Study on International Norms for Foreign Information Manipulation and Interference (FIMI)

November 2023

European Union
EXTERNAL ACTION

Prepared by: Dr. Talita Dias. Research Fellow. Oxford Institute for Ethics, Law and Armed Conflict (ELAC), Blavatnik School of Government. University of Oxford.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

- This research paper is entitled 'Study on International Norms for Foreign Information Manipulation and Interference (FIMI)'. Its purpose is to offer recommendations on the development of international norms specific to FIMI, including the content of those norms and their development processes.
- It will do so by drawing on existing rules and principles of international law applicable to FIMI as well as norm-setting processes established in related fields, such as cyberspace.
- Prominent norm-setting processes include those established within the auspices of the United Nations (UN) to discuss the use of information and communications technologies (ICTs) in the context of international peace and security and internet governance.
- This study is centred on FIMI. Nevertheless, it concludes that, while operational frameworks developed to tackle FIMI tend to be behaviour-centric, international law applies more broadly to information operations writ large. Different factors are relevant when assessing the lawfulness of FIMI and other information operations under international law, particularly their content, means and methods, effects, actors, and targets. This analysis is in many ways similar to and overlaps with the work has already been carried out by the European External Action Service (EEAS) using the so-called ABCDE framework, which looks at the actor, behaviour, content, degree, effect of FIMI operations.
- To understand the international legal framework applicable to FIMI, it is necessary to consider how international law applies to various types of information operations – not just FIMI.
- In line with international law, norms for FIMI should consider not only the means and methods by which these activities are carried out but also their actors, content, targets, effects, and other relevant legal criteria, similarly to the way the EEAS uses the ABCDE framework.
- The international legal framework applicable to FIMI is made up of different but related rules and principles applicable to the behaviour of States and non-State actors online and offline; these must be considered holistically.
- International legal rules and principles applicable to FIMI include sovereignty, non-intervention, due diligence, State responsibility, international human rights law and international humanitarian law.
- They overlap to some extent but cover different phenomena and therefore different types of FIMI, based on their particular triggers, thresholds and conditions.
- The human rights to freedom of expression and information, recognised under international human rights law, lie at the heart and centre of the applicable international legal framework and should inform FIMI norms. They require that any limitations on private speech, including lawful or unlawful FIMI activities, be grounded in law, legitimate, necessary, and proportionate.
- International norms for FIMI should mirror this international legal framework. Drawing on the lessons from the cyber and internet governance contexts, their drafting process should be State-led, inclusive of as many like-minded States as possible, including developed and developed countries, consensus-based, and informed by the input of different stakeholders, such as the industry, academia, and civil society.

INTRODUCTION

Foreign Information Manipulation and Interference (FIMI) is one of the most pressing threats to an open, free, and diverse information environment in the digital age. The European External Action Service (EEAS) defines it as:

> *"a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory."*[1]

The key values, processes and procedures affected by FIMI include a) political processes, such as elections and referendums, b) trust in public institutions and democracy as a whole, c) individual life and health, d) the protection of the natural environment, e) the credibility of scientific knowledge, and f) national or international order, peace and security.[2] FIMI has been deployed in different parts of the world, including developed and developing countries.[3] Most notably, the United States' 2016 presidential election, the Brexit referendum in the United Kingdom, and the fight against COVID-19 have all been undermined by different types of FIMI.[4] More recently, Russia's invasion of Ukraine and its military operations on the ground have drawn strong support from FIMI activities carried out in the digital space.[5] The narratives employed in this context have ranged from false accusations that Ukraine has committed genocide, used its population as human shields, or manufactured biological or chemical weapons.[6]

As a behaviour-centric concept, FIMI is characterised by the deployment of different tactics, techniques and procedures (TTPs).[7] Tactics correspond to the various objectives that FIMI actors may aim at, ranging from the dismissal or distortion of facts to social division.[8] Techniques are the various ways in which those aims can be achieved at the different stages of an operation, namely, planning, preparation and execution.[9] There are a multitude of techniques deployed by FIMI actors, but the most prominent ones include intelligence-gathering, image, video or text manipulation or development, followed by content dissemination and amplification on online platforms.[10] The concept of 'procedures' is more granular and captures trends that bring together tactics and techniques, such as the exact pattern or signature employed by persistent actors.[11]

By focussing on TTPs, the concept of FIMI has important advantages. In particular, it avoids political, social or cultural controversies over the content of the information manipulated as well as overreliance on actor attribution. Relatedly, this behavioural focus enables more rapid responses to FIMI. Behavioural considerations also open the door to new types of frameworks that could be used to counter the phenomenon, such as the DISARM framework.[12] An important tool is the detection of suspicious patterns of behaviour, typically used by cybersecurity experts against malware and now deployed by online platforms to tackle information manipulation.[13] For those reasons, the concept of FIMI lies at the heart of this paper and will be used throughout. At the same time, this study acknowledges that other types of digitally-enabled information or influence operations that do not neatly fall within the definition of FIMI are also cause for concern. These are often closely connected to FIMI activities.

It is important to note that the scope of international law goes beyond FIMI to cover a wider variety of information or influence operations. These can be defined as 'any coordinated or individual deployment [or use] of digital resources for cognitive purposes to change or reinforce attitudes or behaviours of the targeted audience'.[14] Information operations include disinformation (the dissemination of knowingly or deliberately false information), misinformation (the non-intentional dissemination of false or misleading information), propaganda (the selective presentation of information, facts or views to emotionally influence and/or manipulate audiences), malinformation (the intentional dissemination of accurate information, usually obtained by illegal means, such as doxing), and hate speech.[15] Even when carried out by digital means, these have been linked to significant individual and societal harms to the values, processes and procedures identified earlier. Examples include harms to human life and health and reputational harm to individuals, businesses, and public institutions.[16]

The concept of 'information operations' overlaps with but is broader than FIMI. Unlike FIMI, it includes *unintentional conduct, the dissemination of accurate information in harmful ways or for malicious purposes, isolated instances of information manipulation, and domestic influence operations.*[17] But the two concepts or classifications take into account the same or similar factors: a) actors, b) behaviours, including means and methods deployed, c) content or 'narratives', and d) effects.[18]

While this study focuses on FIMI, it takes into account a wider pool of information operations. This is because the same rules that apply to FIMI, such as sovereignty, non-intervention, and due diligence, also apply to other types of information operations. Thus, to understand why and how international law applies to FIMI, one must consider how it applies to other types of information operations too.

When thinking about how international law applies to FIMI, two considerations should be borne in mind. First, international rules and principles do not necessarily focus on the manipulative or harmful *behaviour at hand. Instead, the application of international law in this context depends, first and foremost, on the actor behind it. As will be explored in Section 2, international law as a whole applies online and it does offline.*[19] However, it is State-centric, with most of its rights and obligations still vested in States.[20] When international law recognises rights and obligations for other actors, such as individuals and corporations, different rules apply.[21] Therefore, to understand the extent to which international law applies to FIMI, one must consider which *actors are at the origin of those acts and which ones are affected by them.*

Secondly and relatedly, the manipulation of information and its dissemination are primarily speech or verbal acts.[22] This means that any legal analysis of the subject requires consideration of the rights of individuals and other private entities to receive and impart information freely – the freedoms of information and expression.[23] As will be discussed in the next section, the international legal framework for information operations is an intricate juxtaposition of State rights and obligations that must be balanced against the right of private actors to receive and impart information. This in turn means that an analysis of the content in question is inescapable. To know if States may prohibit, take down or otherwise limit a certain information operation, including strictly lawful speech acts falling within the concept of FIMI, one needs to assess if the content in question amounts to war propaganda, incitement, defamation or affects other public policy interests, such as public health, security or order.[24]

FIMI and other information operations have increased in scale and speed, given the multiplying effect of engagement-based algorithms and advertisement business models.[25] An additional concern has been the use of generative artificial intelligence (AI), especially large language models such as chatbots, to produce false, misleading or otherwise harmful content at an even larger scale.[26] AI-generated information operations can be cheaper, more widespread and persuasive, as well as less detectable than traditional campaigns orchestrated by human beings.[27] This increases the risk of harm resulting from them.

As noted earlier, serious harms – both individual and systemic – have been attributed or linked to information operations. They include increased health risks, scientific confusion, climate inaction, political disenfranchisement, social division, discrimination on different grounds, and even violence. However, the causal connection between information operations and such harms is not a given. As a verbal act, the manipulation or dissemination of information cannot, in and of itself, cause physical damage or wider societal harm.[28] Only moral harms can result directly from an information operation, such as the reputational harm arising from defamation or the moral impact of online hate speech on victims. Information manipulation is a cognitive or psychological operation, acting on the mind of its audience. As such, to cause harm, addressees still need to *act upon any information received. Thus, factual causation between information operations and real-world harms is often indirect.*[29] However, this does not mean that the phenomenon escapes international law.[30] Though international law lacks general standards of factual or legal causation,[31] key rules and principles do not require proof of a direct causal link between conduct and result to apply. Rather, they prohibit conduct that *may cause harm or require action that may prevent it.*[32] Foreseeability or probability of harm, as opposed to actual causation, is the key criterion for this link to be established.[33] Many rules of international law also do not require any effects or results of a certain prohibited conduct to be breached.[34] At any rate, there is growing empirical research in support of the actual and potential impact of FIMI and other information operations on individuals and society at large.[35]

That international law applies to information and communications technologies (ICTs) and information operations in particular is thus the premise of this study.[36] But why is it important to delve deeper into this question, identifying which exact rules apply and how they apply to the phenomenon? Most importantly, why look to such rules and principles to develop international norms for FIMI and other forms of information manipulation?

International law is a global framework of binding rules and principles that seek to constrain the behaviour of States and other actors, including intergovernmental organisations, corporations and individuals. By laying down the rules of the game and ensuring accountability for violations, international law protects important interests whilst bringing clarity, predictability and trust among different actors that operate in an increasingly borderless environment.[37] International law is formally made by States via treaties, customary international law, i.e., the widespread and consistent

practice of States accepted as law and general principles of law derived from domestic law.[38] Its enforcement is also decentralised: there is no single international court or law enforcement agency to apply and enforce it.[39] Different international courts and tribunals resolve disputes by making decisions that are binding on the parties, subject to the consent of the States involved. And only States can use forcible or non-forcible measures to ensure compliance with international law.[40] Yet the making and application of international law increasingly involve varying types and levels of multistakeholder participation.[41] For example, civil society organisations get to observe treaty negotiations and related discussions. Academics play a key role in the interpretation and clarification of international law.[42] And corporations, including tech companies, are instrumental in the enforcement of international law.[43] This is especially true online, where they own or operate key infrastructure and software, such as online platforms and AI. Thus, ensuring respect for international law by all relevant actors is an important tool in the fight against FIMI and its harmful consequences.

In contrast, norms are non-binding, political agreements that seek to establish a common basis for decision-making at different policy levels.[44] Often called 'soft law', they can be developed and agreed on by States as well as non-State actors, such as corporations and civil society organisations, without any particular formalities.[45] They usually set goals or standards of conduct that their authors aspire to, without the threat of legal sanctions for non-compliance. Norms are thus voluntary or non-binding, relying primarily on the carrot rather than the stick to drive compliance. Far from a weakness, this is their main strength: without the fear of formal commitment, States and other stakeholders can go further in *what* they are willing to agree to. While the buy-in costs are low, the incentives are usually high: it looks good for States, corporations, and other actors to have accepted certain commitments as a compromise or a gesture of goodwill vis-à-vis their stakeholders. This far outweighs any social, and reputational costs of non-compliance.

Therefore, norms are a powerful way to find consensus among States (as well as other actors) and fill legal gaps. They are a middle ground between inaction and binding obligations and as such can be a steppingstone to future legal developments. They can bring different stakeholders around the table and offer greater flexibility in terms of what can be agreed upon and how it can be agreed. Norms can be used to complement international law in different ways. Aside from expanding the scope of agreement beyond existing international law, norms can flesh out the interpretation of its rules and principles and provide guidelines or best practices for their actual implementation. Norms can also develop into law, serving as a testing ground for potential legal commitments. In this way, they can foster shared understandings, trust, accountability, peace and stability among States and other stakeholders, both domestically and internationally.

Despite the agreement that international law applies to ICTs, its application to information operations has received little attention in policy, legal and academic circles.[46] This contrasts with significant developments over the last two decades in the interpretation and application of international law to cyber operations – traditionally encompassing malware and other malicious tools or techniques to target computer software, hardware, and data.

Most notably, the United Nations (UN) Secretary-General, at the request of the UN General Assembly, established the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.[47] The GGE recognised that international law, and in particular the UN Charter, applies to ICTs and is essential to maintaining peace, security, stability, openness and accessibility in the cyber context.[48] The Group highlighted several rules and principles of international law of particular importance in cyberspace, including sovereign equality, peaceful settlement of international disputes, the prohibition on the use of force, respect for human rights and fundamental freedoms, non-intervention in the internal affairs of other States, and key principles of international humanitarian law (IHL).[49] Their application to cyber operations was fleshed out in the Group's final report, issued in 2021.[50] The GGE also adopted 11 'norms of responsible State behaviour in the ICT environment, which will be the focus of Part III of this study.[51] In parallel to the GGE, the Assembly also established the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) in 2019.[52] The OEWG both reaffirmed the GGE's findings on international law and endorsed its 11 norms of responsible State behaviour in the ICT environment.[53]

As discussed in Part III below, the OEWG has considered the use of ICTs 'to interfere in their internal affairs […] by means of information operations and disinformation campaigns' as a key threat in its first substantive report.[54] Furthermore, in line with the GGE's 2021 report,[55] the OEWG's 2023 annual progress report has noted the 'worrying increase' in 'malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability

of another State'.[56] According to both groups, 'these uses undermine trust, are potentially escalatory and can threaten international peace and security' and 'may also pose direct and indirect harm to individuals'.[57] Nonetheless, no specific norms, rules or measures for information operations have been discussed within the GGE or OEWG.

Other processes to clarify international law applicable to cyber operations and develop relevant norms have been set in motion outside the UN. Prominent among these are the Tallinn Manuals on the International Law Applicable to Cyber Operations,[58] the Oxford Process on International Law Protections in Cyberspace,[59] and the Paris Call for Trust and Security in Cyberspace.[60] All these processes are multistakeholder in nature, in that they involve the participation not only of States but also of industry and civil society representatives, including academia and NGOs. However, as noted in Part III, only the Oxford Process and the Paris Call have specifically considered the regulation of information operations, and only to a limited extent.

The issue of internet governance has also been subject to different norm- and standard-setting processes. It refers to the rules, policies, standards and practices that shape the evolution and use of the global internet.[61] In particular, the UN Secretary-General proposed to adopt a Global Digital Compact (GDC) setting out 'shared principles for an open, free and secure digital future for all'.[62] Within the GDC's agenda are the 'application of human rights online' and 'promoting a trustworthy Internet by introducing accountability criteria for discrimination and misleading content'. Both these issues are directly relevant to FIMI and other information operations. Nevertheless, the UN Secretary-General has yet to convene specific sessions on this issue, and it remains unclear whether these will ever be convened.[63] Another relevant norm-setting process in the field of internet governance is the Global Network Initiative (GNI).[64] The GNI has developed a set of principles on the rights to freedom of expression and privacy online, as well as corporate responsibility, multistakeholder collaboration, governance, accountability and transparency.[65] Yet no specific mention is made of FIMI or other information operations among them.

