CAMBRIDGE INITIATIVE *on* PEACE SETTLEMENTS

Making peace work through law

UKRAINE SETTLEMENT PROJECT

UKRAINE SETTLEMENT OPTIONS:

Information Operations

By Talita Dias

August 2022

UNIVERSITY OF CAMBRIDGE
Department of Politics and International Studies

Harvard Negotiation Project
HARVARD LAW SCHOOL
LEX ET IUSTITIA

OpinioJuris

Map of Ukraine on digital screen. Credit: Getty Images.

UKRAINE SETTLEMENT OPTIONS PAPER

INFORMATION OPERATIONS IN A RUSSIA-UKRAINE PEACE SETTLEMENT

Dr Talita Dias *is the Shaw Foundation Junior Research Fellow in Law at Jesus College, Oxford, as well as a Research Fellow with the Oxford Institute for Ethics, Law and Armed Conflict (ELAC), at the Blavatnik School of Government.*

A shorter version of this paper has been published on Opinio Juris. The views expressed in this paper are the author's alone.

1. INTRODUCTION

A prime example of 'hybrid warfare', the ongoing conflict between Russia and Ukraine has witnessed a wide range of kinetic and digital operations. Even before the 24 February 2022 invasion and at least since the Russian annexation of Crimea in 2014, cyber and information operations have been deployed side-by-side, setting the stage for and supporting traditional military operations (see here and here). This paper focuses on how information or influence operations should be dealt with in a potential peace settlement between Russia and Ukraine.

Information operations can be defined as 'any coordinated or individual deployment of digital resources for cognitive purposes to change or reinforce attitudes or behaviours of the targeted audience'. Examples include a) propaganda (the selective and carefully orchestrated presentation of information, facts or views to emotionally influence and/or manipulate audiences), b) disinformation (i.e., the dissemination of knowingly or deliberately false information), b) misinformation (i.e., the dissemination of false information without knowledge of its inaccuracy and/or the intention to deceive), c) malinformation (i.e., the dissemination of verifiable information, personal views or opinions to cause harm, such as doxing), and d) hate speech (i.e. the use of rhetoric to attack, denigrate or dehumanise individuals or groups on the basis of protected characteristics, such as race, ethnicity, nationality, religion, gender, sexual orientation or disability). Although each type of information operation has distinctive traits and legal consequences, the four categories often overlap. They have been instrumental in fuelling and sustaining the Russia-Ukraine conflict, by garnering support from soldiers, policymakers, and the public of both conflict parties as well as abroad. Information is power – nowhere is this more evident than in this war.

On the Russian side, the invasion – dubbed a 'special military operation' – has been justified by baseless allegations made on traditional and online media that Ukraine is run and inhabited by 'neo-Nazis' who have subjected ethnic Russians in Eastern Ukraine to genocide and war crimes. Likewise, Russia has not only falsely claimed that civilian objects were being used as military facilities but also that atrocities committed in Mariupol and Bucha were staged by Ukrainian forces. After accusing Ukraine of producing chemical, nuclear and biological weapons, Pro-Kremlin TV outlets suggested that Russia would retaliate by using intercontinental ballistic missiles against western European capitals, contrary to its established military doctrine. Some supporters have explicitly threatened western countries with escalation into World War III if they continue to supply weapons to Ukraine. And in an emblematic mix

of propaganda, disinformation and online hate, Russian state news agency RIA Novosti published an op-ed setting out a clear plan to 'de-Nazify' Ukraine. The plan included not only the 'inevitable hardships of a just war' to punish 'Nazi authorities' and their 'passive supporters', but also the 'elimination' of Ukrainian elites, the imposition of forced labour on other Ukrainian citizens and full-scale Russian censorship to ultimately 'destroy' Ukraine as an independent nation-state. A key step to ensuring control of Russia's online environment was the Kremlin's gradual infiltration of the country's main social media outlet, VKontakte, before the war. These and other systematic information operations have led Russian opposition leader Alexey Navalny to argue that '[p]ropagandists create the kind of public opinion that no longer simply allows Putin to commit war crimes, but demands them of him', justifying their treatment as 'war criminals'.

