INTERNATIONAL LAW AND CYBERSECURITY GOVERNANCE

Edited by François Delerue and Aude Géry

with contributions from Giovanna Adinolfi, Talita Dias, Duncan B. Hollis, Vera Rusinova, and Barrie Sander
INTERNATIONAL LAW AND CYBERSECURITY GOVERNANCE

Edited by François Delerue and Aude Géry,
with contributions from Giovanna Adinolfi,
Talita Dias, Duncan B. Hollis,
Vera Rusinova, and Barrie Sander

July 2022
4. Human rights recognised: the potential role of human rights in the work of the UN General Assembly First Committee 35
4.1. Human rights and the cyber threat landscape 36
4.2. Human rights and concepts of international law 38
4.3. Human rights and proposals for advancing responsible state behaviour in ICTs 40
5. Human rights contested: the risks of pursuing a human rights-based approach in the UN General Assembly First Committee 41

APPLICATION OF SOVEREIGNTY TO INFORMATION AND COMMUNICATIONS TECHNOLOGIES / VERA RUSINOVA 43
1. Introduction 43
2. Setting the scene 43
3. Sovereignty as a rule or as a principle: a unity of opposites 45
4. Sovereignty as a prohibitive rule: legal obstacles for lawmaking 46
5. New ways for the formalisation of sovereignty in ‘cyberspace’ 47
6. Conclusion 50

FROM COROLLARIES TO CONTENTS? ELABORATING THE PRINCIPLE OF NON-INTERVENTION IN CYBERSPACE / DUNCAN B. HOLLIS 51
1. Introduction 51
2. Corollaries 53
3. Contents 53
3.1. Acts attributable to states 54
3.2. Methods of coercion 54
3.3. Internal and external affairs 55
4. Forward path(s)? 56

DUE DILIGENCE IN INTERNATIONAL LAW AND ITS APPLICATION TO INFORMATION AND COMMUNICATIONS TECHNOLOGIES / TALITA DIAS 59
1. Introduction 59
2. Why does due diligence matter in the cyber context? 59
3. What exactly is due diligence in international law? ............................................................. 60
3.1. A general principle? .................................................................................................................... 61
3.2. A cyber-specific rule? ................................................................................................................. 61
3.3. A standard of conduct? ............................................................................................................ 62
3.3.1. The Corfu Channel principle ................................................................................................ 62
3.3.2. The no-harm principle .......................................................................................................... 63
3.3.3. Positive human rights obligations ...................................................................................... 64
3.3.4. Positive obligations under international humanitarian law ......................................... 64
4. Due diligence at the UN GGE and OEWG: does it apply to ICTs? .................................. 65
5. Conclusion: the way ahead ......................................................................................................... 66

ABOUT THE AUTHORS .................................................................................................................... 67

ABOUT EU CYBER DIRECT ........................................................................................................... 70
1. Introduction

In recent years, there have been two main dynamics concerning the international law applicable to cyberspace. The first dynamic concerns the multilateral processes on international cybersecurity. The successive United Nations Groups of Governmental Experts (GGEs) and the Open-Ended Working Group (OEWG) have affirmed the applicability of international law to cyberspace and initiated some discussions on specific aspects and branches of international law. The second dynamic concerns the unilateral approach of states on the matter, as an increasing number of states have been publicly releasing statements and documents outlining their interpretation of how the rules and principles of international law apply in cyberspace. On the basis of the observation of these two dynamics, we convened a group of 16 scholars and experts on 21 January 2022 for the first EU Cyber Direct Research Seminar, the results of which are published in this edited publication.

---


2 The UNGA created two successive OEWGs with a similar agenda in 2018 (2019–2020) and in 2020 (2021–2025): UNGA, Developments in the field of information and telecommunications in the context of international security, Resolution 73/27, adopted on 5 December 2018, UN Doc A/RES/73/27; UNGA, Developments in the field of information and telecommunications in the context of international security, Resolution 75/240, 31 December 2020, UN Doc A/RES/75/240.