While cyber operations employ different tools and techniques, it is often difficult to separate them from FIMI and other information operations. The two types of operations are frequently employed side by side as part of the same political strategy, as seen in the context of the hybrid war in Ukraine. Likewise, insofar as information operations threaten peace, security, stability and freedom on the internet, they cannot escape the principles of internet governance. As noted earlier, the harms that might arise from information operations can be as serious as those caused by malicious cyber operations and other threats to our online information environment. Thus, it is surprising that information operations have not received the same level of attention as cyber operations and internet governance. Nevertheless, important lessons and great inspiration can be drawn from developments in those fields when studying international law and norms for information operations.

Prompted by this knowledge gap, the enormous potential of international law and norms, the legal and normative successes achieved in the related fields, as well as the continuing prevalence and looming expansion of information operations around the globe, this study has three key aims. First, to bring further clarity to the application of international law to FIMI and other information operations. This will be done in Part II below. Second, to assess the content and processes for setting voluntary norms in related fields, including the GGE, OEWG and other forums noted above. This will be the focus of Part III below. Third, drawing on the analysis of how international law currently applies to information operations (Part II) and of norm-setting processes established for related fields (Part III), the paper will offer a set of recommendations for the EU and its Member States, Canada and other partners on *what* norms are appropriate for FIMI and information operations, and *how* these norms should be developed. This will be done in Part IV.

This Study has been carried out by desk research into both legal and policy materials. Legal materials comprise treaties, State practice, international case law and regulatory acts of international organisations. The doctrinal method will be employed in their analysis. This consists of legal interpretation grounded in the text, context and object and purpose of legal provisions, as well as supplementary means of legal interpretation. The policy documents assessed in this Study will include resolutions and other non-binding documents adopted by various UN bodies (including the General Assembly, the Human Rights Council,[66] and the Secretary-General), reports on FIMI and related topics issued by the EEAS and the G7 Rapid Response Mechanism, declarations and statements made by different States and other stakeholders on the topic, as well as relevant academic materials, such as journal articles and book chapters.

II. THE INTERNATIONAL LEGAL FRAMEWORK APPLICABLE TO FIMI AND OTHER INFORMATION OPERATIONS

International law does not have a specific set of rules or principles tailored to FIMI or other information operations.[67] Though some have proposed the adoption or consideration of an 'international law for information operations' (ILIO), especially by the adoption of a treaty on the matter,[68] States are yet to agree on such a legal framework. The content of information operations to be prohibited, permitted, or limited is a clear point of contention among States – including Western and non-Western countries, and even among traditional allies. The most concerning TTPs are also little understood among States – experts have only just begun to study relevant patterns and deploy relevant frameworks. However, the lack of a specific legal regime for information operations does not mean that these exist in a legal vacuum. Quite the contrary: existing international law, as a whole, continues to apply to information operations, just as it applies to other online phenomena, to the extent relevant.[69] Of course, not all rules of international law are relevant to information operations or the online information space for that matter. However, general rules and principles as well as specific legal frameworks do apply and have something to say about it. The purpose of this section is to tease out these key rules, principles and regimes that are most significant to the international regulation of FIMI and other information operations, whether carried out by States or non-State actors.

II.1 SOVEREIGNTY

The first and perhaps more general rule to constrain FIMI and other information operations is sovereignty.[70] Also known as sovereign equality, this is the foundation of the international legal order.[71] As noted earlier, States are the primary subjects of international law – they make, apply, and enforce international law. These 'external' sovereign powers are equal among States, in that each State is an independent political unit in its international relations with other States.[72] International law requires the consent of the States that it binds (though consent can be manifested in different ways, including implicitly and explicitly, by practice or verbal acts). At the same time, States must each respect each other's sovereignty as well as the obligations to which they are bound.[73] Thus, sovereign freedom is not unfettered and subject to international law. States also have internal sovereign powers in their territories, over their property and populations.[74] This means they can exercise governmental powers over those, to the exclusion of other States.[75] Sovereignty concerns the relationships between States: it is chiefly about the rights and obligations that States have vis-à-vis one another.[76]

In the online context, including cyberspace and the digital information environment, sovereignty means that States have powers over the various components or layers of ICTs, namely, hardware, software, data, and the persons who use or operate them.[77] However, there is controversy over whether and to what extent digitally enabled operations, including information operations, can breach sovereignty.[78] One view, endorsed by the United Kingdom,[79] is that sovereignty is simply a principle underlying or informing other rules of international law, as opposed to a self-standing binding rule itself.[80] On this view, cyber operations carried out by one State cannot breach another State's sovereignty. In another view, a State's sovereignty may be breached not only by the physical effects of a cyber operation[81] but also by any conduct that, even if remote, causes functional harm to cyber infrastructure located therein or interferes with the victim State's inherently governmental functions.[82] This view has been endorsed by a majority of experts[83] and by most States that have expressed their views on the topic so far – including several EU member States and Canada.[84] This is the preferred view; not only is it in line with what sovereignty stands for (the protection of a State's independence) but also follows the development of new technologies and their use for malicious purposes.

For present purposes, this all means that information operations carried out by a State that foreseeably cause physical or functional effects on the territory of another State or that otherwise undermine a State's inherently governmental functions will violate the rule of sovereignty under international law.[85] Examples of physical effects that may be caused by FIMI include serious disinformation campaigns leading to the death of individuals (such as false advertisements about deadly medical treatments), environmental harm (such as the manipulation of information relating to the disposal of waste), domestic violence (such as propaganda or hate speech playing to existing racial, ethnical or religious tensions), or even war (such as war propaganda or false news about military activity or the manufacture of nuclear,

biological or chemical weapons). Inherently governmental functions are services that can only be performed by a State's government, such as elections, social services, tax collection, national defence and foreign affairs.[86] Examples of FIMI interfering with or usurping these functions are those meddling with democratic processes (such as electoral mis- or disinformation) or affecting the external relationships between two States (such as false accusations about trade or political measures or the disclosure of confidential information pertaining to those relationships).

II.2 NON-INTERVENTION

The principle of non-intervention or the prohibition of interference in another State's internal or external affairs is a corollary of sovereign equality, so the two principles are closely connected. However, non-intervention is narrower in important ways and broader in others. First, unlike sovereignty, non-intervention only covers coercive forms of interference in another State's affairs. In the words of the International Court of Justice (ICJ), the principle:

> forbids all States or groups of States to intervene *directly* or *indirectly* in internal or external affairs of other States. […] Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the *indirect* form of support for subversive or terrorist armed activities within another State.[87]

Coercion is about constraining the choices available to another State.[88] It is about lack of consent, about forcing a State to take a course of action that it would not otherwise have taken.[89] Thus, as the ICJ noted, it includes not only the use of kinetic, military force but also indirect forms of coercion, such as support for subversive activities of non-State actors in another State. More importantly for our purposes, indirect coercion also includes the use of information to subvert the domestic order of another State or otherwise constrain a State's choices with regards to its internal or external affairs.[90] After all, according to the UN General Assembly, the right to non-intervention also includes '[t]he right of States and peoples to have free access to information and to develop fully, without interference, their system of information and mass media and to use their information media in order promote their political, social, economic and cultural interests and aspirations'.[91]

Examples of FIMI and/or information operations that may violate this right include i) 'the *promotion, encouragement or support,* direct or indirect, of rebellious or secessionist activities within other States, under any pretext whatsoever, or any action which seeks to disrupt the unity or to undermine or subvert the political order of other States'; ii) 'any *defamatory campaign, vilification or hostile propaganda* for the purpose of intervening or interfering in the internal affairs of other States'; and iii) *'the exploitation and the distortion* of human rights issues as a means of interference in the internal affairs of States, of exerting pressure on another States or creating distrust and disorder within and among States o groups of States'.[92] Thus, propaganda, the use of hateful rhetoric, mis- or disinformation campaigns and other forms of information manipulation, as well as malformation, if carried out by States or non-State actors with the support of States, and, by their coercive aims, methods or effects, constrain a State's freedom to decide the course of its internal or external affairs, will breach the principle of non-intervention under international law.

That a prohibited intervention must bear on a State's internal or external affairs broadens the scope of this principle in comparison to sovereignty (which covers only inherently governmental functions). A State's internal or external affairs, also known as its *'domaine reservé'*, encompasses all 'matters in which each State is permitted, by the principle of State sovereignty to decide freely.[93] One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy'.[94] It does not matter whether these are carried out by public or private entities.[95] There is debate on whether the protected scope of a State's internal or external affairs shrinks over time with a State's undertaking of new international obligations.[96] However, the better view is that the scope or list of State powers or functions protected by the principle of non-intervention does not change in this way.[97] Even when a State accepts to be bound by international law, it retains a significant margin of discretion in implementing its international obligations.[98] More importantly, agreement to be bound by international law does not, without more, invite other States to interfere in the matter covered by the rule. As discussed below, responses to breaches of international law, seeking to induce States back into compliance, are regulated by an entire host of rules on the responsibility of States for internationally wrongful acts.[99]

Thus, FIMI activities that are coercive in nature, (i.e., which deploy objectively coercive means, intend to coerce or result in coercion, including by deception), and affect a State's ability to govern its internal or external policies, including

in the political, economic, social and cultural sectors, will breach the principle of non-intervention. Though this can only be assessed on a case-by-case basis, examples may range from health, electoral, and climate-related disinformation to manipulative propaganda campaigns, doxing or information blackmail and hate speech spreading lies or manipulating information about politicians and public figures in another country.

II.3 DUE DILIGENCE

As a concept, due diligence is about taking care or behaving responsibly to avoid causing harm to others.[100] In international law, there is debate about the status of due diligence.[101] Some argue it is a general principle applicable across the board to all sorts of State activity.[102] Others say only specific areas or regimes of international law provide for obligations of due diligence, such as international environmental law, international investment law, law of the sea, and the Genocide Convention. As such, an argument has been made that, in the absence of a cyber-specific obligation of due diligence, States would not be required to behave responsibly in the ICT environment.[103] As noted elsewhere, the better view is that due diligence is a standard of conduct against which the behaviour of States can be judged.[104] This standard is found in a patchwork of binding rules and principles of international law, of general and specific application to the conduct of States.[105] None of these rules is technology-specific. Thus, they apply to ICTs and information operations to the extent relevant.[106]

Though different, due diligence obligations tend to require a certain course of conduct, as opposed to a particular result. In other words, States are required to exercise their best efforts to avoid certain harmful outcomes rather than successfully prevent them. They can be held responsible for failing *to try* to prevent harms caused by their own agents and other actors, including third States and non-State actors. However, foreseeability of potential harms is usually required, and so is some degree of control or influence over the perpetrator or events. Though no direct causal link between the omission and the harmful result is required, as a general rule, responsibility for failure to exercise due diligence only arises when the event materialises (the exception being human rights obligations, discussed below).[107] As a best-efforts standard, due diligence is also subject to a State's capacity to act in the circumstances. Since different States (especially developed and developing countries) have different economic, technological and human resources, due diligence is flexible: it gives effect to the principle of common but differentiated responsibilities.

The most general rule requiring due diligence is the so-called Corfu Channel principle, which derives its name from an ICJ case between the UK and Albania.[108] In that case, the Court found that it is a 'well-recognized principle of international law' that 'every State [has an] obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.'[109] This covers the use of ICTs, including information, by States or non-State actors to undermine the rights of another State, including its rights to sovereignty and non-interference, discussed earlier. Thus, a State might violate the Corfu Channel principle if it fails to take action to prevent unlawful forms of FIMI and other information operations carried out from its territory or infrastructure by other States or non-State actors.[110] Note that this does not require the information operation to be foreign or cross-boundary, so long as it undermines the rights of another State. As seen earlier, examples of information operations that undermine State rights are those that interfere with another State's inherently governmental functions or curtail another State's freedom to determine its internal or external affairs.

A related obligation of due diligence is known as the no-harm or good neighbourliness principle. This principle requires States to take 'all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof',[111] where harm includes damage to the territory, persons, or property of another State.[112] This obligation applies irrespective of the lawfulness of the activity that caused the transboundary harm in question. While it is uncontroversial that this obligation goes beyond ecological or environmental damage to cover all types of transboundary *physical* harm, it is unclear whether it includes non-physical harms. The better view is that it does.[113] This is justified both by the history of the principle – which included, from the outset, moral or reputational damage to persons – as well as subsequent technological developments, particularly the creation of the radio and other means of communication capable of remotely causing cross-boundary harm in new ways. This means that this duty applies neatly to a variety of FIMI activities. It requires States to take all reasonable measures to prevent foreseeable harms or mitigate the risks arising from FIMI activities carried out from their territories or jurisdiction against the persons, territory or property of other States. Failure to do so may give rise to liability to pay compensation for the harm caused, and failing that, international responsibility for wrongful conduct.

Relatedly, the 1936 Convention concerning the Use of Broadcasting in the Cause of Peace,[114] in Articles 1 to 5, provides its own due diligence obligations with respect to

certain forms of propaganda, incitement and information manipulation. Specifically, the Convention requires its States parties to prohibit or stop without delay any transmission from their territories that i) incites civil strife in another State; ii) constitutes propaganda for war against another State; iii) disseminates foreseeably false information 'likely to harm good international understanding; iv) to verify, especially in time of crisis, the accuracy of information concerning international relations; and v) and to provide to other parties, at their request, accurate information that can be conducive to good relations or peace. Though only 29 States are still parties to this convention,[115] its provisions arguably reflect the application of more general due diligence obligations in the international broadcasting context, including today's digital information environment.[116] Indeed, a similar provision requiring states to refrain from and prevent interference in other States' radio services is found in Articles 6 and 45 of the 1992 Constitution of the International Telecommunication Union,[117] whose membership includes 193 States.[118]

Due diligence obligations are also found in international human rights law.[119] International human rights law is found in human rights treaties, including universal and regional, as well as customary international law. The rights recognised in the Universal Declaration of Human Rights[120] and the International Covenant on Civil and Political Rights (ICCPR)[121] – known collectively as the International Bill of Rights[122] – are, for the most part, found in international custom, and, as such, binding on all States.[123] The European Convention on Human Rights (ECHR),[124] adopted by the Council of Europe in 1950 and effective since 1953, binds all EU member States as well as other members of the Council. It reflects, to a large extent, the ICCPR, with some variations in its scope of protection (e.g., the extent of its jurisdiction and the contours of some rights). EU member States are also bound by the Charter of Fundamental Rights of the European Union,[125] which contains additional rights, such as the right to property. The American Convention on Human Rights (ACHR) has been adopted in the context of the Organization of American States (OAS).[126] It has been praised as a protective and effective human rights treaty, especially in the light of the jurisprudence of the Inter-American Court of Human Rights. While Canada is a member of the OAS, it has not ratified the ACHR.[127]

The ICCPR, ECHR and ACHR recognise a significant number of civil and political rights. These are complemented by the International Covenant on Social, Economic and Cultural Rights.[128] Every human right gives rise to negative obligations to respect its enjoyment by individuals and other rights-holders, as well as positive obligations to protect and ensure the fulfilment of those rights.[129] Obligations to protect and ensure human rights are obligations of due diligence.[130] They require States to take all reasonable measures to prevent or mitigate foreseeable risks to the enjoyment of human rights caused by a State's own agents, other States, non-State actors or natural events.[131] States must also remedy any damage resulting from interference with those rights and employ all available resources to ensure that individuals have the conditions to enjoy them in the best possible way.[132]

Several human rights are relevant to FIMI and other information operations, including, most notably, the freedoms of expression and information and the rights to freedom of assembly, privacy, and non-discrimination. Insofar as foreign or domestic information operations interfere with the enjoyment of these and other human rights and fall within a State's jurisdiction – to be discussed in the next section – States have a due diligence obligation to exercise their best efforts to prevent, stop or redress them, as far as possible.