On the Ukrainian side, we have seen the online dissemination of countless videos depicting Russian prisoners of war in coercive conditions. Some of those videos displayed captives' personal information, or contained unverified accounts that soldiers have been conscripted to the 'special operation' against their will. Ukraine has also used facial recognition software to identify dead Russian soldiers and send gruesome photos of their corpses to their families with threatening messages about the war. Online hate against Russian soldiers, leaders and even civilians, including clear expressions of incitement to violence and hostility, has been prevalent on social media. Though it later banned explicit calls to death of Russian leaders and civilians, Meta has allowed hate speech against Russian soldiers and their allies in some countries as 'an expression of self-defence'.

Against this background, this paper argues that information operations ought to feature specifically in any future peace settlement between Russia and Ukraine. This is so given their significance in enabling and supporting the armed conflict. War and atrocities do not happen in a vacuum but require a conducive information environment (see here, here, here, and here). Thus, to stop the war and prevent future conflict, parties should commit to specific measures to tackle information operations that are detrimental to achieving peace and stability in the region, in line with internationally recognised human rights. The parties' negotiated approach to conflict-related information operations should mirror and flesh out existing international law on the matter.

It is important to reiterate that existing international law applies *by default* and *in its entirety* to information and communications technologies (ICTs), just as it does to other technologies. This is true insofar as conventional and customary rules have a general scope of application and can be interpreted to accommodate new phenomena. Though helpful in clarifying how international law applies online, 'domain-specific' state practice and *opinio juris* are not necessary to prove that existing rules and principles apply to digital information operations. Several rules of international law – general and specific – already regulate different types of information operations. Examples include the prohibition of incitement to violence, war propaganda and some types of disinformation concerning international relations. Although crafted decades before digital technologies emerged, the content of these rules is sufficiently broad and flexible to cover analogue and digital information operations.

A negotiated deal between Russia and Ukraine would be a unique opportunity to strengthen those rules and complement them with specific provisions on how the parties should regulate the online environment to stop the war and prevent further conflict. To be sure, a negotiated settlement should neither address the issue in general nor go through the minutiae. Rather, the focus should be on those types and aspects of information operations that relate to the armed conflict and whose regulation is essential to securing peace, without compromising other parts of the agreement. A negotiated settlement should serve to stop the ongoing conflict and deter

future ones. In what follows, this paper explains what this approach should look like for each type of information operation identified above, i.e., propaganda, dis- and misinformation, malinformation, and hate speech. For each of those operations, the paper discusses how parties should craft provisions dealing with both state obligations and individual rights and responsibilities.

2. PROPAGANDA

According to a recent Microsoft report, Russian cyber influence operations have not only targeted Russian and Ukrainian audiences but steadily reached western and non-aligned countries. Notably, these operations 'successfully increased the spread of Russian propaganda after the war began by 216 percent in Ukraine and 82 percent in the United States.' In the same vein, the popularity of President Zelenksy's videos on YouTube and other platforms is a testament to the importance of Ukrainian propaganda or 'communications strategy' in garnering attention and support for the Ukrainian war effort.

Propaganda and other strategies to influence or convince others are part and parcel of social life, domestically and internationally, in peacetime and war. Thus, they have not been generally prohibited under international law. However, certain types of propaganda may cross a threshold of dangerousness given their intention or propensity to incite or support civil unrest, domestic regime change or war. 'Hostile' or 'subversive' propaganda has been prohibited under customary international law at least since the eighteenth century when revolutionary France withdrew its public call to support independence movements abroad (see van Dyke, at 58, 60-65, 73; Preuss, at 652; Larson, at 445-447; Whitton, at 15-18; De Brabandere, §§12-16). Subversive propaganda carried out by state organs directly, or non-state groups acting with the support of a state, has been traditionally considered a violation of the principle of non-intervention in the internal or external affairs of the targeted state. The assumption is that, just like the use or threat of force, subversive propaganda directed at foreign audiences may force a state to steer its internal or external affairs against its will (see *Nicaragua*, § 205). Thus, the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, adopted by the UN General Assembly in 1965, specifically included within the scope of the principle of non-intervention 'the duty of states to abstain 'from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States'. Propaganda that constitutes advocacy for violations of international humanitarian law (IHL), such as indiscriminate attacks against civilians, also runs contrary to states' duty to ensure respect for IHL, enshrined in Article 1 Common to the Geneva Conventions and Article 1 of Additional Protocol I to the Conventions, as well as their customary counterpart.

