This work examines the issue from the perspective of the non-intervention principle. There are three reasons for this. First, the non-intervention principle is well established in international law, providing an irrefutable limit on the exercise of state power outside national borders. Second, there is no *lex specialis* applicable to state cyber operations, no agreed international

[*] Professor of International Law (University of Lancaster). s.wheatley@lancaster.ac.uk

[1] Valery Gerasimov, 'The Value of Science in Prediction', *Military-Industrial Courier* (2013).

[2] Keir Giles, *Handbook of Russian Information Warfare* (Rome: Defense College, 2016), pp. 18 – 24.

[3] Office of the Director of National Intelligence, 'Assessing Russian Activities and Intentions in Recent US Elections', 6 January 2017.

law of cyberspace, or Convention on the Law of Cyberspace. The rules that apply to cyber operations are the same ones that apply the other forms of interferences in the affairs of other states. Finally, those states that feel they have been subject to foreign state cyber operations targeting their democratic practices have framed the issue in these terms. In 2016, for example, the US State Department Legal Adviser, Brian Egan, argued that 'a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention.'[4] In 2018, the UK's Attorney General Jeremy Wright made the same point: the use of cyber power 'to alter the results of an election in another state [...] must surely be a breach of the prohibition on intervention in the domestic affairs of states.'[5]

To show that a cyber operation targeting one of the core practices of democracy is a violation of the non-intervention principle, we must be able to show that it is 'coercive' in nature, following the conclusion of the International Court of Justice in the 1986 *Nicaragua* (Merits) case that intervention is only wrongful 'when it uses methods of coercion'. Hitherto, the literature on non-intervention has not examined in any detail the meaning of the term 'coercion', with the consequence that conduct is presumed to violate the non-intervention principle without it being explained in what way the impugned activity is 'coercive'. We see the problem in attempts to evaluate the legality of the so-called 'DNC hack' that occurred during the 2016 US presidential election, widely blamed on Russia, which resulted in private emails belonging to members of the Democratic National Committee (DNC), the governing body of the Democratic Party, being released on WikiLeaks, confirming that the DNC favoured Hillary Clinton over Bernie Sanders, thereby damaging Clinton's electoral prospects. Jens Ohlin makes the point that whilst this cyber operation 'was certainly corrosive [to the proper functioning of American democracy], it is genuinely unclear whether it should count as coercive', leaving 'an overall impression of illegal conduct, but without a clear and unambiguous doctrinal route towards that conclusion.'[6]

This paper proceeds as follows. It first outlines the non-intervention principle, before considering the putative problem of 'cyber coercion'. Examining the meaning of 'coercion' in the customary non-intervention principle, the work explains that state activity is 'coercive' where the objective is to create a situation in which the target has no choice but to act as the outside power wishes (whether successful, or not), including through the use of cyber threats, the deployment of cyber power, or employment of cyber propaganda to undermine the system of political decision-making in the target state. The paper concludes by detailing the protection afforded to democratic states from state cyber operations targeting the core practices of democracy by the non-intervention principle.

The Non-Intervention Principle

The non-intervention principle first finds expression in Emer de Vattel's, *Law of Nations* [1758], in which he concludes that 'no foreign power has a right to interfere in' 'affairs being

[4] Brian J. Egan, 'International Law and Stability in Cyberspace' (2017) 35 *Berkeley Journal of International Law* 169, 175.
[5] Attorney General Jeremy Wright QC MP, 'Cyber and International Law in the 21st Century'.
[6] Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?' (2017) 95 *Texas Law Review* 1579, 1593 – 1594.

solely a national concern'.[7] The principle is explained as a logical and necessary consequence of the nature of sovereignty and the right of a political community to regulate its own affairs. Where disputes arise, Vattel is clear that 'it belongs *to the nation alone* to judge and determine them conformably to its political constitution.'[8] Vattel's non-intervention principle is expressed succinctly: '[N]o state has the smallest right to interfere in the government of another.'[9]

When the subject came before the International Court of Justice in the 1986 *Nicaragua* (Merits) case, the Court confirmed that the non-intervention principle, i.e. 'the right of every sovereign State to conduct its affairs without outside interference', is 'part and parcel of customary international law.'[10] In reaching this conclusion, the Court noted the divergence in state practice on the ground, and instead focused on the 1965 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, and 1970 Declaration on Principles of International Law Concerning Friendly Relations, along with the 1975 Helsinki Final Act. The International Court of Justice determined that the non-intervention principle

> forbids all States… to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. … Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion… defines, and indeed forms the very essence of, prohibited intervention.[11]

There are four elements to the non-intervention principle outlined by the International Court of Justice. First, this is an inter-state doctrine, which concerns the deliberate actions of one state targeting another state. Second, the interference in the internal or external affairs of the target state must concern an issue that a state should be permitted to decide freely. One of these is, the Court confirmed, is the choice of the political system, and the ICJ refused to 'contemplate the creation of a new rule opening up a right of intervention by one State against another on the ground that the latter has opted for some particular ideology or political system.'[12] Third, intervention is wrongful 'when it uses methods of *coercion* in regard to such choices, which must remain free ones.' Finally, a coercive operation that interferes in the affairs of another state is a violation of customary international law where it cannot be justified as a lawful countermeasure.

The Putative Problem of 'Cyber Coercion'

A state cyber operation with the objective of 'hacking' an election, so that the outside power's preferred candidate was declared the winner, would be an interference in the internal political affairs of the target state, and it is difficult to see how such an action could be justified. The question then turns to whether the activity can be characterized as 'coercive', as required by

[7] Emer de Vattel, *The Law of Nations, Or, Principles of the Law of Nature, Applied to the Conduct and Affairs of Nations and Sovereigns* [1797] (Indianapolis: Liberty Fund, 2008), Book I, Ch III, para. 37.
[8] Ibid., Book I, Ch III, para. 36 (emphasis added).
[9] Ibid., Book II, Ch IV, para. 54.
[10] *Military and Paramilitary Activities in and against Nicaragua*, (Nicaragua v. United States of America), Merits, Judgment [1986] ICJ Rep 14, para. 202. The International Court of Justice noted that the non-intervention principle 'has moreover been presented as a corollary of the principle of the sovereign equality of States': Id.
[11] Ibid., para. 205.
[12] Ibid., para. 263

the ICJ in the 1986 *Nicaragua* case. Where international lawyers have defined the term, and most writings on non-intervention do not, they have explained 'coercion' in terms of an unwilling *conscious* act. Thus, Christopher Joyner, in his entry on the subject in the *Max Planck Encyclopedia of Public International*, defines coercion as 'the government of one State *compelling the government of another State to think or act* in a certain way by applying various kinds of pressure, threats, intimidation or the use of force'.[13] The problem is that cyber operations, specifically clandestine cyber operations, i.e. those not known to the target state, are not 'coercive' in the sense of changing the *conscious* behaviour of the target state. Thus, a remote cyber operation by State P that hacks the computer of the Election Commission in State Q, so that P's preferred candidate is (wrongly) declared the winner (where Q is unaware of the operation), is not coercive on the standard understanding, because there is no attempt to change the conscious behaviour of the Election Commission.