4 See, generally, the list of national positions on the website of the International Cyber Law in Practice: Interactive Toolkit, https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions

5 The participants were: Giovanna Adinolfi (University of Milan), Dennis Broeders (Leiden University), François Delerue (Leiden University), Talita Dias (Jesus College & University of Oxford), Sophie Duroy (KFG Berlin-Potsdam Research Group ‘The International Rule of Law: Rise or Decline?’), Aude Géry (GEODE, Paris 8), Larissa van den Herik (Leiden University), Duncan B. Hollis (Temple University), Matthias C. Kettemann (University of Innsbruck), Patryk Pawlak (EUISS), Przemyslaw Roguski (Jagiellonian University), Annachiara Rotondo (University of Naples Federico II), Vera Rusinova (National Research University
The approach of the European Union has evolved in the past year, following notably what has been described as the ‘geopolitical’ turn of the Commission. This evolution was another driving element in our reflection. On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy. Two specific elements of this strategy are of interest for this paper:

[First element] The EU continues to work with international partners to advance and promote a global, open, stable and secure cyberspace where international law, in particular the United Nations (UN) Charter, is respected, and the voluntary non-binding norms, rules and principles of responsible state behaviour are adhered to. […]

[Second element, the] EU […] should develop an EU position on the application of international law in cyberspace.

The EU Cyber Direct Research Seminar notably aimed at reflecting on these objectives set by the EU as well as on the two dynamics described above. In that perspective, part of the discussion was designed to provide reflections and recommendations that could then be relevant in discussions of how these objectives could materialise and what could be the next step(s) for the EU as a cyber-diplomatic actor. For these reasons, when approaching the question of the complementarity and possible cross-fertilisation between different branches of international law, we have decided to explore branches in which the EU has developed a rich and successful practice, namely human rights law and international economic law, as well as Internet governance.

Building on these elements, the seminar we organised had a twofold goal:

> To identify issues on which further discussions on the rules and principles of international law could be pursued at the multilateral level or in other fora. Part of the discussion also aimed at identifying in which fora, and with which partners, these discussions should take place.

> To identify potential complementarity, cross-fertilisation and overlaps between the discussion on and implementation of the framework of responsible behaviour and processes concerning other branches of international law.

---

Higher School of Economics), Barrie Sander (Leiden University), Nicholas Tsagourias (University of Sheffield), and Pål Wrange (Stockholm University).


7 Ibid., p. 20 (references and emphasis omitted).
2. Complementarity, cross-fertilisation and overlaps with other branches of international law

The EU and its member states have committed to advancing the framework of responsible behaviour developed by previous GGEs and the OEWG. Their commitment has taken different forms, at the multilateral, regional and national levels. The first panel of the seminar was dedicated to the study of potential complementarity, cross-fertilisation and overlaps between the implementation of the framework of responsible behaviour and several branches of international law that were chosen based on the EU’s priorities as stated in its *Cybersecurity Strategy for the Digital Decade*: targeted measures and international economic law, human rights and Internet governance. The three presentations showed both potential convergence and frictions, and highlighted choices that the EU should be making to implement its *Cybersecurity Strategy* and advance peace and security in cyberspace.

2.1. Targeted measures and international economic law

In order to ensure its digital sovereignty and advance peace and security in cyberspace, the EU has been implementing response and preventive measures to address security threats to its networks and those of EU member states. For example, in July and October 2020, the EU adopted targeted restrictive measures against cyberattacks under the Cyber Diplomacy Toolbox. In the field of 5G, the EU has committed to ensuring supply chain resilience, which could potentially lead to limiting access to the EU market by foreign companies. Giovanna Adinolfi’s paper examines the potential venues for the EU to justify the lawfulness of these measures, especially preventive measures, under international economic and investment law if they were to be contested under the EU’s obligations. Adinolfi shows that although several arguments could be advanced to justify the lawfulness of these measures, existing exceptions tend to be difficult to use, except for those in the most recent bilateral trade agreements.