More controversial is the positive duty of states to prevent or prohibit subversive propaganda *by private entities*, given concerns with the rights to freedom of expression and information (see Larson, at 449-450; van Dyke, at 65-68, 72). This is reflected in the reluctance of some states to fully embrace Article 20(1) of the International Covenant on Civil and Political Rights (ICCPR), which requires states to prohibit propaganda for war. Several states, including the United Kingdom (UK), the United States (US), France, Australia, and the Netherlands have made reservations to its scope. However, no state has ever questioned the unlawfulness of incitement to wars of aggression, whether by states or non-state actors (see Kearney, at 123, 148-149; Nowak, 473). If the use of force is itself prohibited and criminalised under international law, so is incitement to engage in it (see, e.g., Whitton, at 21; Larson, at 443-445, and *Ministries case*, at 469). Furthermore, in its General Comment 36 on the right to life (§59),

the UN Human Rights Committee asserted that failure to punish war propaganda might amount to a failure to protect the right to life under Article 6 of the ICCPR. As former members of the Soviet Union, both Russia and Ukraine championed the adoption of this provision and other efforts to curb subversive propaganda by private entities, such as the 1936 Convention concerning the Use of Broadcasting in the Cause of Peace (see, e.g., Kearney, 85-87, 100-101, 135, 137, 147. Articles 1 and 2 of this Convention read as follows:

> Article 1. The High Contracting Parties mutually undertake to prohibit and, if occasion arises, to stop without delay the broadcasting within their respective territories of any transmission which to the detriment of good international understanding is of **such a character as to incite the population of any territory to acts incompatible with the internal order or the security of a territory of a High Contracting Party**.
>
> Article 2. The High Contracting Parties mutually undertake to ensure that transmissions from stations within their respective territories shall not constitute an **incitement either to war against another High Contracting Party or to acts likely to lead thereto**. (emphasis added)

Scholarly writings (see, e.g., Kearney, at 16; Novogrod, at 104; Larson, at 450; Whitton, at 23-25) and international jurisprudence (see, e.g., *Island of Palmas*, at 839; *Trail Smelter*, at 1963) also seem to indicate that subversive propaganda may be covered by broader 'due diligence' obligations under international law, such as the duty to prevent acts contrary to the rights of other states (see *Corfu Channel case*, at 22) or significant transboundary harm or injury to persons, property or the environment (see International Law Commission, Draft articles on Prevention of Transboundary Harm from Hazardous Activities). Nevertheless, any prohibition, criminal or civil, of incitement to or propaganda for war by individuals must be subject to the strict requirements of legality, legitimacy, necessity, and proportionality for limiting the rights to freedom of expression and information (see UN Human Rights Council, Rabat Plan of Action, para 18). Such requirements are found in Article 19(3) of the ICCPR and its regional counterparts, including Article 10 of the European Convention on Human Rights. They are a fundamental safeguard against state action that purports to prevent violence by silencing the opposition.

The war in Ukraine reminds us of the importance of upholding these existing international obligations. The speed and reach of subversive propaganda in the digital age is unprecedented, and so are concerns for protecting freedom of expression and information online. If a ceasefire successfully ends kinetic confrontations but subversive propaganda continues unhinged, any peace settlement will likely be short-lived. Thus, a peaceful settlement should include, at the very least, the following mutual commitments:

a) Not to engage directly in or support propaganda that incites the use of armed force, violence, or regime change, or advocates for IHL violations.
b) To exercise due diligence in preventing, stopping, or redressing propaganda that incites the use of armed force, violence, or regime change, or advocates for IHL violations.
c) To adopt specific steps to reduce the dissemination of propaganda for war online, such as by requiring online platforms operating in their territories to monitor and remove clear instances of incitement to wars of aggression and to deprioritise or otherwise limit the visibility of less serious forms of subversive propaganda or advocacy for IHL violations.
d) That any efforts to curb the effect of war propaganda be undertaken in line with the rights to freedom of expression and information under international human rights law, particularly Article 19(3) of the ICCPR, including the need to enact a clear and accessible domestic legal framework when limiting speech acts and to calibrate limitation measures, such as content moderation, to the seriousness of the content.