II.4. INTERNATIONAL HUMAN RIGHTS LAW

International human rights law binds States via treaties and customary international law, and it applies online just as it does offline.[133] Private entities, including individuals and corporations, are not yet bound by this body of law.[134] Nonetheless, corporations have non-binding human rights responsibilities or social expectations to respect the human rights of those affected by them, such as by mitigating their human rights impact, including online.[135] Individuals also have international criminal responsibility if they affect human rights to the point of committing an international crime – genocide, crimes against humanity, war crimes, or the crime of aggression.[136] At any rate, international human rights law provides a universal language that can guide the behaviour of not only States but also companies and civil society online.[137]

A preliminary question which determines whether a State has human rights obligations is the extent of its jurisdiction. In the human rights context, jurisdiction refers to the scope of application of a State's negative and positive obligations.[138] Under certain human rights treaties, including the ICCPR and the ECHR,[139] a State only has human rights obligations within a certain jurisdictional scope, which could be its territory, a geographical location, the sphere of control over one or more persons, or, more broadly, over the enjoyment of human rights. The meaning of jurisdiction varies according to the treaty and monitoring body or court at hand. While the

ICCPR's Human Rights Committee[140] and the Inter-American Court of Human Rights[141] follow a broad approach (defining jurisdiction as control over the enjoyment of rights),[142] the European Court of Human Rights only goes so far as accepting that ECHR obligations apply when a State has *physical* control over a person.[143] This restrictive view leaves out from the ECHR's protective scope several human rights violations carried out by remote means, including online, such as foreign electronic surveillance and information operations.[144] However, among EU Member States, Germany has followed a broader approach to human rights jurisdiction, including within its scope any remote interference with human rights.[145] This approach is welcome and other EU Member States should follow suit.

The ICCPR has two provisions of direct relevance to information operations. In Article 20, it provides that:

1. Any propaganda for war shall be prohibited by law.

2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.

No State has questioned the importance of the rights, interests and values protected by this provision, which was formulated as a response to the horrors of the Second World War, especially the Holocaust.[146] However, some States parties to the ICCPR, including the US, UK and a few EU Member States (Belgium, Denmark, France, Ireland, Luxemburg, the Netherlands, Malta, and Sweden)[147] have reserved the right to enact the laws envisioned in Article 20, for reasons relating the protection of freedom of expression domestically.[148] However, the core duties underlying this provision – the prohibition on the use of force and to incite to war,[149] the positive obligation to protect the right to life[150] and the positive duty to protect individuals against any incitement to discrimination,[151] are undeniably part of customary international law.[152] Thus, States must refrain from information operations that amount to propaganda for aggressive war (including any unlawful use of force) or incitement to discrimination, hostility or violence on the basis of race, religion or nationality. They must also exercise due diligence to protect individuals from the consequences of those acts, whether by domestic prohibitions or other means at their disposal.[153]

Another key human right when it comes to FIMI and other information operations is the composite right to seek, receive and impart information freely – also known as the freedoms of information and expression. In accordance with Article 19 of the ICCPR:

Everyone shall have the right to freedom of expression; this right shall include freedom to *seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*[154]

Thus, there is no question that rights to freedom of expression and information apply online as they apply offline.[155] As information knows no boundaries, this right also applies across national borders, challenging restrictive approaches to human rights jurisdiction.[156] Importantly, all kinds of information or ideas are protected, including false ones.[157] Thus, as a matter of principle, individuals and other rights-holders (e.g., corporations under the ECHR) are entitled to spread lies or otherwise manipulate information domestically or internationally.

However, the rights to freedom of expression and information are not unfettered. In paragraph 3 of Article 19, the ICCPR provides that:

3. The exercise of the rights provided for in paragraph 2 of this article carries with it *special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*

   a. *For respect of the rights or reputations of others;*

   b. *For the protection of national security or of public order (ordre public), or of public health or morals.*[158]

This means that one's right to express their views online or offline, be them true or false, must be balanced against the rights of others in society to seek, receive and impart accurate information, as well as other human rights and public interests.[159]

Like all rights, the rights to freedom of expression and information give rise to negative obligations of restraint and positive State obligations of protection.[160] Thus, States must not only respect one's rights to seek, receive or impart information but also protect them against unlawful interference. This means that States must refrain from spreading false information themselves whilst promoting accurate information.[161] They must also ensure a plural, independent and robust media and information environment, favourable to public debate and critique,[162] as well as access to diverse content and media, including by preventing media concentration.[163] To fulfil this duty, FIMI and other information operations may only be limited in line with the conditions listed in Article 19(3) ICCPR and similar human rights provisions.

The same goes for the protection of other private rights or public interests threatened by FIMI and information operations more generally. States may well be entitled to protect their public interests and societal values (such as democracy and national security). They also have obligations to protect several rights affected by information operations, such as the rights to life, health, participation in democratic processes, and privacy. However, when limiting information operations to uphold these values, interests or rights, they must observe the conditions laid down in international human rights law for limiting the freedoms of expression and information, reflected in Article 19(3) ICCPR.[164] This is because, as noted earlier, information operations are speech acts and, as such, in principle protected by the rights to freedom of expression and information.

The conditions for limiting information operations and other speech acts have been referred to as the tripartite test of i) legality, ii) legitimacy, as well as iii) necessity and proportionality.[165] Legality refers to the requirement that any limitations on speech acts are provided by sufficiently foreseeable and accessible laws (written or unwritten, but democratically enacted) and subject to judicial review. In the digital information environment, this usually requires the enactment of a basic legal framework laying out which types of FIMI and other information operations may be prohibited or otherwise limited by States or online platforms, and which measures may be adopted to limit them (e.g., criminal or civil sanctions or content moderation measures).[166] Legitimacy means that such limitations must meet a legitimate aim or ground, which usually corresponds to the protection of another human right or a public policy interest, listed in the relevant human rights instrument.[167] Necessity means that limitations must employ the least speech-restrictive means available to achieve the legitimate aim in question.[168] Proportionality means that the limitation on speech must be well-calibrated to the seriousness of the speech act and the importance of the legitimate goal in question.[169] The implication is that criminal sanctions should be reserved for only very serious speech acts, such as incitement to violence, not information manipulation.[170] Less serious measures, such as civil liability, content takedowns, user suspension or content de-prioritisation, should be deployed to tackle information operations.

Of note, in 2017, the Special Rapporteurs on freedom of expression of various organisations and human rights bodies – the UN, the Organization for Security and Co-operation in Europe (OSCE), the OAS, and the African Commission on Human and Peoples' Rights (ACHPR) – adopted a 'Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda'.[171] This is an extremely relevant document when considering the international legal framework applicable to FIMI. It fleshes out how international human rights law applies not only to State conduct in this context (including negative and positive obligations) but also how different private entities (including online platforms, journalists and media outlets) should incorporate human rights principles in their policies. Importantly, the declaration covers not only the substance of State obligations and stakeholder responsibilities when it comes to tackling key types of information operations (such as which types of propaganda and disinformation are prohibited, and which ones are not). It also lays out fundamental procedural safeguards in the fight against those operations, such as the need for clear legal or regulatory frameworks to protect media diversity, digital and media literacy campaigns, clear platform content policies, fact-checking, user appeal mechanisms against content moderation decisions, recognition of the right of correction, and the need for multistakeholder engagement and cooperation to address the problem.[172]

II.5 INTERNATIONAL HUMANITARIAN LAW

International humanitarian law (IHL) applies during armed conflict – international or non-international.[173] It is mostly concerned with the protection of civilians and other persons hors de combat from the effects of such conflicts, as well as combatants from unnecessary suffering on the battlefield.[174] As such, most of its rules and principles apply to kinetic, physical military operations. They also apply to cyber operations that amount to an armed attack.[175] Some provisions of IHL are also relevant to FIMI and information operations.[176] The first is the obligation to ensure respect for IHL.[177] This obligation applies to all States, in peacetime and during armed conflict. It requires States to refrain from and actively prevent the dissemination of any information – true or false – that promotes IHL violations IHL. States and non-State actors that are parties must also refrain from terrorising civilians, including through FIMI and other information operations.[178] They must also refrain from using information manipulation and other information-based techniques to disrupt the work of medical, religious, or humanitarian personnel.[179] In the context of a military operation, they must exercise precautions to spare civilians and civilian objects from the effects of information operations, including data-gathering and information manipulation, such as false flag operations.[180] If States or non-State actors have taken prisoners of war, they must protect their honour from public curiosity, including information operations that might reveal their identities or portray their conditions, save in exceptional circumstances to protect their own life or obtain evidence of war crimes.[181]

II.6 STATE RESPONSIBILITY AND COUNTERMEASURES

If a State engages in FIMI or another information operation or fails to prevent, mitigate or remedy such an operation in a way that breaches international law, it will be held responsible for an internationally wrongful act under the international rules of State responsibility.[182] These rules apply to all States under customary international law[183] and are mostly reflected in the International Law Commission's Articles on State Responsibility for Internationally Wrongful Acts.[184] The main consequence of engaging in an internationally wrongful act – whether by action or omission – is that new obligations arise for that State seeking to bring it back into compliance with international law.[185] These are the obligations to stop the wrongful act (or cessation), to make reparation for it (either by providing restitution, compensation or satisfaction) and, if necessary, to provide just satisfaction and guarantees of non-repetition.[186] Moreover, the breach of a rule of international law entitles States directly injured by the breach to respond to the wrongful act by taking countermeasures to induce or secure compliance with international law.[187] Though the issue is controversial,[188] third States may also be able to take countermeasures in response to unlawful acts, provided that the injured State so requests or the violation in question is a serious breach of an obligation protecting the interests of the international community as a whole, such as the prohibition on the use of force or genocide.[189]

Countermeasures are the suspension of performance of one or more obligations owed to the wrongdoing State.[190] They may be taken in kind (where the injured State suspends the performance of the same obligation breached) or unrelated to the original breach (where a different obligation is suspended to prompt the wrongdoing State to stop or repair the violation). Countermeasures must not be punitive but seek to procure the wrongdoing State to comply with the obligations of cessation and reparation.[191] They must be proportionate or commensurate to the original breach and are subject to a number of substantive and procedural conditions that seek to limit abuse.[192] Importantly for present purposes, countermeasures must be targeted at the wrongdoing State (i.e., the rights that the injured State owes to it) and must not affect fundamental human rights. This means that when States respond to unlawful information operations, in kind or not, they must not violate the rights of individuals or private entities to the freedoms of information and expression.[193] Likewise, any indirect effects on these and other rights must be limited as far as possible.[194] Accordingly, States must not engage in FIMI or other unlawful information operations, such as war propaganda or incitement to violence, in response to these types of acts.[195] They may, however, engage in cyber operations seeking to deactivate the computer system from which the unlawful information operation originates – a measure often referred to as 'hack back' or active cyber defence.[196] This is true provided that the other conditions for taking countermeasures are respected, including having previously made representations (which may be general in nature) to the wrongdoing State that it has breached international law and making sure that any limitations on the freedoms of expression and information and other human rights are lawful.

PART III – INTERNATIONAL NORMS AND NORM-SETTING PROCESSES FOR CYBER OPERATIONS AND INTERNET GOVERNANCE

As noted in the introduction, several non-binding norms have been developed over the past decade in the field of ICT security, focussing on cyber operations, as well as internet governance. Though these do not directly address FIMI or information operations more generally, both the substance of these norms and the processes that have led to them can serve as inspiration for the development of international norms for FIMI. In what follows, this section will first unpack the 11 norms of responsible State behaviour in the ICT environment, developed by the UN GGE[197] and picked up by the OEWG,[198] noting how they were developed and what they have achieved so far. Secondly, it will provide an overview of two influential academic-led processes for the interpretation of international law in cyberspace, as well as their outcomes, namely the Tallinn Process and Manual,[199] and the Oxford Process and Statements.[200] The section will then turn to some relevant aspects of the draft UN Cybercrime Convention.[201] It will finish with a brief analysis of the norms on internet governance in the course of development under the guise of the UN GDC[202] and the GNI.[203] The focus will be on the strengths and pitfalls of each set of norms and processes.

III.1 THE NORMS OF RESPONSIBLE STATE BEHAVIOUR IN THE ICT ENVIRONMENT

Inspired by its work on fleshing out the principle of non-intervention,[204] and confidence-building measures in the context of nuclear deterrence,[205] and prompted by a concern that evolving technologies could be used for malicious purposes,[206] the UN General Assembly started to look into the topic of 'Developments in the field of information and telecommunications in the context of international security' in 1998.[207] On the UN General Assembly's agenda since 2001,[208] the UN GGE was formally established by the Assembly in 2004 to assist the UN Secretary-General 'to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them', and to conduct a study on 'relevant international concepts aimed at strengthening the security of global information and telecommunications systems'.[209] Its mandate was then refined to cover

> '[the] study, with a view to promoting common understandings and effective implementation, [of] possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States.[210]

It was pursuant to that mandate that the Group adopted by consensus its 11 norms of responsible State in the security and use of ICTs in 2015.[211] According to the GGE, the norms were motivated by the need to reduce collective risk and protect critical national and international infrastructure.[212] Specifically, they seek to 'strengthen common understandings', 'increase stability and security in the global ICT environment', and 'reduce risks' thereto by preventing conflict.[213] Ultimately, the norms are meant to 'enable the full realization of ICTs to increase global social and economic development.'[214] They reflect international expectations and set standards for responsible State behaviour against which the activities and intentions of States in cyberspace can be assessed.[215] The group explicitly highlighted that the norms of responsible State behaviour are not intended to limit or prohibit action that is otherwise permitted under international law.[216] As noted elsewhere, these norms cannot derogate from existing binding obligations either.[217] After all, they are non-binding commitments and, as such, cannot formally alter binding international law.[218] International law can only be changed by new rules or principles of international law, be those treaties or international custom. The GGE's norms were subsequently acknowledged by the UN General Assembly in 2015,[219] and endorsed by various iterations of the OEWG.[220]

Now in its second iteration, set to last from 2021 to 2025, the OEWG has continued the work on the five pillars of the GGE's mandate (i.e., the study of threats, international law, norms of responsible State behaviour, capacity-building and confidence-building measures) *across the entire UN membership*.[221] The OEWG both reaffirmed the GGE's findings on international law and its 11 norms of responsible State behaviour in the ICT environment by consensus.[222] In doing so, it explicitly found that 'norms do not replace or alter States' obligations or rights under international law,

which are binding, but rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs'.[223] This clarifies an important function of the norms: not to derogate from or diminish rights or obligations binding under international law, but to interpret or flesh them out. In fact, the norms reflect, to a large extent, existing international law.[224] They do so by picking up on general rules of international law, such as the UN Charter, sovereignty, due diligence, and human rights, and applying international law to specific areas that deserve special protection or have given rise to particular concerns in the ICT environment, such as critical infrastructure, terrorist uses of ICTs, and IT supply chains. Importantly, where there was disagreement about the scope of international law applicable to ICTs, as in the case of sovereignty and due diligence, the norms have helped build consensus among States about what behaviour is considered responsible and is thus expected from them in the ICT environment.