The problem created for the regulation of cyber operations by the element of coercion has led some writers to argue for a reformulation of the non-intervention principle to include the notion of 'cybered coercion', or for doing away with the coercion requirement altogether in the cyber context, or for the formulation of new international law rules. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, drafted by an international group of experts argues, for example, for the recognition of a new rule prohibiting the 'interference with or usurpation of inherently governmental functions',[14] including 'changing or deleting data such that it interferes with… the conduct of elections'.[15] The commentary explains that the rule differs from the non-intervention principle because 'intervention requires an element of coercion.'[16] There are, though, two problems. First, there is limited evidence that a rule prohibiting the interference with, or usurpation of, inherently governmental functions exists as a matter of positive international law (the rule is deduced from sovereignty as a rule of international law); second, as we will see, a proper understanding of the word 'coercion' can capture certain clandestine cyber operations, including the hacking of election computers to change the result of a vote, and sustained cyber propaganda campaigns.

The Meaning of 'Coercion' in the Non-Intervention Principle

Whilst international lawyers are generally agreed on the methodology for the interpretation of written texts – looking to the approach outlined in the Vienna Convention on the Law of Treaties, the rules for the interpretation of customary norms have not been subject to considered and sustained doctrinal examination. The key difference, of course, is that, in the case of custom, there is no text, we are concerned with the interpretation of, what Philip Allott calls, 'unwritten law'.[17] There is, then, a requirement to translate custom into a form that allows for syllogistic and juridical reasoning, whereby the law-applier deduces the legality or validity of an act from the application of law to facts. We see this in the work of the International Court of Justice, where unwritten customary international law norms are translated into written form in order to reach a judgment on the rights and responsibilities of the parties in contentious

[13] Christopher C Joyner, 'Coercion' (2006) *Max Planck Encyclopedia of Public International Law*, para. 1 (emphasis added).
[14] Michael N. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 2nd ed., Cambridge: Cambridge University Press, 2017), Rule 4, Explanatory para. 10.
[15] Ibid., para. 16.
[16] Ibid., para. 22.
[17] Philip Allott, 'Interpretation: An Exact Art', in Andrea Bianchi, et al (eds), *Interpretation in International Law* (Oxford: Oxford University Press, 2015) 373, 384 – 385.

cases. But the application of law to facts rarely allows for only one conclusion, and there is a need for the interpretation of law norms as one part of the process of juridical reasoning, that is of assigning meaning to legal norms, including customary international law norms. The question is how?

There are essentially three possible approaches to the interpretation of law norms: (1) those that look to explain the ordinary or plain meaning of the words used; (2) systemic methods that try and make sense of the rule in its legal context; and (3) teleological arguments that look to explain the provision in light of its aim or objective. Famously, Article 31(1) of the Vienna Convention on the Law of Treaties adopted a 'general rule' on interpretation that included all three approaches in the case of written international law. Albert Bleckmann concludes that the same general approach should be applied to the case of customary international law, with the meaning of customary norms emerging from what he calls (in translation) grammatical, systematic, and teleological methods of interpretation.[18] The International Court of Justice has followed this approach, deploying methods of linguistic or grammatical interpretation, ensuring that an interpretation takes into account existing international law rules, and relying on the object and purpose of the rule to establish its content.

To explain the meaning of the word 'coercion' in the non-intervention principle, then, we have to look, in the round, at (1) the ordinary way the term is used, especially its use in domestic law systems; (2) the way the term has been used in other areas of international law, to ensure consistency of usage; and (3) the object and purpose of the non-intervention principle.

The 'Ordinary' Meaning(s) of Coercion

The *Oxford English Dictionary* defines 'coercion' as the action of coercing, with 'coercing' defined as 'the application of force to control the action of a voluntary agent.' This can be done in one of three ways: coercion of the will, coercion of the body, and coercion of the mind.

Coercion of the Will

The meaning and proper understanding of the word 'coercion' has been subject to sustained analysis by legal and political philosophers. The best known and most influential account is the 1969 essay by Robert Nozick in which he concludes that coercion involves a threat by one actor (P) to another actor (Q) that if Q does not do (or does) a certain action (X), then deleterious consequences will follow for Q.[19] The standard example is the threat by the gunman, 'Your money, or your life'.

Coercive threats result in a change (or maintenance) in the behaviour of others, that is P forces Q to 'Do X' through the threat of deleterious consequences if Q does not 'Do X'. Q is a moral agent presented with an unpalatable choice, which is not, in any rational sense, a choice, although there remains, in the literal sense, a choice for Q, 'Your money, *or* your life?' A focus on coercive threats presupposes that the target acts consciously, albeit unwillingly; a situation which is distinguished from the use of force against the target. Peter Westen notes, for example, that we do not normally use the term coercion when we are acted upon. Thus, if P pushes Q

[18] Albert Bleckmann, 'Zur Feststellung and Auslegung von Völkergewohnheitsrecht' (1977) 37 *ZaöeRV* 504, 526 – 528.
[19] Robert Nozick, 'Coercion', in Sidney Morgenbesser et al. (eds), *Philosophy, Science, and Method: Essays in honor of Ernest Nagel* (New York: St. Martin's Press, 1969) 440, 441 – 445.

into the swimming pool, we say that Q has been *forced* into the water, not that he has been coerced. To say a person has been coerced, 'presupposes an act of will on his part.'[20]

Coercion of the will involves, what the legal philosopher Grant Lamond calls, a forced choice, 'forced both because the choice situation is imposed by another, and because the situation is designed so that only one option will be regarded as acceptable.'[21] We can, then, be made to do something through the creation of a choice situation in which only one course of action is a viable option.