3. MIS/DISINFORMATION

Although 'fake news' has become a buzzword in recent years, it is not a new phenomenon. The intentional or non-intentional dissemination of false or misleading information has been a key feature of warfare and peacetime political strategy for centuries. Think of Nazi Germany's staged border incidents, used to justify the 1939 invasion of Poland, along with Goering and Keppler's fictitious telegram claiming the Austrian government had requested a military intervention from Germany. Think also of the United States' unfounded claims that Saddam Hussein was manufacturing weapons of mass destruction to justify the 2003 Iraq invasion. More recently, COVID-19 disinformation campaigns have led to vaccine hesitancy, serious illness, and death. In this light, it is not surprising that similar types of information operations resurfaced in the context of the Russia-Ukraine conflict.

Uncertainty lurks around the international regulation of mis- and disinformation. This is primarily because of the indirect causal link between the dissemination of false or misleading information and its harmful consequences. As with other types of information operations, addressees need to act upon the information in question for any relevant results to occur. There is also a clear tension between securing a peaceful and stable information space among *states*, and *individual* rights to freedom of expression and information (see De Brabandere, §§3, 8-11). After all, the latter rights are not limited to accurate information (see *Handyside v UK*, §49, and Joint declaration on freedom of expression and "fake news", disinformation and propaganda, preambular para 7).

Nevertheless, these challenges are not unsurmountable. First, the rights to freedom of expression and information belong to *individuals*. Thus, states themselves may not fabricate, sponsor, encourage or further disseminate statements or information that they should reasonably know are false (Joint declaration on freedom of expression and "fake news", disinformation and propaganda, §2(c)). This is true at the very least insofar as the false statements amount to a prohibited intervention in the internal or external affairs of other states (see Larson, at 442, 447-449; De Brabandere, §§17-20, Baade, at 1362-1365). Second, since the meaning of *coercive* interference is not limited to the threat or use of force, it extends to deceptions that intentionally, foreseeably, or effectively force a state to adopt a course of action that it otherwise would not. Thus, false statements aimed at regime change or foreign electoral processes would be contrary to the prohibition of non-intervention, whether online or offline.

However, if false or misleading statements that may cause harm or injury in another state cannot be attributed to states but emanate from individuals, the freedoms of expression and information come into play. Obligations requiring states to exercise due diligence to prevent, stop or redress harm to other states must not overstep permissible limitations to the rights to freedom of expression and information. This is the case for the obligation contained in Article 3 of the 1936 Convention Concerning the Use of Broadcasting in the Cause of Peace, to which Russia is still a party:

> Article 3. The High Contracting Parties mutually undertake to prohibit and, if occasion arises, to stop without delay within their respective territories **any transmission likely to harm good international understanding by statements the incorrectness of which is or ought to be known to the persons responsible for the broadcast**. They further mutually undertake to ensure that any transmission likely to harm good international understanding by incorrect statements shall be rectified at the earliest possible moment by the most effective means, even if the incorrectness has become apparent only after the broadcast has taken place. (emphasis added)

To comply with the rights to freedom of expression and information, any action seeking to prohibit or stop false or misleading statements that threaten international peace and security must be clearly grounded in law, as well as necessary and proportionate to achieve that aim. This will usually mean that, while the intentional dissemination of disinformation may be subject to limitations, such as content moderation and civil liability, the non-intentional spread of such content should not be sanctioned (see Joint declaration on freedom of expression and "fake news", disinformation and propaganda, preambular paras 4 and 5, operative §1(e)). Criminal sanctions should be reserved for the most serious forms of disinformation, such as defamation and libel (Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/HRC/47/25, §§41-43).

In the context of a negotiated peace settlement between Russia and Ukraine, both parties should agree:

a) Not to make, sponsor, encourage or further disseminate statements or information that they know or reasonably should know to be false and may foreseeably interfere in the internal or external affairs of the other party.
b) To exercise their best efforts to prevent, stop and redress the intentional dissemination of false information that is foreseeably contrary to the rights of the other party or otherwise causes harm or injury to persons, property, or the environment therein.
c) To strictly observe the rights to freedom of expression and information in their jurisdiction, particularly by ensuring that any efforts to curb dis- or misinformation are in line with the requirements of legality, legitimacy, necessity and proportionality.