The norms are quite detailed, and it is not the purpose of this study to rehash or delve deep into them, especially because they lack specific provisions for FIMI or information operations. However, while, as a whole, the norms were drafted with traditional cyber operations in mind, some of them do cover important aspects of information operations and their legal framework under international law. First and foremost, norm 'a' is a general reminder of States' commitment to maintain international peace and security as enshrined in the UN Charter.[225] In this spirit, it encourages them to 'cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security'.[226] As noted earlier and acknowledged by both the GGE and the OEWG themselves, FIMI and other information operations can be harmful and pose a threat to international peace and security. As such, this norm also applies to them, inviting States to cooperate to identify concrete measures, such as capacity-building, confidence-building and technical measures to counter harmful information operations.

Norm 'b' notes 'the challenges of attribution in the ICT environment', as well as 'the nature and extent of the consequences' of ICT incidents' and their broader context.[227] As information operations also take place in the ICT environment, they do not escape these challenges. Thus, when accusing other States of carrying FIMI or other harmful information operations, States should exercise care and caution, considering all relevant evidence and information.

Norm 'c' is in essence an articulation of due diligence in the ICT context.[228] It recommends States 'not [to] knowingly allow their territory to be used for internationally wrongful acts using ICTs'.[229] As noted earlier, due diligence is a standard of conduct found in several binding rules and principles of international law. However, it has been framed as a binding norm here given misunderstandings about the nature, status, and scope of this obligation under international law, as well as the reluctance of some UN member States to accept the application of certain obligations in the cyber context.[230] Nevertheless, as noted elsewhere, that due diligence has been framed as a norm of responsible State behaviour in no way denies its binding, legal force under existing international law. Thus, norm 'c' serves best as a reminder of those existing obligations and fleshes out their content in the ICT context.

Indeed, norms 'd', 'g', 'h', 'i' and 'j'[231] then spell out specific measures of due diligence that could fulfil their corresponding legal obligations and normative commitments.[232] These are: i) cooperation or assistance in the exchange of information; ii) prosecution of terrorist and criminal use of ICTs, including assisting other States to this effect; iii) protection of critical infrastructure, such as the health, energy, financial and transport sectors, from ICT threats, including by cooperating with other States and creating a 'global culture of cybersecurity'; iv) cooperation by responding to requests for assistance from States that are victims from ICT threats against their critical infrastructure, especially when those threats emanate from a State's own territory; v) protection of IT supply chains; vi) prevention of malicious ICT tools and techniques; and vi) reporting of ICT vulnerabilities and sharing associated information on available remedies. All these due diligence measures apply, with slight adaptations, to FIMI and other information operations. For example, States should prosecute the use or manipulation of FIMI for terrorist purposes, taking into account applicable rules of international law and human rights in particular. They should cooperate with other States when tackling FIMI and other harmful information operations, especially when these affect critical sectors, such as those protected by the rules of sovereignty and non-intervention. Importantly for the implementation of the DISARM and similar FIMI frameworks, they should not only prevent identified TTPs but also report and share information on them with relevant international partners. With the increasing use of AI to produce and disseminate false content, States should also ensure that AI products, especially chatbots, are not used to carry out unlawful information operations or contain hidden functions enabling these operations.

This shows that while the due diligence norm ('e') came from a place of uncertainty and controversy around the corresponding legal obligations, framing binding international law as a norm has allowed UN member States to move beyond legal disagreement and focus on the actual application and implementation of the rule, as reflected in norms 'd', 'g', 'h', 'i', and 'j'. This is the perfect example of how norms can bridge gaps in legal protection and perhaps dissuade fears and misconceptions about binding international obligations. It is hoped that by following norm 'e' and the best practices reflected in the other norms, States will either come to an agreement about the status of due diligence in international law or at the very least voluntarily behave according to it.

Relatedly, norm 'e' reminds States that their human rights obligations also apply online,[233] highlighting the right to freedom of expression. Again, though the norm is, of course, framed as a recommendation (employing the language of 'should'), it does not and cannot displace States' human rights obligations under international law. As noted above, these must be considered in the implementation of other rules of international law (such as sovereignty and due diligence) as well as the norms of responsible State behaviour. This also applies to FIMI and other information operations, which, as speech acts, are in principle protected by the rights to freedom of expression and information, as well as other human rights.

In the same vein, norm 'f' reaffirms and specifies how existing rules of international law, particularly sovereignty and non-intervention, should apply in the ICT environment and with respect to critical infrastructure.[234] It stipulates that '[a] State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public'.

The 11 norms of responsible State behaviour were adopted by State experts behind closed doors at the GGE. However, they have since been increasingly subject to scrutiny by different stakeholders, including the industry, civil society and academia. Though not without logistical challenges (such as lack of funding to attend meetings in person) or opposition from certain UN member States (particularly Russia and its allies),[235] the OEWG has been allowing those stakeholders to participate in different ways and provide input in the various meetings of the Group. For example, during substantive and intercessional meetings of the OEWG, stakeholders have been allowed to make statements in formal and informal meetings, including dedicated stakeholder sessions with the OEWG chair and open to the participation of all UN member States.[236] This allows for fruitful exchanges of ideas and interaction between Member States and the stakeholder community. Moreover, proposals by different stakeholders, such as Global Partners Digital, Access Now, Oxford University and Chatham House, have made their way into various reports adopted by the OEWG.[237] This includes the sections on ICT threats, capacity-building, and confidence-building, as well as how the norms and international law pillars should be further developed at the OEWG (for example, by receiving input from expert meetings and focusing on topics that are more prone to consensus).[238]

OEWG is yet to flesh out the meaning of international law and the norms of responsible State behaviour in the field of ICT security. Nevertheless, it has made significant progress in the development capacity and confidence-building measures. Notably, it has drafted key principles to guide the implementation of capacity-building measures among States[239] and discussed the creation of the Global Cyber Security Cooperation Portal.[240] The group has also agreed to establish important measures to build confidence among States in the ICT environment, including national points of contact and a global directory for them.[241] The same measures could help build the capacity and confidence of States in tackling FIMI and related information operations. However, in the OEWG's last meetings, there has been a noticeable division between States seeking to focus on the implementation of existing international law and norms (mostly Western States, including most Latin-American States) and others that have been pushing for a new treaty on ICT security and the development new norms (especially Russia, China, Iran and their allies in Latin America, the Middle East, Asia and Africa).[242] The future of the OEWG is uncertain: though it is set to formally conclude its current mandate in 2025, the group is expected to continue its work in the form of a permanent 'Programme of Action'.[243] However, the establishment of this group, which will also encompass the entire UN membership, depends on agreement among all member States on its mandate, including the modalities of participation and its decision-making processes, as well as the topics covered.

II.2 THE DRAFT UN CYBERCRIME CONVENTION

Also in the cyber context, the UN General Assembly set up an Ad hoc Committee to Elaborate an International Cybercrime Convention to enhance 'coordination and cooperation among States in combating the use of [ICTs] for criminal

purposes'.[244] The Zero Draft of the Convention defines several cyber-enabled offences and lays out several procedural and law enforcement measures that parties will be required to enact in their domestic legislation.[245] Though this is not a norm-setting process per se, two aspects of the drafting of the UN Cybercrime Convention are noteworthy.

First, one of the main points of contention between UN member States relates to whether or not and to what extent speech or content-based offences, including those criminalising certain forms of disinformation, should be included in the draft.[246] Following in the footsteps of the Budapest Convention,[247] the current draft contains traditional or 'core' cyber-dependent offences, which most agree should be criminalised. These involve illegal access, interception or interference with computer systems, misuse of devices, computer-related theft and forgery.[248] Also relatively uncontroversial are offences relating to child sexual abuse or child sexual exploitation.[249] However, more controversial is the criminalisation of non-consensual dissemination of intimate images,[250] currently in the Zero Draft, as well as previous proposals to include vaguely worded content-based offences, such as 'extremist-related' offences, 'incitement to subversive activities', distributing materials 'motivated by political, ideological, social, racial, ethnic or religious hatred', 'the spreading of strife, sedition, hatred or racism' and the denial of historical facts.[251] Neither the content nor the criminalisation of these offences is in line with international human rights law, discussed earlier. In particular, the criminalisation of the acts in question may not be sufficiently clear to comply with the principle of legality. It may also be an unnecessary or disproportionate response to the harm and protected interests in question.[252] Thus, the lesson here is that while information operations are a pressing threat, and looking at their content is inevitable under international human rights law, criminalisation is probably not the best remedy for them.

The second noteworthy feature of the UN Draft Cybercrime Convention is the engagement of different stakeholders in the drafting process. Like at the OEWG, all interested stakeholders may make written submissions to the Ad Hoc Committee, whereas approved organisations (i.e., those not vetoed by a member State) can join the Committee's sessions.[253] The Chair of the Committee also holds regular inter-sessional consultations to gather input from different stakeholders on the elaboration of the draft convention.[254] The engagement of stakeholders has been described as essential in the context of a convention to safeguard individuals from malicious uses of primarily privately owned technology.[255] The contributions so far have been extremely detailed and comprehensive, and have been embraced by different member States.[256] However, it remains to be seen whether the idea of criminalising speech acts will be abandoned and whether the input of stakeholders will meaningfully shape the final draft. At the time of writing, UN members were holding article-to-article negotiations to try to reach consensus on the Zero Draft, with the final draft scheduled for adoption in January 2024.[257] If they cannot achieve consensus, the Draft will be open to a vote.

III.3 THE NORMS FOR INTERNET GOVERNANCE

As noted earlier, there are two principal norm-setting processes in the field of internet governance: the UN GDC and the GNI.[258] The GDC was set up by the UN Secretary-General as a multistakeholder process.[259] In fact, one of the Compact's stated purposes is to advance multistakeholder cooperation to achieve an open, free, secure and human-centred digital future.[260] The idea is to leverage the experiences and expertise of different groups to develop shared principles and objectives, as well as identify concrete actions for their implementation.[261] This will lead to a global framework for internet governance (reflected in the Compact itself) and facilitate new governance arrangements.[262] In practical terms, this means that the Compact will be initiated and led by member States (with Rwanda and Sweden appointed as co-facilitators of the intergovernmental process)[263] but will benefit from the full participation of other stakeholders throughout (digital platforms, private sector actors, digital technology-focused coalitions and civil society organizations).[264] Stakeholders are also charged with the implementation of the GDC, and commitment to doing so is a condition of their participation in the process.[265] The UN Secretary-General has proposed to do so via an annual Digital Cooperation Forum to review the GDC through a transparent and action-focussed multistakeholder dialogue and information-sharing process.[266]

At the time of writing, the GDC process is yet to yield any substantive outcomes – an 'Issues Paper' is set to be produced in August 2023, and presented in September 2023, with negotiations taking place up until the Summit of the Future in September 2024.[267] Nevertheless, the UN Secretary-General has made some suggestions both on the substance of what the Compact should cover and the process of its adoption and implementation. Notably, FIMI and other information operations are covered in the section on 'Digital Trust and Safety'.[268] In this regard, the Secretary-General recognises the importance of strengthening 'cooperation across governments, industry, experts and civil society to elaborate and implement norms,

guidelines and principles relating to the responsible use of digital technologies', including industry codes of conduct.[269] Likewise, these norms should be accompanied by 'robust accountability criteria and standards for digital platforms and users to address disinformation, hate speech and other harmful online content'.[270] To this end, the Secretary-General calls on States to 'build capacity and expand the global cybersecurity workforce and develop trust labels and certification schemes as well as effective regional and national oversight bodies'.[271] A gendered perspective is recognised as key in technology design, with zero tolerance for gender-based violence.[272] To achieve those aims, the UN Secretary-General proposes cooperation among 'online safety commissioners from different jurisdictions', online platform co-regulation mechanisms, such as social media councils, and multistakeholder alliances to track patterns of harm.[273]

From a procedural perspective, the GDC process is also interesting because it has been set up by the UN Secretary-General and is thus more distanced from the politics of the UN General Assembly and Security Council. The GDC has also been living up to its promise of multistakeholderism: submissions are open to everyone, and anyone can join the GDC deep-dive sessions, which have been held online. It remains to be seen what States and stakeholders will agree to – if anything at all –, and if the proposed multistakeholder model will actually work, with so many participants and ideas to manage. Nevertheless, the proposals made by the UN Secretary-General seem promising and may be useful in tackling harmful information operations on a global, regional and national scale.

For its part, the GNI is a multistakeholder platform that has been put in place by ICT companies, human rights and press freedom organisations, academics, and investors to respond to some of the key challenges in the context of internet governance.[274] Because it does not involve State participation, it is less relevant to the present study. However, the GNI is remarkable for its focus on the protection of freedom of expression and privacy online. Thus, the GNI principles follow on from those rights.[275] Likewise, the GNI tackles issues that directly involve said rights, namely, network disruption, intermediary liability and content regulation, surveillance, jurisdiction assertions and limits.[276] However, misinformation, disinformation and other information operations have been addressed as part of content regulation issues, on the GNI has issued various policy briefs.[277] The GNI principles are complemented by detailed implementation guidelines,[278] which provide important procedural recommendations on how ICT companies, especially online platforms, should incorporate human rights in their decision-making processes, such as by undertaking human rights assessments. As seen earlier, human rights not only impose substantive limits on information operations and the measures seeking to counter them but also important procedural safeguards, such as the principles of legality, necessity and proportionality.

III.4 THE TALLINN AND OXFORD PROCESSES

The Tallinn and Oxford Processes are two of the most prominent academic-led processes that seek to clarify how existing international law applies to ICTs or cyberspace.[279] Both were explicitly cited in Costa Rica's recent national position on international law in cyberspace[280] and, behind the scenes, have informed and influenced many more national positions and statements on the topic. Though the focus of both processes has been on the international law applicable to cyber operations, specific interpretations or articulations of general rules and principles have been proposed for the ICT context. These articulations have included standards of behaviour and best practices for the implementation of international law that are not binding per se – after all, neither process has been led or adopted by States.