On this topic, the authors of this paper identify two recommendations for the EU, which are built on the paper of Adinolfi as well as on the discussion we had during the seminar. The first recommendation is strengthening the WTO (World Trade Organization) framework in the digital age: the trends in targeted measures question the ability of the WTO framework to deal with cybersecurity issues. Considering the cybersecurity legislation adopted by the EU, further work should be conducted in the field of international economic law to ensure EU laws’ compliance with it and

---

strengthen the rule of law. The second recommendation is the review of the bilateral trade investments treaties concluded by the EU and its member states to include cybersecurity exceptions.

2.2. Human rights

The promotion and protection of human rights offline and online is at the core of the EU’s international agenda. Barrie Sander’s paper examines the potential role of human rights within ongoing discussions taking place in the First Committee of the General Assembly of the United Nations. Sander argues that while a human rights approach could expand the scope of the framework of responsible behaviour, it is not without drawbacks as it could be used to legitimise human rights restrictions in the cyber domain.

On this topic, the authors of this paper identify three recommendations for the EU, building on the paper prepared by Sander as well as on the discussion during the seminar. The first recommendation is that the EU should engage in a reflection on the most appropriate venue(s) to advance human rights online and develop ad hoc strategies for each potential venue. The second recommendation, based on a human rights approach, is to identify which issues could be addressed within the OEWG while avoiding any possible securitisation and then promote them. As the authors of this paper, we are adding a third recommendation flowing from the key role of non-state actors regarding human rights violation but also respect and protection, which is to advance human rights and businesses’ responsibility in the field of the digital economy.

2.3. Internet governance

The EU is a strong supporter of the multi-stakeholder model for Internet governance. However, as demonstrated by Matthias Kettemann in his presentation, the issue of Internet governance has never been so fragmented and is more and more becoming an issue of national security. According to Kettemann, this results in two trends: a sectoral approach that lacks a global and comprehensive perspective; and a risk for the multi-stakeholder model itself. At the same time, the multiplication of initiatives blurs their

---


10 In his presentation, Kettemann argued that Internet governance had become very segmented (digital economy, human rights instruments, international security) and that it was hard to go beyond this fragmentation and have a comprehensive approach on all issues.
coherence, visibility and impact. This situation could weaken the EU’s discourse on the multi-stakeholder model at a time where numerous states question it.

On this topic, the main recommendation identified by the authors of this paper is to favour existing fora and processes, such as the Internet Governance Forum, to launch new initiatives and thus advance a more comprehensive approach and avoid any duplicative efforts.

3. Advancing the discussions on the rules and principles of international law applicable in cyberspace and their interpretation

The second panel of the seminar had the objective to use the successive GGE and OEWG reports as a starting point and reflect on what may be the next step(s) for the discussions on the interpretation of certain rules and principles of international law. For this panel, we selected three rules and principles of international law on which speakers were invited to provide an input presentation: Vera Rusinova on sovereignty, Duncan B. Hollis on non-intervention and Talita Dias on due diligence. Before diving into the recommendations inferred from the papers and the discussion, there is a series of general recommendations the authors of this paper would like to highlight.

The different processes taking place at the United Nations, namely the GGEs and OEWGs, have been decisive in the (re)affirmation of the applicability of international law to cyberspace. International law remains one of the pillars of the work of the ongoing second OEWG as well as of the proposed Programme of Action (Cyber PoA). Yet we may wonder whether these processes constitute the relevant venue to advance the discussion on the rules and principles of international law. Indeed, these are political processes and international law is only one aspect of their work, together with discussions on the threat landscape, norms of responsible behaviour, confidence-building and capacity-building. In that perspective, we argue that these processes constitute suitable places to discuss the politics of international law, including exchanges of views among states on the interpretation of the rules and principles of international law, on their implementation and capacity-building efforts on the matter, but that may not be relevant in advancing the work on the actual content of the rules and principles.