Coercion of the Body

We can also be made to do something through the application of physical force. So instead of saying 'Your money, or your life!', the gunman can simply march you to the cashpoint, force your finger on your iPhone, and compel you to withdraw money from your account, without the need for you to make any conscious decision. In the case of physical compulsion, it is our bodies, rather than our minds, that are controlled by the other person, and, in contrast to moral coercion, where we rationally choose not to resist, 'physical compulsion is [literally] irresistible'.[22] It is the very success of physical coercion that makes it coercive.

Force is coercive where P compels Q to 'Do X' in order to achieve some objective of P's, and Q, in fact, 'Does X'. Force is only coercive when P uses force to get Q *to do something*. Force cannot be characterised as coercive when P simply *does something to* Q. Thus, when P pushes Q into the swimming pool, P *forces* Q into the water; but when P grabs Q's hand and makes her sign a document (where Q is physically incapable of resisting), then P *coerces* Q. That it, P achieves a certain objective by working *through* Q, treating Q, in the words of A. E. Farnsworth, as a 'mere mechanical instrument'.[23]

Coercion of the Mind

In an early draft of what become Article 51 of the Vienna Convention on the Law of Treaties (Coercion of a Representative of a State), the International Law Commission's Special Rapporteur, Gerald Fitzmaurice explained that 'duress or coercion, whether physical or mental' could include 'certain modern methods of compulsion summed up by the term "brainwashing"'.[24] He was writing immediately after the term was coined by Edward Hunter to explain the fact that American troops captured in the Korean War (1950-53) had returned from prisoner-of-war camps as apparently committed communists.

Evan Stark explains that 'brainwashing', a form of psychological coercion, was understood to work through a process of breaking down the target's sense of 'self' and their understanding of the world, and its replacement with 'the controller's altered picture of reality'. This was typically achieved through random acts of reward and punishment.[25] Stark has successfully

[20] Peter Westen, ''Freedom' and 'Coercion': Virtue Words and Vice Words' (1985) *Duke Law Journal* 541, 565.
[21] Grant Lamond, 'Coercion and the Nature of Law' (2001) 7 *Legal Theory* 35, 40.
[22] Grant Lamond, 'The Coerciveness of Law' (2000) 20 *Oxford Journal of Legal Studies* 39, 44.
[23] A. E. Farnsworth, *Contracts* (Boston: Aspen, 1982), p. 257.
[24] Third Report on the Law of Treaties by Mr. G.G. Fitzmaurice, Special Rapporteur, Yearbook of the International Law Commission: 1958, vol. II, p. 38, para. 58.
[25] Evan Stark, *Coercive Control: How Men Entrap Women in Personal Life* (New York: Oxford University Press, 2007) 359, reference to Edgar H. Schein, *Coercive Persuasion: A Socio-psychological Analysis of the 'brainwashing' of American Civilian Prisoners by the Chinese Communists* (W.W. Norton, 1995).

argued that we can expand the notion of psychological coercion to include situation of 'coercive control' in domestic violence situations, and that in all cases, 'The victim's agency is [the] principal target' of the coercer.[26]

Coercive control in intimate partner relationships has now been criminalized in a number of jurisdictions.[27] In England and Wales, for example, Section 76(1) of the Serious Crime Act 2015 establishes that, a person commits an offence if he repeatedly engages that is controlling or coercive, and the behaviour has a serious effect on the victim. The Government department responsible for the legislation has explained that 'Controlling or coercive behaviour does not relate to a single incident, it is a purposeful pattern of behaviour which takes place over time in order for one individual to exert power, control or coercion over another.'[28]

One form of psychological coercion to have entered the public imagination is that of 'gaslighting', a term included in the Oxford English Dictionary in 2004, meaning: 'The action or process of manipulating a person by psychological means into questioning his or her own sanity'. The expression, 'gaslighting', was taken from Patrick Hamilton's 1938 play, *Gas Light*, later made into a film starring Ingrid Bergman, which tells the story of a man intent on convincing his wife she is insane, so he can steal her jewels. Kate Abramson makes the point that gaslighting, both in the film and in daily life, is a form of psychological manipulation in which the gaslighter attempts 'to induce in someone the sense that her reactions, perceptions, memories and/or beliefs are not just mistaken, but utterly without grounds – paradigmatically, so unfounded as to qualify as crazy.[29] The objective of the gaslighter is to gain control over the target, by removing the possibility of disagreement with an actor capable of moral agency, i.e. of deciding for herself, for her own reasons, so that when P suggests that Q 'Does X', Q is certain to 'Do X'.[30]

Psychological coercion, or coercion of the mind, describes a situation where there is a pattern of behaviour by P, with the objective that Q will behave in a certain way. P's actions towards Q results in the destruction of Q's capacity to make decisions for herself, and the information provided by P makes it inevitable that Q will act as directed by P. Q can appear to act on her own volition, but she is, in reality, destitute of freedom, because her capacity for meaningful agency has been destroyed by P.

The Meaning of 'Coercion' in International Law

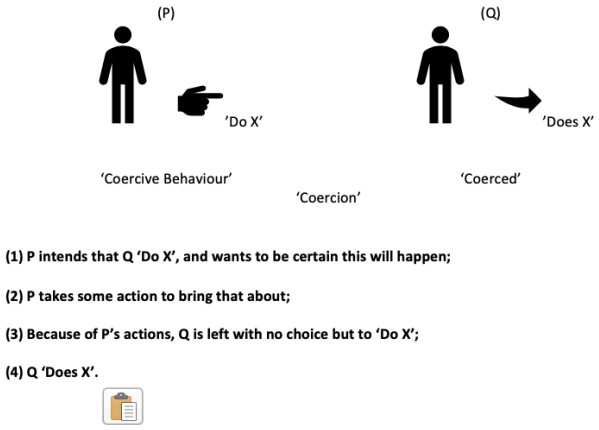
In the ordinary meaning of the word, we can think of 'coercion' as involving two actors 'P' and 'Q', with a timeline of events. (1) P desires that Q 'Do X', but is concerned that Q will not, or might not, 'Do X'; (2) P acts with the objective of ensuring that Q 'Does X'; (3) P's actions results in a denial of meaningful agency for Q, so that it is inevitably that Q will 'Do X'; (4) Q 'Does X'. The standard example is when the Gunman ('P') says to his Victim ('Q'), "Your money, or your life!" ('Do X, or else!'). In this scenario, both P and Q are moral agents, i.e. actors with the capacity and will to decide things for themselves, for whatever reasons of their own. P intends that Q 'Do X' (here, give him the money), and he wants to be certain that this will happen. Rather than try to persuade Q, by providing a reasoned argument based on the

[26] Stark, ibid., 370.
[27] See also Section 39(1) Ireland Domestic Violence Act 2018; and Domestic Abuse (Scotland) Act 2018.
[28] Home Office, 'Controlling or Coercive Behaviour in an Intimate or Family Relationship: Statutory Guidance Framework', December 2015, para. 10.
[29] Kate Abramson, 'Turning Up The Lights On Gaslighting' (2014) 28 *Ethics* 1, 2.
[30] Ibid., 14-15 (emphasis in original).

facts, or offering incentives or disincentives, or by manipulating Q by providing false information, P acts to create a situation where it is inevitable that Q will 'Do X'. Because of P's actions, Q has no choice but to 'Do X' and Q's moral agency, her right to decide for herself whether to give P the money, or not, has been negated.