Spearheaded and led by Professor Michael Schmitt, a prominent academic in the field of international law and cyber operations, the Tallinn Process has been hosted by the North Atlantic Treaty Organization (NATO)'s Cooperative Cyber Defence Centre of Excellence (CCDCOE) since 2009.[281] It was inspired by past initiatives that sought to clarify how international law applied to topical issues of the day, such as the 1880 Oxford Manual on the Laws of War on Land and the 1994 San Remo Manual on International Law Applicable to Armed Conflict at Sea.[282] Like these, the outcomes of the Tallinn Process – the two Tallinn Manuals on International Law Applicable to Cyber Operations – have become hugely influential resources for practitioners and academics working in the field.[283] A third Manual is forthcoming.[284] Both existing Manuals were drafted by a group of independent international law experts, including practitioners and scholars, in their independent capacity.[285] Representatives of 50 States did take part as observers in the drafting process of Tallinn Manual 2.0, though the Manual is not representative of their views.[286] The Manuals are made up of 'rules' which are meant to reflect existing international law as applicable to cyber operations.[287] While the rules were adopted by consensus among the experts, a detailed commentary fleshes out the content of the rule and explains its background, including an overview of legal controversies on the matter between the experts and among States.[288]

As comprehensive law books aimed at providing an accurate picture of how international law applies in cyberspace, the Manuals are not the best model for a norm-setting process in the context of FIMI or other information operations. In particular, their focus is on how various rules and principles apply to cyber operations in general, as opposed to particular types of operations or factual phenomena like FIMI. The Manuals have also been criticised for being too Western in their perspective and the composition of the expert groups.[289] However, their drafting process is interesting in its segmented or compartmentalised way: different experts led the drafting of different parts, based on their areas of expertise.[290] Most importantly, drafting the rules themselves in general terms allowed experts to agree on their content, leaving disagreements to be flagged in the commentaries on the rules.

The Oxford Process was similarly driven by leading academics from different universities – primarily Professors Dapo Akande (Oxford University), Harold Koh (Yale University), and Duncan Hollis (Temple University).[291] It started during the COVID-19 pandemic as an attempt to find consensus on the legal protection of particularly important objects or sectors that had been the target of recurring and crippling cyber operations in a moment of extreme vulnerability, such as the healthcare sector and vaccine research efforts.[292] It then expanded into other areas or types of operations that were particularly serious or concerning, such as cyber-enabled electoral interference, information operations, ransomware, and IT supply chain attacks.[293] For each of these topics, the Process kicked off with scoping and agenda-setting internal team meetings. Research and background papers were prepared by members of the team or commissioned to relevant experts. Then workshops were held to dive deeper into the issues and try to find common ground on how international law applies to the issue at hand.[294]

To avoid legal controversies and garner consensus on the law and best practices, emphasis was placed not on which legal rules or principles applied, but on which State behaviour was prohibited, limited, or required by them.[295] Thus, following each workshop and a careful drafting process involving the team members with input from external experts, Statements were prepared, if agreement was forthcoming on the issue discussed.[296] These lay down in some detail how States must behave to protect a certain object or tackle a certain type of operation in accordance with existing international law.[297] Legal interpretations, standards of behaviour and best practices were proposed in each Statement. Statements were then open for signature by international law experts, including academics and practitioners, among which many current and former government lawyers or advisors.[298] Five Statements in total were adopted.[299] Each has over 100 signatories from all regions of the world.[300]

The main value of the Oxford Process lies in its consensus outlook: the aim was always to find agreement, or at the very least the minimum common denominator between experts from different backgrounds and eventually States. This goal led to a conduct-based approach to articulating how international law applies to ICTs. In light of this goal, and the context against which it took place, the Process also focussed on specific phenomena – including the whole range of ICT threats or risks to critical sectors or objects (healthcare, vaccine research and electoral processes), particularly concerning types or methods of ICT-based operations (information operations, ransomware, and IT supply chain attacks), or especially divisive issues (countermeasures).[301] Not all of these topics were prone to consensus, which is why not all of them were covered by a particular Statement. One Statement is of particular relevance to this study: The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities.[302] Aside from recognising that international law applies to information operations, the Statement gathered agreement among 121 international lawyers[303] around how the various rules and principles discussed earlier – sovereignty, non-intervention, due diligence, human rights and IHL – as well as certain rules of international criminal law, apply to such operations.[304] In particular, the Statement recognised that war propaganda for war and any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence are prohibited under international law.[305] It also recognises that States must protect individuals from information operations that interfere with their human rights, such as life and health, whilst respecting the right to freedom of expression and other rights guaranteed under international law.[306] The Statement also concludes that certain information operations may amount to international crimes, such as genocide, including direct and public incitement thereto, war crimes and crimes against humanity, where the elements of those crimes are fulfilled.[307]

PART IV - CONCLUSIONS AND RECOMMENDATIONS

`This section draws on the previous sections to reach conclusions and make recommendations on a) the possible substance of international norms for FIMI, as well as b) their appropriate drafting and negotiating process. To do so, it will bring together key insights from the analysis of international law applicable to information operation and lessons learned from existing norm-setting processes, particularly the UN GGE and OEWG.

IV.1 THE SUBSTANCE OF NORMS

As noted throughout this study, the content of the messages conveyed by FIMI activities and other information operations lies at the centre of the applicable international legal framework. Under all international rules and principles discussed earlier, the foreseen harms or risks arising from these operations, including the issues, persons, and interests they affect, are key considerations. Thus, whether a specific FIMI activity is prohibited, limited, or permitted under international law will depend, in large part, on its content.

Likewise, who is behind and who is affected by these activities will dictate which international rules and principles apply. On the one hand, sovereignty only applies if the FIMI activity in question can be attributed to a State actor and undermines the inherently governmental functions of another State. Similarly, non-intervention only applies when a State actively engages in or provides support to a FIMI activity that affects the rights of other States. On the other hand, due diligence obligations cover State failure to take action against FIMI carried out by *any* actor against the rights of other States, individuals, or the environment. Notably, certain due diligence obligations are particularly relevant for the regulation of FIMI because they cover both unlawful and lawful but harmful conduct in an international setting. As seen earlier, this is the case of the no-harm principle, which applies to significant transboundary harm to persons, property or the environment, including by digital means. For its part, international human rights law requires States to refrain from certain types of FIMI – including both lawful and unlawful speech acts –, as well as to actively protect individuals against them. Corporations are also encouraged to adopt a similar course of conduct. IHL binds all parties involved in armed conflict – including States and non-State armed groups.

That is not to say that the methods or techniques employed in FIMI activities are irrelevant. Quite the contrary. Non-intervention is only breached by FIMI activities that are coercive in their aims, expected results or methods. Similarly, under international human rights law, particularly the freedoms of expression and information, assessing whether limits to FIMI activities are necessary and proportionate depends on the analysis of their methods and context. For example, the more deceptive, planned and widespread an operation is, the more stringent the measures needed to counter it. Relevant criteria include the severity of the content itself, the means of dissemination (such as the type of online platform, its reach, the role of recommendation and ranking algorithms, and the use of bots), the speaker (including their intentions and prominence), the audience (including its volume and vulnerability), and the local context. All these need to be factored in before restrictive measures to counter FIMI activities are taken.

FIMI norms may be divided into three key pillars, focussing on three categories of FIMI that are regulated differently under international law: i) lawful but harmful; ii) potentially unlawful, depending on the circumstances; and iii) clearly or manifestly unlawful. The freedoms of expression and information should be an overarching consideration across all three pillars.

i. Lawful but harmful FIMI

Because FIMI includes ‘mostly lawful’ conduct, norms to address the phenomenon should start by making recommendations about which types of *lawful but harmful* information manipulation activities should be addressed, in line with the no-harm principle and international human rights law. Relatedly, the norms also should list the types or examples of measures that can or should be used to tackle them. Thus, norms for FIMI should stipulate that States and non-State actors should, as far as possible, strive to prevent, stop or redress foreign manipulation activities that cause significant physical or non-physical transboundary harm on the territory or infrastructure of another State. As seen earlier, examples of those harms are those that affect the life or health of individuals, stoke national, ethnic, racial, or other group-based division, fuel internal or international armed conflict, affect democratic processes, values or institutions, and undermine environmental efforts or trust in scientific knowledge, including with respect to climate change. These harms may not only be caused by the content of FIMI activities but also by their means or methods. Indeed, consistent activities that seek to undermine a free information environment online, even if legally permitted,

may gradually deteriorate it. Examples include systematic or widespread attacks on specific users or internet freedom more generally by troll armies or bot farms. Measures that can be used to tackle lawful but harmful FIMI include:

a. National legislation, especially for online content governance, data protection, and anti-trust or fair competition between technology companies;

b. Investigations and other enforcement action by competent regulatory authorities, such as the imposition of fines on non-compliant platforms and users

c. Cybersecurity protections, such as firewalls, antivirus, pattern detection software, and active cyber defence measures to disable bots and computer systems used for harmful FIMI;

d. Operational frameworks, such as DISARM and ABCE;

e. Risk assessments, including the regular production of statistics and reports on FIMI and table-top exercises to prevent, stop and mitigate them;

f. International cooperation, including threat, vulnerability and incident information-sharing, which can be facilitated by the conclusion of international treaties and other arrangements;

g. Education and training, including of professionals working on FIMI and the general public, and covering a wide range of subjects relevant to FIMI, such as computer science, behavioural economics, psychology and human rights;

h. Public awareness campaigns, focussing on building citizen resilience against FIMI;

i. Content moderation measures, focussing on measures short of content removal and user de-platforming, such as de-reprioritisation, content labelling, digital nudges, and algorithmic reform;[308]

j. Institutional arrangements to implement the various measures above, including domestically and internationally.

This pillar should also contain a general provision on how, lawful FIMI activities carried out by private entities are in principle protected by the rights to freedom of expression and information. As such, any limitation on those speech acts should observe the tripartite test of legality, legitimacy, necessity and proportionality. A general provision protecting speech that cannot be limited following this tripartite test should also be included. This provision should note that certain types of speech deserve heightened protection, given the public interest in their dissemination. This includes independent journalist content and information published by public officials or politicians.[309] The freedoms of expression and information should be at the heart of any set of norms for FIMI.

ii. Potentially unlawful FIMI

While most FIMI activities are lawful, and should thus be covered by the recommendations above, many are prohibited under international law. But their lawfulness under different international legal rules or regimes (such as sovereignty, non-intervention, due diligence, international human rights law, IHL and international criminal law) depends on a case-by-case assessment of different criteria. These include the author of the information operation, the potential victim(s), sector(s) or interest(s) affected, and the context and severity of the operation in question.[310] Thus, the second pillar of FIMI norms should be more general or flexible, following the example of the Oxford Statement on Information Operations and Activities[311] as well as the Joint Declaration on Freedom of Expression, "Fake News", Disinformation and Propaganda.[312] Specifically, norms should indicate, in general terms, that FIMI should not be contrary to sovereignty, non-intervention, international human rights law, international criminal law and IHL, drawing on the legal criteria analysed above and providing some non-exhaustive examples of when these rules are breached. Norms should also recommend that States refrain from and prohibit internationally wrongful FIMI activities under their domestic laws, whilst cooperating with other States to put an end to them. For example, the norms could stipulate that States should:

Refrain from engaging in FIMI that causes physical effects or functional damage in the territory of another State or otherwise undermines its inherently governmental functions, such as disinformation or propaganda affecting electoral processes or public crisis management policies;

Refrain from interfering in the internal or external affairs of other States, such as on political, cultural, economic, and social matters, through coercive FIMI activities, i.e., those that aim to coerce, employ coercive means, or cause coercive effects on the victim State, such as propaganda or disinformation;

Refrain from carrying out FIMI activities that infringe upon the human rights of individuals or entities within a State's jurisdiction, i.e., insofar as it exercises effective control over the enjoyment of those rights – online or offline, such as hate speech, disinformation, maliformation, and data-gathering techniques.

Refrain from engaging in FIMI activities that violate the rules of IHL, such as using FIMI to disrupt the activities of medical, religious or humanitarian personnel, or to expose prisoners of war to public curiosity;

Prevent, stop or redress unlawful FIMI activities that undermine the rights of other States or cause transboundary harm against their citizens, property or environment, such as certain forms of hate speech, disinformation, propaganda, and malinformation.

As in the case of lawful FIMI activities, the rights of *private* entities to freedom of expression and information should be explicitly protected under his pillar. Recall that most rules of international law are addressed to States, which means that most FIMI activities that are unlawful under international law are carried out by or can be attributed to States. As abstract public entities, States are not entitled to the rights to freedom of expression and information under international human rights law. Nevertheless, due diligence obligations of States, including positive human rights obligations, do cover the conduct of non-State actors, including private FIMI activities and other speech acts. Thus, under this pillar, the proposed norms should mention explicitly that, when seeking to prevent, stop or redress lawful or unlawful FIMI activities by non-State actors, States must respect the right of private entities to freedom of expression and information. This means that, while domestic legislation prohibiting unlawful forms of FIMI is key for the implementation of international law, these prohibitions need not be criminal. Civil or administrative sanctions may be as effective in ensuring compliance by States and other relevant stakeholders with FIMI norms. Aside from domestic legislation and law enforcement action, other measures listed above under the first pillar may also be useful to tackle unlawful forms of FIMI.

iii. Clearly unlawful FIMI

The last pillar of FIMI norms should spell out the types of FIMI that are clearly or manifestly unlawful under international law and thus 'off-limits' for States and non-State actors alike. As seen earlier, these amount to:

a. War propaganda;

b. Propaganda that advocates civil strife in another State;

c. Advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law;

d. Direct and public incitement to commit genocide;

e. Incitement or instigation to commit other international crimes.

It is worth noting that the rights to freedom of expression and information also apply to clearly unlawful FIMI activities. Even though these activities are manifestly unlawful under international law (therefore meeting the legality and legitimacy tests), the exact measures adopted to tackle them (criminal sanctions, content takedowns, user suspension etc.) must still be necessary and proportionate in the circumstances.[313] For example, while war propaganda is serious in and of itself, its non-intentional dissemination need not be criminalised. Likewise, the publication of materials inciting international crimes on one platform should not justify widespread internet or platform shutdowns.[314] Criminal or civil prohibitions under domestic law are likely the most effective measures to tackle manifestly unlawful FIMI activities. But the other measures listed above may also be helpful tools, especially if coupled with clear laws and readily available accountability mechanisms.

Overall, norms for FIMI should list examples of measures that may be available to States, online platforms, civil society, and other stakeholders to tackle different types of FIMI. They should always be designed and implemented in line with international human rights law standards. Examples of the most common and effective measures have been listed earlier. But others may be developed and added to the list over time as threats and defensive technologies or methods evolve. In this way, FIMI norms should provide a 'menu' of (counter)measures that States and other stakeholders can compare against the various types of FIMI they are facing. These could be mixed and matched in different circumstances, depending on the international rules and principles at play and the tripartite test for protecting the freedoms of expression and information. A matrix could also be developed to assist with the interpretation of the norms, laying out a) different types of FIMI activities; b) different types of measures to counter them, and c) different legal and factual considerations at play.