---

of international law.\textsuperscript{12} On this basis, it would be necessary for states and other actors to dissociate matters linked to the politics of international law from matters relating to the content and implementation of its rules and principles, and to determine what objectives they are seeking in these different categories.

Work and discussions on the content and implementation of the rules and principles of international law should not take place in these political processes. If states want to develop further the work on the content of the rules and principles of international law and how they apply in cyberspace, they should consider referring these matters to more relevant processes. In the short term, a recommendation could be to continue to promote the release by states of their approach on the matter and provide active support as part of capacity-building efforts for other states willing to do so. These different documents could then be used as a starting point for further discussions and efforts to reach similar views. On a longer term and hypothetical perspective, two possible venues could be, for instance, requesting an advisory opinion of the International Court of Justice (ICJ) or referring the matter to the International Law Commission (ILC) of the United Nations.\textsuperscript{13} We are not arguing that states should refer the matters to the ICJ or the ILC; rather we are raising the argument that these may constitute more appropriate venues in cases where states want to have further work on the content of the law. Duncan B. Hollis discusses these possible venues regarding non-intervention in his paper, but for the authors of this paper, his observations can also apply more generally to other rules and principles of international law.

We will now outline the main points of discussion of the three topics discussed on this panel.

### 3.1. Sovereignty

Sovereignty, and its corollaries, is one of the cornerstones of international law. Because of this specific centrality of sovereignty, and the existence of different corollaries, it is sometimes difficult to reconcile the different, if not divergent, approaches. The dawn of cyberspace has added some layers of complexity, notably in challenging the territorial dimension of states and of their activities.

One of the corollaries of sovereignty, states’ territorial sovereignty, is of particular interest in the dynamics of the international law applicable to cyberspace. While states agree on the existence of a general principle of sovereignty, they have divergent opinions on the


rules flowing from that principle and on what may amount to a breach of territorial sovereignty in terms of cyber operations, ranging from the affirmation that territorial sovereignty cannot be breached by a cyber operation to the opposite approach, claiming that any cyber operation penetrating a foreign system or producing effects over it constitutes a violation of sovereignty. The example of territorial sovereignty shows the possible dynamics of a corollary to sovereignty.

Vera Rusinova invited us for a deep dive into different dimensions of the application of sovereignty in cyberspace and how to reconcile them, which led to a very rich discussion with the participants. A key recommendation to be drawn from Rusinova’s paper and the discussion is that the divergence among states’ approaches should be better understood and should not be overestimated, since divergences of views among states on international legal matters are common and are generally solved through state practice. International law is equipped with different mechanisms that will contribute to reconcile these different approaches and solve potential legal interpretative conflicts, namely the peaceful dispute resolution mechanisms. In order to identify possible divergences as well as to work towards possible common approaches, states should continue their capacity-building efforts on legal matters and exchanges of views. This constitutes the second recommendation on sovereignty identified by the authors of this paper.

3.2. Non-intervention

The prohibition of intervention by a state in the affairs of another state is one of the corollaries of states’ sovereignty and received particular attention during the Cold War era. In analysing examples of alleged state-sponsored cyber operations, it can be observed that an important part of them is conducted with the objective to influence, and even to coerce, the targeted state on its internal or external affairs; they are thus likely to constitute prohibited forms of intervention under certain conditions. An important focus of Duncan B. Hollis’ presentation, as well as of the discussion, was the ‘coercive element’, which appears sometimes challenging to characterise regarding cyber operations.

The contours of the prohibition of intervention are relatively well defined, as shown by Hollis, notably because of the number of related cases before the ICJ and other tribunals as well as other international documents. Building on this observation, as well as on the paper prepared by Hollis and the rich discussion during the seminar, the authors of this paper identified that the main recommendation on non-intervention is for states to assess the desirable further development of this principle, either on one of the specific elements such as the ‘coercive element’ or more generally on the interpretation

---

of the principle. **These possible developments are likely to focus on the content of the principle and its implementation.**

### 3.3. Due diligence

Due diligence may be described as a polymorphic standard that adopts different forms depending on the branches of international law concerned. This explains why, in addition to the dedicated presentation by Talita Dias and the subsequent discussion, due diligence has been discussed in relation to other topics during the seminar, notably human rights and international economic law.