Where P does in fact 'Do X', we have all the elements of 'coercion'. Where the efforts of the Gunman are not successful, we can still speak of 'coercive behaviour'. To establish coercive behaviour we focus on the intentions and actions of P. Where a reasonably observer would conclude that the most likely explanation for P's behaviour is that P *intends* to create a situation where Q must 'Do X', then we can describe that behaviour as 'coercive'. Thus, when the Gunman says to his Victim, "Your money, or your life!", that is coercive behaviour, whether or not the threat is effective.

The structure of the ordinary meaning of the term 'coercion' can be represented as follows:



The same basic structure of coercion can be seen in its usage in international law. Article 51 of the Vienna Convention on the Law of Treaties establishes, for example, that 'The expression of a State's consent to be bound by a treaty which has been procured by the coercion of its representative through acts or threats directed against him shall be without any legal effect.' The notion of 'acts or threats directed against him personally', is taken to include 'not only a threat to his person, but a threat to ruin his career by exposing a private indiscretion, as also a threat to injure a member of the representative's family with a view to coercing the representative.'[31] Oliver Dörr and Kirsten Schmalenbach explain that coercion, in this context, includes acts or threats that 'induce such fear [that the representative] feels compelled to express the represented State's consent [when] she would not have done without such compulsion'[32] ("Your consent to the treaty, or…").[33]

The notion of coercion is also found in Article 18 of the International Law Commission's draft Articles on State Responsibility.[34] Thus, where State P 'coerces' State Q into breaking its international law obligations owed to State Z, P will be responsible for Q's actions. Coercion

[31] Yearbook of the International Law Commission (1966), vol. II, p. 246[2].
[32] Oliver Dörr and Kirsten Schmalenbach, *Vienna Convention on the Law of Treaties: A Commentary* (Berlin: Springer, 2012), p. 862.
[33] Article 52 concerns the coercion of a state by the threat or use of force: 'A treaty is void if its conclusion has been procured by the threat or use of force in violation of the principles of international law embodied in the Charter of the United Nations.'
[34] 'A State which coerces another State to commit an act is internationally responsible for that act'.

involves an action, in the words of the International Law Commission, 'deliberately exercised in order to procure the breach of one State's obligation to a third State.' The commentaries explain the point in the following way: 'Nothing less than conduct which forces the will of the coerced State will suffice, giving it no effective choice but to comply with the wishes of the coercing State.'[35] The coercing state 'is the prime mover in respect of the conduct and *the coerced state is merely its instrument*.'[36]

'Coercion' in the Non-Intervention Principle

In a lecture delivered at All Souls College, Oxford, in December 1860, Mountague Bernard, the inaugural Chichele Professor of International Law, explained that the existence of the non-intervention principle reflected the fact that international law was founded on two cardinal principles: that 'States are severally sovereign or independent', and, at the same time, they are also 'members of a community united by a social tie.'[37] Here, Bernard captures the essential function of the non-intervention principle, which is to delimit the boundary between unfriendly interferences in the affairs of sovereign and independent states, and unlawful interventions.

In the 1986 *Nicaragua* (Merits) case, the International Court of Justice explained that 'The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference'.[38] A prohibited intervention 'must accordingly be one bearing on matters in which each State is permitted, by the principle of state sovereignty, to decide freely.'[39] Specifically, the Court concluded that adherence by a state 'to any particular doctrine does not constitute a violation of customary international law; to hold otherwise would make nonsense of the fundamental principle of State sovereignty on which the whole of international law rests, and the freedom of choice of the political… system of a State.'[40]

The right to freedom of political self-determination is not, though, exercised in a vacuum. In an inter-connected and inter-dependent world society, there is a requirement for co-operation and co-ordination between formally sovereign and independent states, a need reflected in the very existence of international law. Given that the actions of any one nation can affect any other, states will inevitably take an interest in the political situation in other countries, and may wish to influence the processes of political decision-making. The function of the non-intervention principle is to delimit unfriendly interferences from unlawful interventions, and it does this with the inclusion of the criterion of 'coercion'. States can offer advice or inducements to the populations or governments of other states, or try and *influence* the decision-making processes in some other way, but they cannot act with the objective of bringing about a certain outcome because this would amount to a denial of the right of the target state to freedom of political self-determination. Such actions would be 'coercive' in their very nature as we can see from a comparison between the ordinary meaning of 'coercion' and its function in the non-intervention principle, as explained by the International Court of Justice in the 1986 *Nicaragua* (Merits) case:

[35] International Law Commission, Draft Articles on the Responsibility of States for Internationally Wrongful Acts with Commentaries, p. 69.
[36] Ibid., p. 65 (emphasis added).
[37] Mountague Bernard, *On the Principle of Non-intervention* (Oxford: J. H. & J. Parker, 1860), p. 7
[38] *Military and Paramilitary Activities in and against Nicaragua*, (Nicaragua v. United States of America), Merits, Judgment [1986] ICJ Rep 14, para. 202.
[39] Ibid., para. 205.
[40] Ibid., para. 263.