4. MALINFORMATION

The dissemination of accurate information or opinions with the intent to cause harm is not per se prohibited under international law. However, malinformation may violate the prohibition of non-intervention insofar as the leak or publication is intended to coerce, or foreseeably or effectively coerces, a state in matters within its internal or external affairs. This could happen if, for example, leaked confidential information about the identity or location of undercover state operatives compromises law enforcement or military operations. Likewise, states must exercise due diligence in preventing or redressing the release of such information if it is of such a nature as to contravene the rights of the victim state or to cause harm or injury to persons, property or environment therein.

Malinformation is usually preceded by cyber espionage and/or electronic surveillance operations. While many would argue that the exfiltration of governmental data is not itself unlawful under international law, the method by which such information is extracted may violate a primary rule of international law, depending on the consequences of the operation in question (see Coco, Dias and van Benthem). In the same vein, electronic surveillance against individuals may violate the right to privacy, unless the operation is carried out in accordance with law and is necessary and proportionate to achieve a legitimate aim (see, e.g., Article 17 ICCPR, and Article 8, European Convention on Human Rights).

Specific rules of IHL also prohibit or otherwise limit the disclosure of private information relating to prisoners of war. Examples include Articles 13(2) and 14 of the Third Geneva Convention, which protect prisoners of war from insults and public curiosity, and entitles them to respect for their persons and honour. According to the International Committee of the Red Cross, this means that the dissemination of videos or images depicting prisoners of war is generally unlawful, even if it serves as proof of life or evidence of international crimes. This is

so unless the identity of prisoners can be protected, or there is a compelling public or individual interest in revealing their identity, such as when prisoners are missing or accused of war crimes.

In a future peace settlement between Russia and Ukraine, both parties should:

a) Caution against the use of malimformation and commit not to employ it in a manner contrary to established rights and obligations under international law, such as non-intervention, due diligence, individual privacy and IHL;
b) Specifically agree not to release images, videos, or other information about prisoners of war into the public domain in ways that would attract public curiosity or otherwise violate prisoners' honour.

5. ONLINE HATE SPEECH

The term 'online hate speech' does not refer to a single phenomenon. Rather, the concept encompasses a multitude of digital content – from hateful emojis ('hatemojis') to fully-fledged direct and public incitement to commit genocide of the kind seen during the Rwandan genocide. Thus, international legal responses to online hate will naturally vary depending on the content, as well as the speaker, audience, medium, and context. A tiered approach to the problem is warranted, taking into account two key international legal frameworks: international human rights law and international criminal law.

The first tier corresponds to the most serious types of online hate speech amounting to international crimes and entailing both individual criminal liability and state responsibility for internationally wrongful acts (see *Bosnian Genocide* case, §§ 160-169). Within this category falls the inchoate offence of direct and public incitement to commit genocide, prohibited under Article III(c) of the Genocide Convention and its customary counterpart. Although context is key in determining whether seemingly neutral expressions do amount to direct incitement to genocide, such as the use of coded language calling for violence by targeted audiences, only the most serious forms of online hate speech amount to this offence. As in the case of Rwandan cartoons and radio broadcasts, referring to individuals or groups as animals that ought to be killed, such as snakes, rats, cockroaches, or other parasites, in the context of intercommunal violence, may amount to direct and public incitement to genocide (see Lynne, at 175-176; *Media Case*, §477-672; see also Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar, §§1316-1318).

Serious forms of online hate speech may also amount to instigation or aiding and abetting international crimes, including genocide, crimes against humanity and war crimes (see, e.g., Report of the Independent International Fact-Finding Mission in Myanmar, A/HRC/39/64, §§83-89). However, in those instances, participation in crime requires not only an intention to instigate, or assist in the commission of the relevant crime but also a subjective or objective causal link between the criminal conduct and the result (see *Media Case*, §477-672). 'Mere hate speech' below this threshold is unlikely to amount to the commission of international crimes, especially given the lack of a sufficiently clear criminalisation of the speech acts in question (see Partly Dissenting Opinion of Judge Theodor Meron in the Media Case, §§5-8).

The second tier consists of hateful expressions amounting to incitement to certain types of unlawful action. A prominent example is found in Article 20(2) of the ICCPR, which stipulates that '[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.' Like the prohibition of propaganda for war, the wording and the very inclusion of this provision in the Covenant were not without controversy. Some states, like the US, the UK and the Netherlands, still reserve

their right not to enact legislation to give effect to this provision, citing freedom of expression concerns (see Temperman, at 72-74). For its part, the Human Rights Committee has suggested that Article 20(2) ICCPR is part of customary international law so that any reservations would be invalid or ineffective (see General Comment no. 24, §8). Thus, the Committee has insisted that insufficient national legislation prohibiting, though not necessarily criminalising, incitement to violence, hostility or discrimination, may be incompatible with the provision (see General Comment no. 11). A similar debate exists over the scope and status of Article 4(a) of the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD).