Due diligence is an important element of the international law applicable to cyberspace for different reasons, as notably outlined by Dias in her paper. Firstly, it allows us to go behind the politically weighted debates on public attribution. Secondly, due diligence connects international law and domestic law, notably through the adoption of a domestic legal framework allowing states to increase cyber hygiene domestically as well as to comply with their international obligation of diligence. The development of the law of the EU, notably with the adoption of the *Network and Information System Security (NIS) Directive*\(^{15}\) and the *General Data Protection Regulation (GDPR)*\(^{16}\), is to be commended in that perspective.

From these observations, as well as the paper prepared by Dias and the rich discussion during the seminar, the authors of this paper identified a **key recommendation**: it is **important to take into account the plurality of forms of due diligence**. From that starting point, the second recommendation is to identify where it is possible and desirable to develop further the obligation of diligence, in both international and domestic legal frameworks. **The third recommendation would be for the EU to highlight how it is implementing and complying with its obligations flowing from due diligence when adopting and implementing its own regulations**, as already mentioned concerning the NIS Directive and the GDPR. In doing so, the EU would at the same time contribute to the implementation and strengthening of the framework of responsible behaviour and the obligation of due diligence. Finally, **a fourth recommendation could be the elaboration of a document detailing how the EU**

---


implements the obligation of due diligence, which could serve as an example of best practices.

4. Concluding remarks: towards an EU position on the application of international law in cyberspace?

The first EU Cyber Direct Research Seminar aimed at reflecting on the current dynamics on international law and cybersecurity governance as well as identifying possible ways forward. In pursuing this objective, the seminar revolved around two main dimensions, on which the two panels of the discussion were designed.

The first panel aimed at identifying potential complementarity, cross-fertilisation and overlaps between the discussion on and implementation of the framework of responsible behaviour and processes concerning other branches of international law. The discussions showed that the implementation of the framework of responsible behaviour was not without drawbacks and opportunities for other branches of international law. For example, it might be an opportunity to develop human rights law or economic and investment law.

The second panel aimed at reflecting on the discussions and work on international law of the UN-led processes, namely the GGEs and OEWGs, in terms of both content and possible venues. Ultimately, both panels came to the conclusion that other branches of international law could be relevant to developing and implementing the framework of responsible behaviour but that, at the same time, the current forum was not the best place to advance international law obligations. The various papers as well as the discussion during the seminar highlighted that while the OEWG remains the forum to advance questions related to the politics of international law, questions related to the interpretation of rules and principles of international law could hardly be advanced there. If states were willing to advance international law in multilateral fora, it has been argued that it could be preferable to refer these matters to institutions designed to work on legal questions, to obtain some concrete advancements, while keeping a stream of discussion on the politics of international law in the general processes, such as the current OEWG or a potential Cyber PoA.

In the introduction of this paper, we mentioned the 2020 EU Cybersecurity Strategy, and in particular the objective to ‘develop an EU position on the application of international law in cyberspace’. Building on the papers gathered in this publication as well on the discussion during the seminar, the authors of this paper are compiling a series of remarks and recommendations in that perspective.

17 Ibid., p. 20 (references and emphasis omitted).
Of the states having publicly released documents outlining their approach on the application of international law, some are member states of the EU. Despite a certain diversity in the formats of these documents, they generally show a high level of convergence among the released approaches by the member states. From this observation, one may wonder what the next step for the EU and its member states could be. Apart from publishing its own views on the application of international law to states’ conduct in cyberspace, a different path for the EU would be to show how the diversity of documents published by its member states is not challenging their capacity to collectively cooperate as well as promote and implement the rules and principles of international law in cyberspace. The authors of this paper recommend pursuing this second path. In that perspective, the action of the EU could first focus on supporting the effort of member states to define and publicly release their views on the application of international law to cyberspace, as well as on fostering the exchange of good practice and the development of joint capacity-building efforts.