The Ordinary Meaning of Coercion	**Coercion in *Nicaragua* (Merits)**
(1) P intends that Q 'Do X' Coercion not concerned with P doing something to Q	**(1) P intends that Q 'Do X'** Nicaragua complained that the US two objectives: (a) The overthrow of the government of Nicaragua; and (b) 'to coerce the government of Nicaragua into the acceptance of United States policies' (para. 239)
(2) P takes some action to bring that about (coercion will, body, mind) The statement 'P coerced Q into killing X' can be understood in one of the following ways… ***(a) Coercive of the Will*** P threatened Q ('Kill X, or else') ***(b) Coercion of the Body*** P pointed a gun at X, put Q's finger on the trigger, and applied pressure to Q's finger so that the gun fired, killing X ***(c) Coercion of the Mind*** P 'brainwashed' Q to kill X, which is the plot of *The Manchurian Candidate* (1962).	**(2) P takes some action to bring that about (coercion will, body, mind)** State P coerces State Q by… ***(a) Coercion of the will (moral coercion).*** 'the United States intended, by its support of the contras, to coerce the Government of Nicaragua in respect of matters in which each State is permitted…to decide freely' (para. 241) ***(b) Coercion of the body (physical coercion).*** 'The element of coercion… is particularly obvious in the case of an intervention which uses force' (para. 205). ***(c) Coercion of the mind (propaganda).*** {See below}
(3) Because of P's actions There is a denial of Q's capacity for moral agency, i.e., Q is not a willing participant in the act of killing X.	**(3) Because of P's actions** In all cases, there is a denial of State Q's capacity for political self-determination.
(4) Q 'Does X'	**(4) Q 'Does X'**

In both cases, where Q 'Does X', we have all the elements of coercion. The amount of pressure exerted by P is irrelevant. It is then a mistake to see the different between military force and coercion in the non-intervention principle as a matter of degree. The notion of coercion has a specific meaning in both the ordinary meaning of the word, and in international law. Coercion describes a situation where one moral agent intends that another moral agent act in a certain pre-determined way, and acts to bring this about by removing the target's capacity to decide on the matter for themselves. But there is a difference between behaving *coercively* and the fact of *coercion*, in that coercive behaviour need not always result in the outcome desired by the coercing actor. Thus, where P intends that Q 'Do X' and takes some action to bring that about, we can describe that behaviour as 'coercive', whether or not it actually coerces the target.

The point is significant, because in the 1986 *Nicaragua* (Merits) case, the International Court of Justice confirmed that there is a violation of the non-intervention principle where we see coercive behaviour: where 'one State, *with a view to the coercion of another state*, supports and assists armed bands in that State whose purpose is to overthrow the government of that State, that amounts to an intervention'.[41] There was no consideration in the judgment as to whether the US had been successful in overthrowing the government of Nicaragua. By supporting the contra forces, the US was 'in breach of its obligation under customary

[41] Ibid., para. 241 (emphasis added).

international law not to intervene in the affairs of another State'.[42] The same point can be made about US efforts to force the Nicaraguan government to change its policy positions. Again, there was no consideration as to whether the US had been successful, with the ICJ concluding: 'Intervention is wrongful *when it uses methods of coercion* in regard to such choices, which must remain free ones.'[43]

The non-intervention principle prohibits, then, (1) the deliberate and targeted actions of one state ('P') (2) aimed at interfering in the domestic political affairs of another state ('Q'), where (3) the behaviour of P is 'coercive' in nature, and (4) the action cannot be justified as a lawful countermeasure, or on some other recognized ground under international law. Where State P's actions are successful, and Q 'Does X', then Q has been coerced, and we have a factual situation of coercion. But if P is unsuccessful, if P's action do not result in Q 'Doing X', then P's behaviour is still coercive in nature. In other words, we look to P's intention and actions to determine whether P's behaviour is 'coercive'. The relevant question is: "Has State P acted with the objective of putting State Q in a situation where they have no choice but to 'Do X'?" Where this is the case, the behaviour is 'coercive', and, unless it can be justified, it will be an internationally wrongful act.

Having established the meaning of 'coercion' and 'coercive' behaviour in the non-intervention principle, we can now turn to the legality of cyber operations targeting the core practices of democracy: (1) cyber operations hacking the election, in order to change the outcome of the vote; and (2) information operations undermining the capacity of the democratic polity to effective political self-determination.

The Cyber Hacking of Elections

Scott Shackelford and his colleagues identify a number of aspects of the electoral process that are potentially vulnerable to being hacked by way of modification of the software used in Election computers: (a) the electoral rolls used to verify voters' eligibility might be hacked and names deleted, denying citizens the right to vote; (b) the electronic voting machines (where e-voting is used) could be hacked to change the preferences of voters, or make votes 'disappear'; and (c) the tabulation systems used to aggregate the results of an election to determine the winners might be hacked, and the outcome of the vote changed.[44]

According to reports, democratic states are right to be concerned about the possibility of an election being hacked. In 1994, a hacker managed to add votes to the tallies of three right-wing parties in South Africa's first democratic election, cutting into the lead of Nelson Mandela's African National Congress party. The hack was discovered, but there was a delay as the counting method was switched from electronic to manual. In 2014, Ukraine's presidential vote was targeted by cyber-attackers, who accessed the computer of the Central Election Commission and changed the result to show the winner was a far-right candidate. The Election Commission noticed the hack and managed to avoid naming the wrong winner, although Russian state-controlled media did broadcast the false result. In 2016, the website of Ghana's Central Election Commission was hacked and false results announced from the Commission's

[42] Ibid., para. 292 (3).
[43] Ibid., para. 205 (emphasis added).
[44] Scott Shackelford et al., 'Making Democracy Harder to Hack' (2017) 50 *University of Michigan Journal of Law Reform* 629, 636 – 638.

Twitter account while votes were still being counted. During the 2016 United States presidential election, there were attempts to hack voter rolls and change voter records.

A cyber operation attributable to State P hacking the computer of the Election Commissioner in State Q, so that State P's preferred candidate was (wrongly) declared the winner, would be an example of *coercive* cyber power. P's objective is for Q to 'declare P's preferred candidate the winner'. Rather than offer inducements or warnings, a more or less generous aid package, for example, where there is no guarantee the population will vote for P's preferred candidate, P uses its cyber power to ensure the Election Commission in Q 'declare its preferred candidate the winner', in circumstances in which State Q is unaware of the usurpation of its government functions.

Cyber power is coercive where State P compels State Q to 'Do X', and Q 'Does X'. It is the very success of the deployment of cyber power that makes it *coercive*. The scale of the cyber operation is irrelevant. It follows that any cyber operation, including the insertion of a few bits of data into a software programme, which achieves P's objective of having its preferred candidate declared the winner, would, by definition, be coercive. The cyber operation contains all the elements of coercion: (1) P's objective is for Q to 'do X' ('declare its preferred candidate the winner); (2) P achieves this objective by working through the government institutions in Q (the Electoral Commission); and (3) there is no possibility of Q resisting (because Q is unaware of the hack), meaning there is a denial of meaningful freedom of action.