IV.2 NORM-SETTING PROCESSES

Drawing on the norm-setting processes assessed earlier, including their strengths and pitfalls, norms for information operations should be led by States, if they aim to fill legal gaps in protection and eventually crystallise into law. This means that States should chair the process, prepare relevant drafts, and vote on them. The process could start among a select group of partner States (in the context of this Study, the EU and Canada). But it should gradually be expanded to include other like-minded States in Europe (including the UK, Switzerland, and Norway), the Americas (such as the United States, Mexico, Costa Rica, and Brazil) and others in the Asia-Pacific region (such as Japan, South Korea, Australia, and New Zealand). The involvement of an existing international organisation or body, such as the UN Secretary-General, could bring greater legitimacy to the process. FIMI and other information operations are a global phenomenon. Thus, addressing it requires as widespread agreement and coordination as possible among States.

The issue is divisive even among traditional allies, including within the EU itself. However, emphasis may be placed on areas or issues that are conducive to agreement or compromise, such as clearly unlawful types of information operations that should be off-limits, as well as clearly protected speech acts. And if other norms are framed in sufficiently general or flexible terms, agreement is possible even among those that subscribe to different views. Participant States should strive to agree on the text by consensus – not unanimity, as compromises will be needed. Because these are non-binding norms, legitimacy is important. Thus, States should feel that at least the text, viewed as a whole, is acceptable to them. As one delegate commented at the OEWG, perfect cannot be the enemy of good.[315] Voting would neither be necessary nor appropriate in this context. Where agreement cannot be reached on certain norms, the text could be divided into two or more parts: i) a core part containing the norms that all parties subscribe to, likely crafted in more general terms; ii) an annexe containing some implementation guidelines, formulated in more specific terms but not necessarily agreed by everyone; and iii) a commentary, outlining the background to the discussions and areas of agreement and disagreement.

Given the role of the private sector, academia, civil society, and individuals in the ICT environment, any norm-setting process for information operations should involve meaningful participation of these and other relevant stakeholders. As with the OEWG and the Ad Hoc Committee for a UN Draft Cybercrime Convention, these stakeholders should be able to provide input throughout the processes, including on the content of the norms and the format of the meetings. They should be invited to provide both written submissions at relevant stages of the process, attend formal and informal meetings that do not involve confidential matters, and make comments during dedicated consultative stakeholder sessions. Experts should be invited to give briefings on particularly vexed questions, such as legal controversies and technical challenges relating to the implementation of (counter)measures. More informal roundtables or workshops among States and stakeholders, in smaller settings, could be facilitated or convened by other institutions, such as research institutes, think tanks or NGOs.

In this light, the key takeaways of this Study are:

- To fully understand how international law applies to FIMI and effectively design responses to this phenomenon, other types of information operations governed by international law should be borne in mind, such as misinformation and malformation.

- In accordance with international law, norms for FIMI should consider not only the methods by which they are carried out but also their actors, content, effects, targets, and other relevant legal criteria.

- The international legal framework applicable to FIMI and other information operations is made up of different but related rules and principles applicable to the behaviour of States and non-State actors; these must be considered holistically.

- At the heart of this international legal framework are the human rights to freedom of expression and information, which require that any limitations on speech acts by private entities, including lawful or unlawful FIMI activities, be grounded in law, legitimate, necessary, and proportionate.

- International norms for FIMI should mirror this international legal framework. Drawing on the lessons from the cyber and internet governance contexts, their drafting process should be State-led, inclusive of as many like-minded States as possible, including developed and developed countries, consensus-based, and informed by the input of different stakeholders, such as the industry, academia, and civil society.

REFERENCES

1 EEAS, SG.STRAT.2, '1st Report on Foreign Information Manipulation and Interference Threats', https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf, , 4.

2 See Nicolas Hénin, 'FIMI: Towards A European Redefinition of Foreign Interference', EU Disinfo Lab (April 2023), 5

3 EEAS, '1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence' (February 2023), 9-13.

4 Thomas Colley, Francesca Granelli and Jente Althuis, 'Disinformation's Societal Impact: Britain, Covid, And Beyond' (8) 2020 Defence Strategic Communications, NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/pdfjs/?file=/publications/download/colley_web.pdf?zoom=page-fit.

5 EEAS (n 3) 7, 9; Microsoft, 'Defending Ukraine: Early Lessons from the Cyber War' (22 June 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK, 3–4, 12–22; TS Allen and AJ Moore, 'Victory without Casualties: Russia's Information Operations' (2018) 48 Parameters 59, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2851&context=parameters; Christian Perez, Information Warfare in Russia's War in Ukraine: The Role of Social Media and Artificial Intelligence in Shaping Global Narratives, Foreing Policy (22 August 2022), https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/.

6 Jack Goodman and others, 'War in Ukraine: The Making of a New Russian Propaganda Machine', BBC News, 29 May 2022, www.bbc.co.uk/news/world-europe-61441192; Alexey Kovalev, 'Russia's Ukraine Propaganda Has Turned Fully Genocidal' Foreign Policy (9 April 2022), https://foreignpolicy.com/2022/04/09/russia-putin-propaganda-ukraine-war-crimes-atrocities/; Leanne Quinn, 'Timeline of Chemical and Biological Weapons Developments During Russia's 2022 Invasion of Ukraine', Arms Control Association (August 2022), https://www.armscontrol.org/factsheets/timeline-chemical-biological-weapons-developments-during-russias-2022-invasion-ukraine; Vera Bergengruen, 'Inside the Kremlin's Year of Ukraine Propaganda' (22 February 2023), https://time.com/6257372/russia-ukraine-war-disinformation/; Global Affairs Canada, 'Countering disinformation with facts - Russian invasion of Ukraine', https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng (last accessed 2 September 2023).

7 EEAS (n 1) 3, 25; EEAS (n 3) 13-20; Hénin (n 2) 6.

8 EEAS (n 3) 4, 12; Hénin (n 2) 6.

9 EEAS (n 3) 4, 14; Hénin (n 2) 6-7.

10 EEAS (n 3) 13-14; Hénin (n 2) 7.

11 EEAS (n 3) 4, 30-31; Hénin (n 2) 7-8.

12 DISARM Foundation, 'DISARM Framework', https://www.disarm.foundation/framework.

13 EEAS (n 3) 14, 27-29; Hénin (n 2) 5, 9.

14 See 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities', https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities/; Tsvetelina van Benthem, Talita Dias, and Duncan Hollis, 'Information Operations under International Law' (2022) 55 Vanderbilt Journal of Transnational Law 1217, 1219.

15 van Benthem, Dias, and Hollis, ibid, 1228-29.

16 The Online Information Environment: Understanding How the Internet Shapes People's Engagement with Scientific Information', The Royal Society (January 2020), https://royalsociety.org/-/media/policy/projects/online-information-environment/the-online-information-environment.pdf?la=en-GB&hash=691F34A269075C0001A0E647C503DB8F; Jon Bateman and others, 'Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research', Carnegie Endowment for International Peace (18 June 2021), https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824.

17 See 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities', https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities/; 17, 1219, n 1

18 Camille François, Actors, Behaviors, Content: A Disinformation ABC: Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses (20 September 2019; 'ABCDE' Framework, including the analysis of the effects of FIMI incidents, in James Pamment, 'The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework', Working Paper of the Carnegie Endowment for International Peace (September 2020) https://carnegieendowment.org/files/Pamment_-_Crafting_Disinformation_1.pdf.

19 See Dapo Akande, Antonio Coco, and Talita de Souza Dias, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies' (2022) 99 International Law Studies 4.

20 James Crawford, Brownlie's Principles of Public International Law (OUP, 2019), 14-15, 18-19; Martti Koslenniemi, 'What is International Law For? in Malcom D Evans (ed.), International Law (OUP 2014), 33.

21 Crawford (n 20), Chapter 4.

22 Talita Dias, 'Limits on Information Operations Under International Law', 2023 15th International Conference on Cyber Conflict 345, 349.

23 van Benthem, Dias, and Hollis (n 14), 1242.

24 See, e.g., Articles 20 and 19(3) of the International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

25 Miriam Fernándeza, Alejandro Bellogínb and Iván Cantador, 'Analysing the Effect of Recommendation Algorithms on the Amplification of Misinformation' (2021), https://arxiv.org/pdf/2103.14748.pdf; Nathalie Maréchal, Rebecca MacKinnon and Jessica Dheere, 'Getting to the Source

of Infodemics: It's the Business Model: A Report from Ranking Digital Rights, New America (27 May 2020), https://www.newamerica.org/oti/reports/getting-to-the-source-of-infodemics-its-the-business-model/.

26 Written by Anti-Defamation League, Avaaz, Decode Democracy, Mozilla and New America's Open Technology Institute, 'Trained for Deception: How Artificial Intelligence Fuels Online Disinformation: A report from the Coalition to Fight Digital Deception' (1 September 2021), https://foundation.mozilla.org/en/campaigns/trained-for-deception-how-artificial-intelligence-fuels-online-disinformation/; De Angelis L, Baglivo F, Arzilli G, Privitera GP, Ferragina P, Tozzi AE and Rizzo C (2023) ChatGPT and the rise of large language models: the new AI-driven infodemic threat in public health. Front. Public Health 25 April 2023, Vol 11 (2023); doi: 10.3389/fpubh.2023.1166120; JA Goldstein, G Sastry, M Musser, R DiResta, M Gentzel, K Sedova, 'Generative language models and automated influence operations: Emerging threats and potential mitigations', Cornell University Research Paper (10 January 2023) https://arxiv.org/abs/2301.04246.

27 OpenAI, 'Forecasting potential misuses of language models for disinformation campaigns and how to reduce risk' (11 January 2023), https://openai.com/research/forecasting-misuse.

28 van Benthem, Dias, and Hollis (n 14), 1270; Dias (n 22) 348-349.

29 Henning Lahmann, 'Infecting the Mind: Establishing Responsibility for Transboundary Disinformation' (2022) 33 European Journal of International Law 411, 426-427, 436.

30 Dias (n 22) 350-353.

31 Vladyslav Lanovoy, 'Causation in the Law of State Responsibility' (2022) British Yearbook of International Law, https://doi.org/10.1093/bybil/brab008, 4-5; Lahmann (n 29), 426; International Law Commission (ILC) 'Draft Articles on the Responsibility of States for Internationally Wrongful Acts, with commentaries' (2001) A/56/10 (DARSIWA) 92–93, comm (10) to art 31.

32 Dias (n 22) 352-353.

33 E.g., Lanovoy (31) 65; Antonio Coco and Talita de Souza Dias, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32 European Journal of International Law 771, 778; Vladislava Stoyanova, 'Causation between State Omission and Harm within the Framework of Positive Obligations under the European Convention on Human Rights' (2018) 18 Human Rights Law Review 309, 315–16; Vladislava Stoyanova, 'Fault, Knowledge and Risk Within the Framework of Positive Obligations Under the European Convention on Human Rights' (2020) 33 Leiden Journal of International Law 601, 618–19;

34 Dias (n 22) 353. An example is the right to life, see HRC, 'General Comment No 36 on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life' (2018) UN Doc CCPR/C/GC/36 (GC 36) paras 6–7.

35 Laura Courchesne, Isra M Thange, and Jacob N Shapiro, 'Review of Social Science Research on The Effects of Influence Operations' Empirical Studies of Conflict Report (17 July 2021), https://scholar.princeton.edu/sites/default/files/cts_2021_effects_of_ios_evidence_review.pdf; Jon Agley and Yunyu Xiao, 'Misinformation About COVID-19: Evidence for Differential Latent Profiles and a Strong Association with Trust in Science' (2021) 21 BMC Public Health 89.

36 Dias (n 22) 349-350; van Benthem, Dias, and Hollis (n 14), 1223, 1230; Akande, Coco and Dias (n 19).

37 Koskenniemi (n 20) 30-33.

38 Crawford, (n 20), 18-34; Hugh Thirlway, 'The Sources of International', in Malcom D Evans (ed.), International Law (OUP 2014), 91-115.

39 Crawford, (n 20), 14-16; Christopher Greenwood, 'Sources of International Law: An Introduction', UN Legal, https://legal.un.org/avl/pdf/ls/greenwood_outline.pdf; Frederic L. Kirgis, 'Enforcing International Law', (1) ASIL Insights 1996, https://www.asil.org/insights/volume/1/issue/1/enforcing-international-law.

40 See Articles 2(4), 42 and 51 of the Charter of the United Nations, 24 October 1945, 1 UNTS XVI (UN Charter).; International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, 12 December 2000 (ARSIWA), Article 22.

41 Crawford, (n 20), 35-41; Math Noortmann, August Reinisch and Cedric Ryngaert (eds), Non-State Actors in International Law (Hart, 2015); James Summers and Alex Gough (Eds), Non-State Actors and International Obligations

Creation, Evolution and Enforcement (Brill 2018).

42 Crawford, (n 20), 40.

43 Jay Butler, The Corporate Keepers of International Law, 114(2) American Journal of International Law 189-220.

44 Australian Strategic Policy Institute, 'The UN norms of responsible state behaviour in cyberspace Guidance on implementation for Member States of ASEAN', https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace, March 2022, at 14.

45 Alan Boyle, 'Soft Law in International Law', in in Malcom D Evans (ed.), International Law (OUP 2014), 118-133.

46 E.g., van Benthem, Dias, and Hollis (n 14); Dias (n 22); Lahmann (n 29); Henning Lahmann, 'Information Operations and the Question of Illegitimate Interference under International Law' (2020) 53 Israel Law Review 189; Björnstjern Baade, 'Fake News and International Law' (2018) 29 European Journal of International Law 1357.

47 See UNGA Resolutions 58/32 (18 December 2003); 59/61 (16 December 2004); 60/45 (8 December 2005), 61/54 (6 December 2006), 62/17 (5 December 2007), 63/37 (2 December 2008), 64/25 (2 December 2009), 65/41 (8 December 2010, 66/24 (2 December 2011), 67/27 (3 December 2012), 68/243 (27 December 2013), 69/28 (2 December 2014), 70/237 (23 December 2015), 71/28 (5 December 2016) and 73/266 (2 January 2019).

48 UN GGE 2015 Report, UNGA Resolution A/70/174 (22 July 2015), para 24.

49 Ibid, paras 26-27.

50 UN GGE 2021 Report, UNGA Resolution A/76/135 (14 July 2021), paras 69-73.

51 UN GGE 2015 Report (n 48), para 10. See also UN GGE 2021 Report (n 50), para 15.

52 UNGA Resolution 73/27 (11 December 2018)

53 OEWG 2021 Final Substantive Report, UNGA Resolution 75/816 (18 March 2021), paras 7, 24, 34. See also OEWG 2022 Report, UNGA Resolution A/77/275 (8 August 2022), paras 2-3, 12, 14.