Such an approach would then be beneficial for the collaboration with states outside of the EU and more generally for international discussions on the politics of international law taking place in multilateral fora. It would demonstrate the ability of the EU and its member states to navigate different approaches and that the adoption of a common approach, either at the European or at the multilateral levels, is not a prerequisite.

In some cases, the divergence of views could lead to dispute among states. Yet, as already noted, international law is equipped with peaceful dispute resolution mechanisms and the EU could, in exposing its approach to these matters, highlight the usefulness and relevance of these mechanisms.

Finally, these efforts could be complemented with the publication of a repository of best practice of the EU and its member states on the international law applicable to cyberspace and its implementation.

This edited publication consists of five papers offering more in-depth views on the matters discussed during the seminar and in this introduction. Firstly, Giovanna Adinolfi discusses international economic law and possible unilateral measures to be adopted by states in reaction to cyber operations. Secondly, Barrie Sander examines the existing and potential role of human rights within ongoing discussions on the international law applicable to cyber operations taking place at the United Nations. Thirdly, Vera Rusinova discusses the application of sovereignty in cyberspace and its different interpretations. Fourthly, Duncan Hollis examines the prohibition of intervention. Finally, Talita Dias navigates the different dimensions of due diligence in cyberspace.

18 Namely Czech Republic, Estonia, Finland, France, Germany, Italy, Netherlands, Romania.
1. Introduction

States do not overlook the role that could be played by economic measures in opposing harmful cyberattacks originating in foreign countries. These measures can be classified into two categories. On the one hand, we observe response measures addressed against those held responsible (e.g. a foreign state, its agencies and/or nationals) for cyber operations that have already been launched and have caused an injury, such as the interruption or malfunctioning of information systems and critical infrastructures, the cancellation or alteration of digital data, or the interception of non-public digital data. Reference can here be made, for instance, to the travel bans and freezing of assets introduced by the EU since 2019 against foreign citizens and entities deemed to be involved in significant cyberattacks against the EU and its member states.\(^{19}\)

On the other hand, anticipatory or preventive measures are discernible. Their intent is to reduce the risk of being the target of cyberattacks, preventing them at the origin. The aim of lowering vulnerability of national information and communication systems to hostile cyber operations originating from outside is pursued by prohibiting (or subjecting to specific conditions) commercial or investment operations in the domestic market by foreign information technology (IT) companies. A good illustration is the US measures adopted since 2018 banning the use of equipment and services produced or supplied by some Chinese state-owned or state-directed companies, including Huawei, which, according to the US, could strengthen the ability of foreign entities to exploit the vulnerabilities of the US communication and information systems and thus to commit malicious cyberattacks.\(^{20}\) A further example is the use of the so-called ‘golden powers’ by governmental authorities to deny the authorisation or to impose conditions on investments, or on the conclusion of commercial deals by foreign IT equipment and services suppliers.\(^{21}\)

Against this background, international economic law deserves specific attention, since the use of either response or preventive measures to counter cyberattacks could be

---

\(^{19}\) See Council decision (CFSP) 2019/797 and Regulation (EU) 2019/796, OJ L 129 I (17 May 2019), respectively, 1 and 13. The persons and entities harmed by the EU are listed in an annex to the two acts.

\(^{20}\) For an overview, see Federal Communications Commission, Notice of Proposed Rulemaking and Notice of Inquiry, 17 June 2021, FCC 21-73.

inconsistent with obligations states have accepted in their mutual economic relations, triggering their international responsibility for internationally wrongful acts.