Likewise, a failed cyber operation with the objective of changing the results of an election would be a violation of the non-intervention principle – where, for example, the cyber defences of the target state are sufficiently robust to repel the attack. The International Court of Justice was clear in the 1986 *Nicaragua* case that there is a violation of the non-intervention principle where a state seeks to interfere in the domestic political affairs of another state, and its actions can be described as 'coercive'. Behaviour is coercive where one state acts to get the target state to 'Do X', including through the deployment of physical force, and the target has no option but to 'Do X'. In the case of hacking an election, the objective is to change the vote so that P's preferred candidate is (wrongly) declared the winner. If the hack is successful this will happen: P's preferred candidate *will* be declared the winner and there will be nothing that Q can do about the situation. Consequently, an attempt to hack an election is, by definition, coercive, because the objective is to get Q's computer to 'Do X', leaving the Electoral Commission in Q with no choice but to comply.

Cyber Information Campaigns

We have seen that the notion of 'coercion' can be applied to the deployment of coercive threats in international relations and to the use of coercive force. These are direct forms of coercion, whereby State P looks to affect the constitutional system in State Q with the objective of changing (or maintaining) the government or changing (or maintaining) some aspect of government policy. Propaganda works differently, in that P aims to bring indirect pressure on Q by influencing or manipulating the population in Q in a certain predefined way, with the population then directly influencing the constitutional system of political decision-making.

In the 1986 *Nicaragua* (Merits) case, the Court confirmed that the non-intervention principle concerned 'the right of every sovereign State to conduct its affairs without outside

interference'.[45] But what amounts to an 'interference' in the political affairs of another state, and what constitutes an unlawful intervention? The following section explain the long-standing prohibition on subversive interventions before considering the problem of 'fake news', and going on to outline the general position on propaganda under the non-intervention principle.

Subversive Interventions

One of the notable points about alleged Russian cyber operations is that they are not considered to be aimed at supporting a particular ideology, in contrast, for example, to the situation in the Cold War (1947–91), when the Soviet Union would assist communist and other left-wing political parties, and the United States supported right wing parties. Russian interference today is seen as destructive by Western states, with, for example, the US Office of the Director of National Intelligence concluding that Russian cyber and propaganda operations during the 2016 presentation election were, in part, motivated by a desire to undermine the faith of the American public in the democratic process,[46] and the British Prime Minister, Theresa May complaining that Russia is 'seeking to weaponise information. Deploying its state-run media organisations to plant fake stories and photo-shopped images in an attempt to sow discord in the West and undermine our institutions.'[47]

Efforts to undermine the trust of the population in the government (elected or otherwise) with the objective of changing the system of government are characterized in international law as 'subversive interventions'. The illegality of subversive intervention is well established in international law doctrine and practice, with Emer de Vattel declaring in 1758 that 'It is a violation of the law of nations to invite those subjects to revolt who actually pay obedience to their sovereign, though they complain of his government'.[48] Two recent inclusions in the *Max Planck Encyclopedia of Public International Law* make the same point. Eric de Brabandere concludes that the prohibition on subversive propaganda is 'a deep-rooted principle of customary international law';[49] Philip Kunig concurs: Subversive interventions 'are prohibited, if they aim to foment revolt or civil strife in another State'.[50]

A subversive intervention is an interference in the domestic political affairs of the target state with the objective of introducing a new constitutional system of government, often more sympathetic to the intervening power. Quincy Wright concurs with the illegality of subversive interventions, including by way of propaganda 'with the intent or likelihood of inciting sedition or revolt against the governments of other states',[51] but concludes that mere criticism of the policy of a state is 'in a different category, and [is], of course, permissible.'[52] Others take a different view, with, for example, Maziar Jamnejad and Michael Wood concluding that

[45] *Military and Paramilitary Activities in and against Nicaragua*, (Nicaragua v. United States of America), Merits, Judgment [1986] ICJ Rep 14, para. 202.
[46] Office of the Director of National Intelligence, 'Assessing Russian Activities and Intentions in Recent US Elections', 6 January 2017, p. ii.
[47] PM speech to the Lord Mayor's Banquet, 13 November 2017. Available <https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017>, accessed 30 April 2018.
[48] Emer de Vattel, *The Law of Nations, Or, Principles of the Law of Nature, Applied to the Conduct and Affairs of Nations and Sovereigns* [1797] (Indianapolis: Liberty Fund, 2008), Book II, Ch IV, para. 56.
[49] Eric de Brabandere, 'Propaganda' (2012) *Max Planck Encyclopedia of Public International Law*, para. 11.
[50] Philip Kunig, 'Intervention, Prohibition of' (2008) *Max Planck Encyclopedia of Public International Law*, para. 24.
[51] Quincy Wright, 'Subversive Intervention' (1960) 54 *American Journal of International Law* 521, 523.
[52] Ibid., 532.

political interference covers any situation 'where one state becomes involved in the internal political processes of another', and is, in principle, prohibited under international law.[53]

What, then, would we make of US President Barack Obama's plea to the British public to vote against Brexit, and warning that the UK would be at the 'back of the queue' in any trade deal with the US, if the country chose to leave the European Union?[54] There is no doubt this was an *interference* in UK domestic politics. The *Oxford English Dictionary* explains the meaning of 'interference' in terms of the action of interfering or intermeddling, with intermeddling defined as 'to concern oneself with what is none of one's business'. Given that the object and purpose of the non-intervention principle is to protect the right of political self-determination, with the element of coercion having the function of delimiting unfriendly interferences from unlawful interventions, we can understand 'interference' in the normal sense of any action that looks to intermeddle in the internal political affairs of another state, including any comment aimed at the domestic population concerning a matter of political controversy. The key question remains whether an interference can be categorized as 'coercive', and therefore prohibited.

'Fake news'

The term 'fake news' came to prominence during the 2016 US presidential election, including the claim that Pope Francis had endorsed Donald Trump prior to the election, and it was named 'word' of the year in 2017. Fake news mimics traditional news media, but lacks its commitment to accuracy and credibility, and studies show that people often struggle to distinguish fact from fiction on the Internet and in social media.

There is widespread agreement that factual information produced by a state intended to inform the citizens of another state, including information about the actions of their own government, does not constitute a violation of the non-intervention principle. It follows, as Thomas and Thomas point out, that news broadcasts do not fall within the definition of propaganda, 'for news broadcasts are the transmission of facts.'[55]

'Fake news' does not, self-evidently, enjoy the exemption applied to factual information under the non-interference rule. To consider the position of 'fake news', consider the following (hypothetical) example:[56]

> The objective of State P is to see the removal of President Jones in forthcoming elections in State Q. President Jones is a social conservative and in order to reduce his support amongst the electorate, the intelligence agency in P creates, and then releases on the Internet, a video that appears to show, in convincing detail, President Jones engaged in unlawful sexual acts.