A closer look at the drafting history of Article 20(2) ICCPR reveals that no state has disputed the need to prohibit incitement to violence and similar lawless action (see Kearney, at 123, 164). Notably, Article 13(5) of the American Convention of Human Rights, which requires states to prohibit 'incitement(s) to lawless violence or any other similar action against any person or group of persons on any grounds', was drafted by the US, one of the few states still opposing Article 20(2) ICCPR and Article 4(a) ICERD (Kearney, at 179). This wording purposely mirrors the so-called *Brandenburg* test (see *Brandenburg v Ohio*), devised by the US Supreme Court to draw the boundaries of permissible interference with freedom of expression, in accordance with the First Amendment to the US Constitution. Thus, a strict reading of both Article 20(2) ICCPR and Article 4(a) ICERD to include only imminent cases of incitement or violence or other serious harm could find common ground between states. It would also conform with the requirements for limiting freedom of expression and information under Article 19(3) ICCPR, which also apply to Article 20 (see UN Human Rights Council, Rabat Plan of Action, para 18; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/74/486, §§12-13).

The third tier of online hate is 'limited speech', i.e., hateful expressions that are in principle protected but may be limited pursuant to the four-part test described in Article 19(3) ICCPR and equivalent provisions, i.e., legality, legitimacy, necessity and proportionality. Thus, denial of historical facts such as the Holocaust, while not necessarily amounting to incitement to violence or other harm within the meaning of Article 20(2), may nonetheless be limited by law in contexts where this would be a necessary and proportionate step to safeguard the rights or reputations of others or public order (see, e.g., Human Rights Committee, *Faurrison v. France*, 8 November 1996). All other forms of online hate falling below this threshold, i.e., that cannot be limited via the four-part test, must be protected. Though there is no defined category of 'protected speech', since all speech acts, including hate speech, may potentially be subject to limitations, some types of speech should receive heightened protection. This includes political speech and statements whose dissemination is in the public interest, such as impartial journalistic reporting on public affairs.

This tiered approach to online hate speech should be reflected in any peace deal between Russia and Ukraine. In particular, a negotiated settlement should:

a) Reaffirm the prohibition and criminalisation of direct and public incitement to genocide as well as the participation in the commission of other international crimes via hate speech acts that amount to instigation or aiding and abetting such crimes.
b) Reaffirm the duty of both parties to exercise due diligence in preventing and punishing all core international crimes, i.e., genocide, crimes against humanity, war crimes and the crime of aggression.
c) Clarify that hate speech online and offline that amounts to incitement to imminent violence or harm to individuals or groups on any ground must be prohibited by clear and accessible laws that provide for measures that are necessary and proportionate to

sanction or limit such speech acts, in line with the rights to freedom of expression and information under international human rights law.

d) Reiterate that other forms of hate speech online and offline must in principle be protected, unless it becomes necessary and proportionate to limit such speech acts by law to respect the rights or reputations of others or for the protection of national security, public order, public health, or morals.

CONCLUSION

The frequency and intensity of information operations in connection with the conflict between Russia and Ukraine call for specific treatment of such operations in any future peace settlement. This should be an opportunity for both parties to reaffirm and flesh out their commitment to existing international law protections applicable online, including those specific to information operations. Though these operations and their specific international regulation have often been overlooked in debates over cyber conflict or hybrid warfare, the analysis above has shown that international law already provides for robust protection against their harms and risks, whilst safeguarding fundamental human rights online and offline. Most pressing among the parties' existing international obligations are the prohibitions of propaganda for war and incitement to genocide, breach of which could seriously undermine a peace settlement. Thus, the parties should consider agreeing to monitor the implementation of those commitments, whether through an existing institution, such as a United Nations body or a third state, or an ad hoc monitoring mechanism. Navigating the inherent tensions between state and individual interests will not be easy, especially considering the internet's decentralised architecture, coupled with its unprecedented speed and reach. However, taking up this task is imperative if both parties are truly committed to resolving the conflict and preventing future war.