54 OEWG 2021 Report (n 53), para 7.
55 UN GGE 2021 Report (n 50), para 9.
56 OEWG 2023 Report, UNGA Resolution A/AC.292/2023/CRP.1 (28 July 2023), para 14.
57 UN GGE 2021 Report (n 50), para 9; OEWG 2023 Report (n 56), para 14.
58 Michael N. Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017); Michael N. Schmitt (ed), Tallinn Manual on the International Law Applicable to Cyber Warfare (CUP 2013).
59 https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/.
60 https://pariscall.international/en/call.
61 https://www.internetgovernance.org/what-is-internet-governance/; https://www.unesco.org/en/internet-governance.
62 UN Secretary-General, 'Our Common Agenda: Report of the Secretary-General', https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf, para 93.
63 https://www.un.org/techenvoy/global-digital-compact/intergovernmental-process.
64 https://globalnetworkinitiative.org/.
65 https://globalnetworkinitiative.org/gni-principles/
66 E.g., 'Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan', UN General Assembly Resolution A/HRC/47/25, 13 April 2021 ('UN Report on Disinformation and Freedom of Expression').
67 Van Benthem, Dias and Hollis (n 14), 1281.
68 Duncan B. Hollis, Why States Need an International Law for Information Operations, 11 Lewis & Clark L. Rev. 1023 (2007).
69 See n 36 above.
70 Van Benthem, Dias and Hollis (n 14), 1262-1264.
71 Island of Palmas Case (or Miangas), United States v Netherlands, Award, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), 838.
72 Matthew Craven, 'Statehood, Self-determination, and recognition' in in Malcom D Evans (ed.), International Law (OUP 2014) 202, 213; Rule 3, Tallinn Manual (n 58), 16-17.
73 Island of Palmas (n 71) 839; S.S. 'Lotus', France v Turkey, Judgment, Judgment No 9, PCIJ Series A No 10 (1927), 18-19; Rule 2, Tallinn Manual (n 58), 16, para 12.
74 Rule 2, Tallinn Manual (n 58) 13-16.
75 Island of Palmas (n 71) 838.
76 Rule 4, Tallinn Manual (n 58), para 2.
77 Rule 1, Tallinn Manual (n 58), 11-13.
78 Rule 4, Tallinn Manual (n 58), paras 13-21; Harriet Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention', Chatham House Research Paper (2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks, paras 20-21, 46-54.
79 Suella Braverman KC MP, 'International Law in Future Frontiers', UK Attorney-General's Office (19 May 2022), https://www.gov.uk/government/speeches/international-law-in-future-frontiers.
80 Moynihan (n 79) paras 20, 55. See also 'Sovereignty', Cyber Law Toolkit, https://cyberlaw.ccdcoe.org/wiki/Sovereignty.
81 Rule 4, Tallinn Manual (n 58), para 12; Priya Urs, Talita Dias, Antonio Coco and Dapo Akande, The International Law Protections against Cyber Operations Targeting the Healthcare Sector, https://www.elac.ox.ac.uk/wp-content/uploads/2023/04/ELAC-Research-Report_International-Law-Protections-against-Cyber-Operations-Targeting-the-Healthcare-Sector.pdf, 140-143.
82 Rule 4, Tallinn Manual (n 58), esp. paras 10-22; Urs, Dias, Coco and Akande (n 81), 145-154.
83 See Moynihan (n 79), para 21.
84 See 'Sovereignty', Cyber Law Toolkit (n 80).
85 Van Benthem, Dias and Hollis (n 14), 1264; Urs, Dias, Coco and Akande (n 81), 160-161; Marko Milanovic and Michael N. Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations During a Pandemic' (2020) 11 Journal of National Security Law and Policy 247, 252-254.
86 Rule 4, Tallinn Manual (n 58), paras 16-17.
87 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States) (Merits) [1986] ICJ Rep 14, para 205 (emphasis added). See also Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of Congo v Uganda) (Merits) [2005] ICJ Rep 168, paras 162–64.
88 Rule 66, Tallinn Manual (n 58), para 18.
89 Steven Wheatley, Cyber and Influence Operations Targeting Elections: Back to the Principle of Non-Intervention, EJIL: Talk! (Oct. 26, 2020), https://www.ejiltalk.org/cyber-and-influence-operations-targeting-elections-back-to-the-principle-of-non-intervention/; van Benthem, Dias and Hollis (n 14), 1259.
90 Dias (n 22), 354-355.
91 UNGA, UNGA, 'Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States' UN Doc A/RES/36/103 (1981), <https://digitallibrary.un.org/record/27066?ln=en> accessed 7 March 2023, Annex, I(c)
92 Ibid, II (f), (j) and (l) (emphasis added).
93 Nicaragua (n 87) para 205; Rule 66, Tallinn Manual (n 58) paras 6-8.
94 Nicaragua (n 87) para 205.
95 Milanovic and Schmitt (n 85) 257.
96 Rule 66, Tallinn Manual (n 58) paras 13-15; van Benthem, Dias, and Hollis (n 14) 1260-1260.

97 Moynihan (n 79) paras 106-107.
98 Urs, Dias, Coco and Akande (n 81) 108-110
99 See Articles 49-54, ARSIWA (n 40).
100 'Due diligence', Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/due-diligence.
101 Coco and Dias (n 33) 772-773; 'Due Diligence', Cyber Law Toolkit (https://cyberlaw.ccdcoe.org/wiki/Due_diligence); Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views', The Hague Program For Cyber Norms Policy Brief (March 2020), https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/153989/roguski_application_of_international_law_to_cyber_operations_2020.pdf, 11-12; Rule 6, Tallinn Manual (n 58) paras 25, 30
102 Koivurova, 'Due Diligence', Max Planck Encyclopaedia of Public International Law (MPEPIL) (2010), opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1034?prd=EPIL, paras 1-2; International Law Association (ILA), Study Group on Due Diligence, 2nd Report (2016), available at https://www.ila-hq.org/index.php/study-groups, 6.
103 Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', 97 International Law Studies 395 (2021), 404.
104 See McDonald, 'The Role of Due Diligence in International Law', 68 International and Comparative Quarterly (ICLQ) (2019) 1041, at 1043–1044; Heike Krieger and Anne Peters, 'Due Diligence and Structural Change in the International Legal Order', in Heike Krieger, Anne Peters and Leonard Kreuzer (eds.), Due Diligence and Structural Change in the International Legal Order (OUP 2020); Coco and Dias (n 33) 774.
105 Coco and Dias (n 33) 774.
106 Akande, Coco and Dias (n 19) 24-28.
107 See Article 14(3) ARSIWA (n 40).
108 Corfu Channel Case (United Kingdom v Albania), Judgment, 9 April 1949, ICJ Reports (1949) 4.
109 Ibid 22 (emphasis added).
110 Dias (n 22) 357-359.
111 ILC, Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, in Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001), UN Doc. A/56/10, Article 3.
112 Ibid, Article 2(b). See also Brunée and Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance', 58 GYIL (2015) 129, 134–135; Koivurova (n 103), paras 16, 23, 44-45.
113 See Coco and Dias (n 33) 790; 'Costa Rica's Position on the Application of International Law in Cyberspace', https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf, para 29.
114 Adopted 23 September 1936, entered into force 2 April 1938, 186 UNTS 301.
115 https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280046246&clang=_en.
116 Dias (n 22) 359.
117 Constitution and Convention of the International Telecommunication Union (with annexes and optional protocol), adopted on 22 December 1992, entered into force 1 July 1994, 1825 UNTS 31251.
118 https://www.itu.int/online/mm/scripts/gensel8.
119 Coco and Dias (n 33) 776.
120 UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).
121 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.
122 https://www.ohchr.org/en/what-are-human-rights/international-bill-human-rights
123 Proclamation of Teheran, Final Act of the International Conference on Human Rights, Teheran, 22 April to 13 May 1968, U.N. Doc. A/CONF. 32/41 (1968), 3.
124 Convention for the Protection of Human Rights and Fundamental Freedoms (adopted on 4 November 1950, entered into force 3 September 1953) ETS No 5.
125 Adopted on 26 October 2012, 2012/C 326/02.
126 Charter of the Organization of American States (OAS) (adopted on 22 January 1969, entered into force 13 December 1951) 119 UNTS 3.
127 https://www.cidh.oas.org/basicos/english/Basic4.Amer.Conv.Ratif.htm.
128 International Covenant on Economic, Social and Cultural Rights (adopted 19 December 1966, entered into force 3 January 1976) 993 UNTS 3.
129 ICCPR art 2(1); UN Human Rights Committee (HRC), 'General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.1, paras 3, 5–6 and 10.
130 Ibid, para 8; S Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!' (2020) 9(1) ESIL Reflections 2, 4-5
131 HRC, General comment no. 31 (n 131) para 8.
132 Ibid paras 7-8.
133 Human Rights Council Resolution 26/13, 'The promotion, protection and enjoyment of human rights on the Internet', UN Doc A/HRC/RES/26/13, para 1; UN GGE Report 2021 (n 50) para 15; UN GGE Report 2015 (n 51), para 10; Rule 34, Tallinn Manual (n 58) and 179-182.
134 Nicolás Carrillo-Santarelli, 'Corporate Human Rights Obligations: Controversial but necessary' (24 August 2015), https://www.business-humanrights.org/en/blog/corporate-human-rights-obligations-controversial-but-necessary/; Crawford (n 20) 111.
135 UN Office of the High Commissioner for Human Rights, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf. See also UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on

Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression And "Fake News", Disinformation and Propaganda' (3 March 2017) https://www.osce.org/files/f/documents/6/8/302796.pdf ('Joint Declaration'), preambular para 11 and operative paras 4-6.

136 See, e.g., Articles 5-8bis and 25, UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998 (ICC Statute).

137 Evelyn Mary Aswad, 'The Future of Freedom of Expression Online' (2018) 17 Duke Law and Technology Review 26, 65-67.

138 Lea Raible, 'Between facts and principles: jurisdiction in international human rights law', (13) 2022 Jurisprudence 52–72; Marko Milanović, 'From Compromise to Principle: Clarifying the Concept of State Jurisdiction in Human Rights Treaties', Human Rights Law Review (3) 2008 411–448.

139 Art 2(1) ICCPR, Art 1 ECHR. See also Art 1(1) ACHR.

140 HRC, 'General Comment No. 36 Article 6: Right to Life' (3 September 2019) UN Doc CCPR/C/GC/36 ('General Comment 36'), paras 21-22, 63.

141 Advisory Opinion OC-23/17 (15 November 2017), paras 72-82.

142 See also Costa Rica's Position (n 131), para 32.

143 See, e.g., Banković and others v Belgium and others (Appl. no 52207/99) (ECtHR, 12 December 2001) paras 74–82; and Al-Skeini and others v United Kingdom (App no 55721/07) (ECtHR, 7 July 2011), paras 136–137. For a recent analysis, see Marko Milanovic, 'The Murder of Jamal Khashoggi: Immunities, Inviolability and the Human Right to Life' (2020) Human Rights Law Review 1, 23–24

144 See Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa' (26 May 2021) EJIL: Talk!, https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/.

145 German Constitutional Court (Bundesverfassungsgericht, or 'BVerfG'), Bundesnachrichtendienst (19 May 2020) 1 BvR 2835/17, https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html.

146 Manfred Nowak, UN Covenant on Civil and Political Rights: CCPR Commentary (2nd edn, NP Engel 2005), 475.

147 https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND

148 See Jeroen Temperman, Religious Hatred and International Law: The Prohibition of Incitement to Violence or Discrimination (CUP, 2015), 32-61, 73

149 Art. 2(4) UN Charter; UNGA, 'Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations' (1970) UN Doc A/RES/2625(XXV), Para 1, Principle 5.

150 Art. 6 ICCPR; Art. 2 ECHR; HRC, General Comment 36 (n 141) paras 6–7.

151 Art. 7 UDHR

152 See Hurst Hannum, 'The Status of the Universal Declaration of Human Rights in National and International Law' (1996) 25 Georgia Journal of International and Comparative Law 287, 342–43; Dias (n 22) 361-362.

153 Dias (n 22) 356, 361-362; van Benthem, Dias, and Hollis (n 14) 1240.

154 Emphasis added. Article 10(1) of the ECHR is very similar and reads: 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.'

155 Dias (n 22) 357.

156 Joint Declaration (n 136) para 1(c) and (h).

157 Ibid, preambular para 7; UN Report on Disinformation and Freedom of Expression (n 66) para 38.

158 Emphasis added. Article 10(2) ECHR similarly provides that 'The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary'.

159 Urs, Dias, Coco and Akande (n 81) 222, 229-230.

160 HRC, 'General comment No. 34 - Article 19: Freedoms of opinion and expression' (12 September 2011) UN Doc CCPR/C/GC/34 ('General Comment 34') para 7; Nowak (n 147) 440–441.

161 Joint Declaration (n 136) 2(c)-(d); Milanovic and Schmitt (n 85) 272; UN Report on Disinformation and Freedom of Expression (n 66) paras 38, 88, 93.

162 Joint Declaration (n 136) preambular para 9 and operative para 3(a); General Comment 34 (n 161) paras 14, 40; Dink v Turkey (App nos 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09) (ECtHR, 14 September 2010), para 137.

163 Joint Declaration (n 136) preambular para 8, operative para 3(a)-(d); HRC, 'General Comment No. 10: Article 19 (Freedom of Opinion'' (29 June 1983) ('General Comment 10') para 2; UN Report on Disinformation and Freedom of Expression (n 66)para 38; NIT S.R.L v Moldova [GC] (App no 28470/12) (ECtHR, 5 April 2022), paras 101, 185; Centro Europa 7 S.R.L. and Di Stefano [GC] (App no 38433/09) (ECtHR, 7 June 2012), paras 129–30.

164 Urs, Dias, Coco and Akande (n 81) 222-229.

165 Evelyn Mary Aswad 'To Protect Freedom of Expression, Why Not Steal Victory from the Jaws of Defeat?' (2020) 77(2) Washington and Lee Law Review 609, 618.