[53] Maziar Jamnejad and Michael Wood, 'The Principle of Non-intervention' (2009) 22 *Leiden Journal of International Law* 345, 368.
[54] Anushka Asthana and Rowena Mason, 'Barack Obama: Brexit would put UK 'back of the queue' for trade talks', *The Guardian* 22 April 2016.
[55] Ann Van Wynen Thomas and A. J. Thomas Jr., *Non-Intervention: The Law and Its Import in the Americas* (Dallas: Southern Methodist University Press, 1956), p. 290.
[56] Albeit not so far from reality, given creation and release of a 'Hillary Clinton hotel sex tape' by Russia's Internet Research Agency: Ben Collins, 'Russia-linked account pushed fake Hillary Clinton sex video', NBC News 11 April 2018 <https://www.nbcnews.com/tech/security/russia-linked-account-pushed-fake-hillary-clinton-sex-video-n864871> (Last visited 27 February 2019.)

The video is false, this is 'fake news'. The objective of P in our scenario is to affect the outcome of the election in Q. Rather than rely on reasoned argument, or offer incentives or disincentives to the population, so that the population in Q can make a decision based on the facts, and a correct understanding of the facts, P decides to try and manipulate the electorate by way of the publication of a falsehood, with the aim of persuading the population not to vote for President Jones.

The publication of the video is an example of propaganda, defined by Eric de Brabandere as a method of communication 'aimed at influencing and manipulating the behaviour of people in a certain predefined way. The element of influence and manipulation is at the centre of the concept, and distinguishes it from mere factual information.'[57] 'Manipulation' is defined by the *Oxford English Dictionary* as 'the exercise of subtle, underhand, or devious influence or control'. But there is a difference between manipulation and coercion. 'Manipulation, by definition, *influences* decision-making',[58] albeit it an immoral fashion, but it does not predetermine the outcome of the decision-making, as the target retains the ability to make her own decision, albeit on the basis of false information. Thus, where, through the production of 'fake news', a state looks to *influence* the population of the target state, this does not constitute coercive behaviour because the interfering state has not acted to create a situation where it is inevitable that the target population will 'Do X'. The production of fake news is not, then, intrinsically coercive, and does not, of itself, constitute a violation of the non-intervention principle.

Cyber Propaganda

In his major study on *The International Law of Propaganda*, first published in 1968, Bhagevatula Satyanarayana Murty explained that propaganda is coercive when it exerts 'high psychological pressure on the audience to adopt a particular attitude or behaviour'.[59] Whereas attempts at persuasion leave the individual with a number of alternatives, coercion subjects the target 'to a high degree of constraint in the choice of alternatives'.[60]

Before the Internet, it was almost impossible for an outside power to control the information environment in another state, and that remains the position today. In an open, democratic, society, citizens can gain knowledge from a variety of sources, including a plurality of voices from inside and outside the country. In a closed, authoritarian state, it is difficult to imagine an outside power supplanting the propaganda efforts of the domestic government. However, as more people get their news and commentaries on politics from sources such as Facebook and Twitter, it becomes more difficult for democratic governments to control the information available to citizens, and the possibility increases of a foreign power creating an information environment in which a single political narrative predominates, and citizens see themselves as having only one (rational) choice.

One of the complaints by the United States following the 2016 presidential election was that the Russian Federation's 'state-run propaganda machine' had conducted an 'influence campaign' which sought to sway the election, including by making favourable comments about

[57] Eric de Brabandere, 'Propaganda' (2012) *Max Planck Encyclopedia of Public International Law*, para. 1.
[58] See Robert Noggle, 'The Ethics of Manipulation', in Edward N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Summer 2018 Edition), para. 3.3 (emphasis added).
[59] B.S. Murty, *The International Law of Propaganda: The Ideological Instrument and World Public Order* (New Haven: Martinus Nijhoff, 1985), p. lxvii.
[60] Ibid., p. 28.

Donald Trump, while consistently offering negative coverage of Hilary Clinton. The scale of the alleged activity is noteworthy, with the *New York Times* reporting that Russian agents were responsible for posts on Facebook that reached 126 million US citizens, with the content focusing on divisive issues in American politics, such as race, religion, gun rights, and gay and transgender issues.[61]

Cyber propaganda constitutes an interference in domestic political affairs where State P publishes non-factual material on the Internet, which can be accessed by the citizens in State Q, with the objective of influencing the citizens in Q to change the government, or call for a change in government policy. Under the non-intervention principle, state propaganda is an internationally wrongful act when it can be characterized as 'coercive'.

We have seen that the ordinary meaning of the word 'coercion', as understood in domestic law systems, has expanded to include psychological coercion, a situation in which P seeks to control the actions of Q by undermining Q's capacity to decide things for herself, for her own reasons. Rather than try and persuade Q through reasoned argument, or manipulate the situation in order to influence the outcome, P aims to ensure that a certain decision will be reached by undermining Q's capacity for moral agency. Moral agency, or meaningful self-determination, depends on two factors: (1) the ability of an actor to decide things for herself, and relatedly to see herself as a deliberative agent; and (2) the possession of relevant information in order to make a decision. Psychological coercion subverts one or more of these elements, undermining the target's capacity for meaningful agency, and creating an information environment that suggests there is only one sensible choice.

The notion of 'gaslighting' as one manifestation of psychological coercion is concerned with the undermining of the target's capacity to decide things for herself, for her own reasons. Gaslighting is coercive because P intends to exercise control over Q, so that Q does as P wishes (i.e. Q 'Does X'). P acts to bring this about by undermining Q's sense of self over time, so that Q will doubt her own sanity. Where P is successful, and Q does directed by P, then, we have all the elements of coercion.

Increasingly, the term 'gaslighting' is applied to Russia's information warfare operations, specifically its reflexive control techniques.[62] Han Bouwmeester, for example, describes Russian activity in terms of 'creating a pattern or providing partial information that causes an opponent to react in a predetermined fashion without realizing that he is being manipulated[;] all is mixed up, and at the end the opponent cannot see the wood for the trees.'[63] Giles Keir and his colleagues argue that Russia is seeking to influence decision-making in other states by supplying 'polluted' information to the public, often on social media, in order to influence the population to adopt a particular policy position and undermine the capacity of the state to engage in meaningful and effective political self-determination.[64]

[61] Mike Isaac and Daisuke Wakabayashi, 'Russian Influence Reached 126 Million Through Facebook Alone', *New York Times*, 30 October 2017.
[62] See, for example, Brandon Valeriano et al., '5 things we can learn from the Russian hacking scandal', *Washington Post*, January 9, 2017.
[63] Han Bouwmeester, 'Lo and Behold: Let the Truth Be Told: — Russian Deception Warfare in Crimea and Ukraine and the Return of ''Maskirovka' and 'Reflexive Control Theory', in P.A.L. Ducheine and F.P.B. Osinga (eds.), *Netherlands Annual Review of Military Studies 2017* (Berlin: T.M.C. Asser Press, 2017) 125, 140.
[64] Giles Keir, et al., 'Russian Reflexive Control' (Kingston, On: Royal Military College of Canada, 2018), p. 8.

Cyber propaganda, in the form of disinformation and fake news, is an international wrongful act under the non-intervention principle where a reasonable person would conclude that there is evidence of a sustained information campaign with the objective of denuding the capacity of the target state for effective political self-determination, where, for example, cyber propaganda 'pollutes' the democratic debate in the target state to such an extent that it undermines the capacity of the population to make a meaningful choice based on the facts, and a proper understanding of the facts.

Where a reasonable person would conclude, based on the evidence, that the objective of the outside state is to undermine the democratic process by mixing up truths with falsehoods and creating an information environment with the objective that the population reach a position predetermined by the outside power, then, such a cyber campaign is coercive in nature, and, as a consequence, is an internationally wrongful act. The success, or otherwise of the propaganda campaign is irrelevant. The prohibition in on 'coercive' behaviour (1986 *Nicaragua* (Merits) case), that is on cyber propaganda operations undertaken with the objecting of producing a particular outcome.

Conclusion

Not all uses of cyber power by states against other states are unlawful under international law. States are free to carry out cyber operations, providing there is not a rule of international law prohibiting the relevant activity. The deployment of cyber power is unlawful under the non-intervention principle where the objective is to (a) change (or maintain) the existing government in the target state, (b) change (or maintain) a particular government policy, or (c) change (or maintain) the political opinions of the population – and the activity can be categorized as coercive (and it cannot be justified).

There is no doubt that any attempt by a state to involve itself in the domestic political affairs of another state constitutes an interference in its internal affairs. The line between unfriendly interferences and unlawful interventions is, as we have seen, provided by the criterion of 'coercion' in the non-intervention principle. The ordinary and juridical meanings of the term both describe a situation whereby one actor ('P') intends that another actor ('Q') do something (or refrain from doing something), i.e. that they 'Do X' (or not 'Do X'), and P wants to be certain that this will happen. P then acts to ensure that Q 'Does X', either through the use of coercive threats (coercion of the will), or the deployment of coercive force (coercion of the body), or psychological coercion (coercion of the mind). Because of P's actions, Q has no choice but to 'Do X', and there is consequently a denial of Q's moral agency, or capacity for self-determination. Where Q 'Does X', we have all the elements of coercion. But where Q does not 'Do X', P's behaviour can still be categorized as 'coercive' where a reasonable observer would conclude that P's actions were undertaken with the objective of putting Q in a situation where she had no choice but to 'Do X'.

Cyber power is coercive where State P compels State Q to 'do X' in order to achieve some objective of P's, and Q 'Does X'. Applying this understanding to foreign state interferences in democracy, we can see that the hacking of elections would be an example of coercion. P is deploying its cyber power in order to get Q to 'Do X'. Where this is successful and Q 'Does X', we have all the elements of coercion. There is an absolute prohibition on states using cyber power to change the outcome of an election in another state, by, for example, hacking the electoral roll to remove voters that have traditionally supported one party; hacking voting

machines to change voters' preferences or make votes disappear; and hacking the computers used to aggregate the results of the election to determine the winners. The key point is that State P works through the government institutions in State Q to realize its objective in such a way that the Election Commission in a mere mechanical instrument in State P achieving its objective. Where P is not successful (perhaps because State Q has robust cyber defences), P's actions can still be described as 'coercive', because P's objective is to get Q to 'Do X', and, if the hack were successful, Q would have had no choice but to 'Do X'.

The position in relation to information operations is more complicated. There is a long-standing prohibition in international law on subversive interventions, that is explicit calls on the population to reject the system of government. Emer de Vattel explains the point succinctly: 'It is a violation of the law of nations *to invite those subjects to revolt* who actually pay obedience to their sovereign'. It is the very fact of calling for revolution in another state which is wrongful, its success or failure is irrelevant. The prohibition on subversive interventions does not, however, prevent an outside power from seeking to influence the outcome of the existing constitutional process (a subversive intervention is concerned with the destruction or replacement of the constitutional system).

There are two relevant issues when considering the legality of state propaganda under the non-intervention principle, including cyber operations: (1) is the information true; and (2) if it is not true, can it be characterized as 'coercive'? There is widespread acceptance that the interdiction against one state interfering in the domestic political affairs of another state does not apply to factual information. The converse is not the case, however: 'fake news' is not, ip*so jure*, prohibited under the non-intervention principle. Fake news, that is information that mimics the traditional news media, but lacks its commitment to accuracy, is manipulative; it is not coercive, and the line between unfriendly interferences in the political affairs of democratic states and unlawful interventions is provided by the element of 'coercion'.

Propaganda is a form of psychological coercion, which works by undermining the capacity of the target to decide things for herself, for her own reasons; and/or creating an information environment in which the target sees herself as having only one choice (i.e. to 'Do X'). The target can appear to be acting freely, but in reality her capacity for meaningful self-determination has been destroyed, in order that she does as directed by the coercing power.

Propaganda works by mixing up truth and lies, fact and fiction, undermining the capacity of the target population for meaningful political self-determination. When accompanied by an overwhelming information campaign whereby a single narrative dominates the political discourse, State P can bring about a situation whereby the population in State Q has no choice but to 'Do X' (elect P's preferred candidate as President). Where an outside power intends to determine the outcome of the political processes of another state, and acts on that intention, that behaviour is 'coercive' in nature. Thus, where a reasonable observer would conclude that the objective of a foreign state cyber operation, undertaken over a period of time, was to undermine the capacity of the target population for meaningful political participation through the promulgation of fake news and the development of a single political narrative, that behaviour would be coercive, and, consequently, an internationally wrongful act, allowing the target state to introduce counter-measures to force the outside power to cease its offensive cyber operation.