166 Joint Declaration (n 136) para 3(b).

167 Aswad (n 166) 625

168 General Comment 34 (n 161) paras 33–36

169 Ibid.

170 Joint Declaration (n 136) para 1(e).

171 Joint Declaration (n 136)
172 Ibid paras 3-6.
173 International Committee of the Red Cross (ICRC), 'What is International Humanitarian Law?' (6 April 2022), https://www.icrc.org/en/document/what-international-humanitarian-law.
174 Ibid.
175 Rule 80, Tallinn Manual (n 58).
176 See ICRC, 'Harmful Information – Misinformation, disinformation and hate speech in armed conflict and other situations of violence: ICRC initial findings and perspectives on adapting protection approaches' (9 July 2021), https://www.icrc.org/en/publication/4556-harmful-information-misinformation-disinformation-and-hate-speech-armed-conflict; Costa Rica's Position (n 131) para 57.
177 Article 1 common to: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field 1949, 75 UNTS 31; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea 1949, 75 UNTS 85; Convention (III) relative to the Treatment of Prisoners of War 1949, 75 UNTS 135; Convention (IV) relative to the Protection of Civilian Persons in Time of War, 75 UNTS 287.
178 Art. 51(2) Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts 1977 (AP I), 1125 UNTS 3; Art. 13(2) Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts 1977, 1125 UNTS 609 (APII); ICRC, Customary IHL Database, Rule 2, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule2.
179 See Rules 25, 26, 31, 32 ICRC Customary IHL Study, https://ihl-databases.icrc.org/en/customary-ihl/v1.
180 Rule 15, ICRC Customary Study, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule15; Article 57(1) AP I; Article 13(1) AP II.
181 See ICRC, 'Commentary to Convention (III) relative to the Treatment of Prisoners of War, Geneva, 12 August 1949', Articles 13 and 14 (2020), https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-13/commentary/2020?activeTab=undefined; https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-14?activeTab=undefined.
182 Arts 1-3 ARSIWA (n 40).
183 'Customary Law on State Responsibility', Georgetown Law Library, https://guides.ll.georgetown.edu/c.php?g=371540&p=2511830.
184 ARSIWA (n 40).
185 DARSIWA (n 31), Commentary to Chapter II, Part III, at 128-129.
186 Arts 30, 31 and 37 ARSIWA (n 40).
187 Arts 22 and 49 ARSIWA (n 40).
188 See Martin Dawidowicz, Third-Party Countermeasures in International Law (CUP 2017); Council of the EU, COJUR, 'Working Party on Public International Law: Revised paper on third-party countermeasures under international law', WK 10275/2022 INIT (17 November 2022), https://www.asktheeu.org/en/request/13284/response/48490/attach/html/9/wk15858.en22.pdf.html.
189 Costa Rica's Position (n 131) para 15; Ministry of Foreign Affairs of Poland, 'The Republic of Poland's position on the application of international law in cyberspace' (December 2022) https://www.gov.pl/attachment/3203b18b-a83f-4b92-8da2-fa0e3b449131, 8; UNODA, 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States', UNODA, A/76/136, August 2021, Estonia, at 28.
190 Art. 49(2) and Commentary (6) DARSIWA (n 31).
191 Art. 49(1) and Commentary (1) DARSIWA (n 31).
192 Arts. 49-53 and Commentary DARSIWA (n 31).
193 Joint Declaration (n 136) preambular para 12.
194 Art. 51 and Commentary (7) DARSIWA (n 31).
195 See, e.g., UNGA, Unilateral sanctions in the cyberworld: tendencies and challenges, A/77/296, (17 August 2022), paras 19-24, 31, 47-49, 92-95; UN Human Rights Council, 'Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, on his mission to the Russian Federation', A/HRC/36/44/Add.1 (27 July 2017), paras 10-13.
196 Henning Lahmann, Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution (CUP 2020) 125; Tallinn Manual (n 58), Glossary of Technical Terms.
197 UN GGE 2015 Report (n 51), para 13.
198 E.g., OEWG 2021 Final Substantive Report (n 53), paras 7-25.
199 North Atlantic Treaty Organization (NATO), Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'Tallinn Manual', https://ccdcoe.org/research/tallinn-manual/; 'The Tallinn Manual & Primary Law Applicable to Cyber Conflicts', Georgetown Law Library, https://guides.ll.georgetown.edu/cyberspace/cyber-conflicts.
200 The Oxford Process, 'Overview', Oxford Institute for Ethics, Law and Armed Conflict (ELAC), https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/; 'The Oxford Process on International Law Protections in Cyberspace: A Compendium', ELAC, https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf ('Oxford Process Compendium'), 10-13.
201 UNODA, 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes', https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.
202 UN Office of the Secretary-General's Envoy on Technology, 'Intergovernmental Process led by the Co-facilitators Rwanda and Sweden', https://www.un.org/techenvoy/global-digital-compact/intergovernmental-process
203 GNI, 'About the GNI', https://globalnetworkinitiative.org/about-gni/.
204 UN General Assembly, 'Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States', A/RES/36/103, Annex, especially principle 1(c).

205 UN General Assembly Resolution 43/78 H (7 December 1988).
206 UN General Assembly Resolution 53/70 (4 January 1999), preamble.
207 Ibid, para 4.
208 UN General Assembly Resolution 56/19 (7 January 2002), paras 2 and 4.
209 UN General Assembly Resolution 57/53 (30 December 2002), paras 2 and 4; UN General Assembly Resolution 58/32 (18 December 2003), paras 2 and 4. The UN GGE had four iterations (the original one in 2004, 2009, 2012 and 2019) and different compositions (see UNGA Resolution 57/53 (n 210), para 4; UNGA Resolution 60/45 (6 January 2006), para 4; UNGA Resolution 65/41 (11 January 2011), para 4; UNGA Resolution 73/266 (2 January 2019), para 3). It was initially made up of experts from 15 UN member States and ended up with one or more representatives of 25 States, selected on the basis of equitable geographical distribution (see UN GGE 2021 Report (n 50) Letter of Transmittal, 5; UNODA, 'Group of Governmental Experts', https://disarmament.unoda.org/group-of-governmental-experts/). The Group adopted four consensus reports (in 2010, 2013, 2015 and 2021).
210 UN GGE 2021 Report (n 50) Letter of Transmittal, 5
211 UN GGE 2015 Report (n 48), para 13.
212 UN GGE 2010 Report (n 212), para 18(i).
213 UN GGE 2015 Report (n 48), paras 9-10.
214 Ibid, para
215 Ibid, para 10.
216 Ibid.
217 Akande, Coco and Dias (n 19) 29-35.
218 Ibid 31-32, 35.
219 UNGA Resolution 70/237 (n 47)para 1.
220 E.g., OEWG 2023 Report (n 56) paras 6, 4, 23; OEWG 2022 Report (n 53) paras 2, 14; OEWG 2021 Final Substantive Report (n 53) paras 7, 24.
221 UNGA Resolution 75/240 (4 January 2021). See also Digwatch, 'GGE vs OEWG', https://dig.watch/processes/un-gge.
222 OEWG 2023 Report (n 56) paras 6, 4, 23, 28; OEWG 2021 Final Substantive Report (n 53), paras 7, 24, 34; OEWG 2022 Report (n 53) paras 2-3, 12, 14.
223 OEWG 2021 Final Substantive Report (n 53), para 25.
224 Akande, Coco and Dias (n 19) 33-35.
225 UN GGE 2015 Report (n 48) para 13.
226 Ibid para 13(a).
227 Ibid para 13(b).
228 Coco and Dias (n 33) 772-773.
229 UN GGE 2015 Report (n 48) para 13(c).
230 Coco and Dias (n 33) 783.
231 UN GGE 2015 Report (n 48) para 13.
232 See Talita Dias and Antonio Coco, 'Cyber Due Diligence in International law', ELAC Report (March 2021), https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf, 170.
233 UN GGE 2015 Report (n 48) para 13(e), referring to Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age.
234 UN GGE 2015 Report (n 48) para 13(f)
235 See Cybersecurity Tech Accord, 'Industry Perspective Rejected: Cybersecurity Tech Accord releases joint statement on veto by UN cyber working group' (21 July 2012), https://cybertechaccord.org/industry-perspective-rejected-cybersecurity-tech-accord-regrets-decision-by-states-to-reject-participation-in-un-open-ended-working-group-on-cybersecurity/.
236 See Burhan Gafoor, OEWG Chair, 'Agreed modalities for the participation of stakeholders in the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025' (22 April 2022), https://documents.unoda.org/wp-content/uploads/2022/04/Letter-from-OEWG-Chair-22-April-2022.pdf; Let's Talk Cyber, 'OEWG Agrees on Modalities for Multistakeholder Participation After Silent Procedure' (22 April 2022), https://letstalkcyber.org/news/oewg-agrees-on-modalities-for-multistakeholder-participation-after-silent-procedure; Digwatch, 'Modalities of multistakeholder participation', https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/modalities-of-multistakeholder-participation.
237 See UNODA, https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=author_type_documents_%3ANon-governmental%20organization.
238 OEWG 2023 Report (n 56) paras 27 and 31(b).
239 OEWG 2021 Report (n 53) para 56.
240 OEWG 2023 Report (n 56) para 43(f).
241 Ibid para 37.
242 See papers listed in the Annex D of OEWG 2023 Report (n 56), especially the Russian Federation's 'Updated Concept Of The Convention Of The United Nations On Ensuring International Information Security' (2021), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf.
243 See UN General Assembly Resolution A/C.1/77/L.73 (13 October 2022). See also Paul Meyer, 'UN OEWG – Walking the Talk: For a new UN Program of Action (PoA) for Responsible State Behaviour in Cyberspace', ICT4Peace (19 October 2022), https://ict4peace.org/activities/un-oewg-walking-the-talk-for-a-new-un-program-of-action-poa-for-responsible-state-behaviour.

244 UNGA Resolution 74/247 (20 January 2020) preamble, para 2.
245 Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 'Draft text of the convention', UNGA Resolution A/AC.291/22 (29 May 2023) ('Zero Draft')
246 See ARTICLE 19, 'UN: Cybercrime Convention must meet international free speech standards' (4 January 2023) https://www.article19.org/resources/un-draft-cybercrime-convention-free-speech-standards/; Barbora Bukovská, 'New U.N. cybercrime treaty threatens human rights' (27 January 2023), https://www.context.news/surveillance/opinion/new-un-cybercrime-treaty-threatens-human-rights; Faouzia Mebarki and Joyce Hakmeh, 'Global protection against cybercrime now within reach' (Chatham House, 14 June 2023), https://www.chathamhouse.org/2023/06/global-protection-against-cybercrime-now-within-reach; Katitza Rodriguez and Tomaso Falchetta, 'Submission by Electronic Frontier Foundation and Privacy International to the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose' (2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/EFF_contribution.pdf.
247 Council of Europe, Convention on Cybercrime, 23 November 2001, European Treaty Series-No. 185.
248 Zero Draft (n 256), Arts 6-12.
249 Ibid Arts 13 and 14.
250 Ibid Art. 15.
251 See ARTICLE 19, 'Comments on the Consolidated Negotiating Document on the Elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes' (2023), https://www.article19.org/wp-content/uploads/2023/01/ARTICLE-19-analysis-of-the-Cybercrime-Convention-Negotiating-Document-January-2023.pdf.
252 Joint Declaration (n 136) para 2(a).
253 UN Office on Drugs and Crime, 'Participation of multi-stakeholders in the sessions of the Ad Hoc Committee', https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/information-for-multi-stakeholders.html; UN General Assembly Resolution A/AC.291/6 (2 March 2022).
254 Ibid, Annex II, para 4.
255 Mebarki and Hakmeh (n 57).
256 Ibid.
257 Katitza Rodriguez, 'First Draft of UN Cybercrime Convention Drops Troubling Provisions, But Dangerous and Open-Ended Cross Border Surveillance Powers are Still on the Table', EFF (20 July 2023), https://www.eff.org/deeplinks/2023/07/first-draft-un-cybercrime-treaty-drops-troubling-provisions-dangerous-and-open.
258 Supra n 203 and 204.
259 UN Secretary-General, Our Common Agenda (n 62), para 93.
260 UN Secretary-General, 'Our Common Agenda Policy Brief 5' (2023), https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-gobal-digi-compact-en.pdf, 11.
261 Ibid.
262 Ibid 12.
263 UN Office of the Secretary-General's Envoy on Technology (n 203).
264 UN Secretary-General (n 271) 12.
265 Ibid 19.
266 Ibid 20.
267 UN Office of the Secretary-General's Envoy on Technology, Roadmap for the intergovernmental process on the Global Digital Compact (2023), https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-Updated-Roadmap.pdf.
268 UN Secretary-General (n 271) 15
269 UN Secretary-General (n 271) 15-16.
270 Ibid 15.
271 Ibid.
272 Ibid 15-16.
273 Ibid 16.
274 GNI (n 204).
275 GNI, 'The GNI Principles', https://globalnetworkinitiative.org/gni-principles/
276 GNI, 'Issues', https://globalnetworkinitiative.org/policy-issues/
277 GNI, 'Intermediary Liability & Content Regulation', https://globalnetworkinitiative.org/policy-issues/intermediary-liability-content-regulation/
278 GNI, 'Implementation Guidelines', https://globalnetworkinitiative.org/implementation-guidelines/.
279 For reasons of space, this study will not delve into other non-State-led indicatives, such as 'The Paris Call for trust and security in cyberspace', https://pariscall.international/en/.
280 Costa Rica's Position (n 131) para 6.
281 NATO CCDCOE (n 200).
282 Tallinn Manual (n 58) 1.
283 NATO CCDCOE (n 200) and Georgetown Law Library (n 200).
284 NATO CCDCOE, 'CCDCOE to Host the Tallinn Manual 3.0 Process', https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/.
285 Tallinn Manual (n 58) 1-2.
286 Ibid 2 and 6.
287 Ibid 3.

288 Ibid 3-5.
289 Eric Talbot Jensen, 'The Tallinn Manual 2.0: Highlights and Insights' (48) 2017 Georgetown Journal of International Law 735, 738.
290 Tallinn Manual (n 58) 5-6.
291 The Process was also co-founded by the author of this report (Dr Talita Dias, Chatham House and Oxford University), Dr Antonio Coco (Essex University), Ms Tsvetelina van Benthem, and Mr Jim O'Brian. It was supported by Microsoft and the Government of Japan. See Oxford Process Compendium (n 201) 23.
292 Ibid 10, 14-15.
293 Ibid 14.
294 Ibid 15-17.
295 Ibid 12-15.
296 Ibid 17.
297 Ibid 18-19.
298 Ibid 17.
299 Ibid 13-14.
300 Ibid 536-581.
301 Ibid 14-15.
302 Ibid 365-367; The Oxford Process, 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities', ELAC (2 June 2021) https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities/;
303 Oxford Process Compendium (n 201) 566-573.
304 Ibid 365-367, 373-392.
305 The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities (n 313) para 3.
306 Ibid para 4.
307 Ibid para 9.
308 See, e.g., Council of Europe, 'Combating hate speech - Recommendation CM/Rec(2022)16 and explanatory memorandum (2022)', https://edoc.coe.int/en/racism/11119-combating-hate-speech-recommendation-cmrec202216-and-explanatory-memorandum.html.
309 Case of Mouvement Raëlien Suisse v Switzerland App no 16354/06 (ECtHR, 13 July 2012) para 61; Council of Europe, 'Recommendation CM/Rec(2022)4 of the Committee of Ministers to member States on promoting a favourable environment for quality journalism in the digital age' (17 March 2022) https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a5ddd0.
310 Report on Disinformation and freedom of opinion and expression (n 66) para 43.
311 The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities (n 313).
312 Joint Declaration (n 136).
313 See General Comment 34 (n 161) para 50; Report on Disinformation and freedom of opinion and expression (n 66) paras 43-44.
314 Ibid paras 50-51.
315 The author of this Study attended the meetings of Fifth Substantive Session of the OEWG, where this statement was made orally. A recording of the relevant meeting is available at UN Web TV, '9th Meeting of the OEWG' (28 July 2023), https://media.un.org/en/asset/k1s/k1sfeesjsl.


European Union
EXTERNAL ACTION