2. The legitimacy of response measures

Response measures can be appraised according to the customary rules of international law as codified by the Draft Articles on the Responsibility of States for Internationally Wrongful Acts, adopted in 2001 by the International Law Commission of the United Nations. It is generally accepted that injured states may resort to measures of self-help, i.e. acts of retorsion and countermeasures. Retorsions are defined as unfriendly but lawful acts expressing disagreement with the conduct of another state; the notion of countermeasures covers unlawful behaviours aiming at persuading a wrongdoing state to cease the unlawful act (if continuing) and to provide both guarantees of non-repetition and reparation of the material and moral injuries.

The legitimacy of measures of retorsion, even as a response to hostile but lawful cyberoperations, does not raise substantive concerns, to the extent the measures are not inconsistent with general or treaty rules applicable between the parties concerned. This may be the case for the measures enacted in 2021 by the US Treasury prohibiting domestic financial institutions from lending funds to, or from purchasing on the primary markets bonds issued by, the Central Bank, the Ministry of Finance and the National Wealth Fund of the Russian Federation. Indeed, the restrictions on capital outflows implied by these measures do not infringe any prescriptive customary or treaty rules, including the obligations accepted by the US on trade in financial services under the General Agreement on Trade in Services (GATS) of the World Trade Organization (WTO). Indeed, the GATS sets out market access obligations in favour of foreign services suppliers (e.g. Russian financial institutions wishing to enter and operate in the US financial market), not in favour of foreign consumers (such as the targeted Russian authorities).

---

24 A wide and comprehensive analysis of the unlawfulness of cyberattacks according to primary rules of international law is offered by François Delerue, Cyber Operations and International Law (Cambridge: Cambridge University Press, 2020). In particular, see p. 193 ff., where the author tests the lawfulness of cross-border cyberattacks against international human rights law and the principles of territorial sovereignty and non-interference in internal affairs.
26 This conclusion is supported by analysis of the US commitments on trade in financial services under the relevant modes of supply, as set out in the Schedule of Specific Commitments annexed by the US to the GATS (WTO doc. GATS/SC/90/Supp.3, 26 February 1998), the WTO Understanding on the Commitments in Financial Services, accepted by the United States (ibid.), and the
Moving to countermeasures, even though states’ responses to cyberattacks have hardly been described in these terms, the use by a victim state of an internationally unlawful cyberattack cannot be excluded. Although the 2021 Report of the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security did not reach a consensus on this point, this view was formulated by several states in their individual considerations. As is well known, lawful countermeasures must respond to specific substantive conditions. In particular, they can be taken by an injured state in response to an international unlawful act of another state and addressed against that state; their purpose is to force the wrongdoing state to comply with the obligations arising under the law of international responsibility; further, countermeasures have to be reversible (as far as possible) and commensurate with the injury suffered, in accordance with the principle of proportionality; finally, they must not affect obligations on the protection of fundamental human rights, arising under peremptory norms of international law or under rules of humanitarian character prohibiting reprisals.

The above-mentioned freezing of the assets introduced by the EU since 2019 can be gauged against this background. As a premise, it is worth underlining that even though secondary EU law on the fight against cyberattacks expressly excludes that the application of restrictive measures against individuals or entities amounts to an attribution of responsibility to a third state, a presumption in this direction could be supposed when these measures are addressed against persons who hold a public position in a third state, as officers of the armed forces or military intelligence, or against entities that are part of the institutional organisation of a third state.

Unlike the previous examples of retortions, it cannot be excluded that that the freezing of assets amounts to a violation of the right to property established under international human rights treaty law or of the rules of international customary law on the treatment of aliens and their assets. However, some considerations help to better frame it under the law on international responsibility. First, the freezing of assets provided for by the...
EU is reversible, as it does not deprive the affected individuals or entities of the property over the targeted items. Furthermore, taking into account the pursued aim, the proportionality requirement under the ILC Draft Articles could be met when the restrictive measure is addressed against persons or entities whose involvement in a wrongful cyber operation can be substantiated by conclusive evidence. It is worth considering that the right to property can hardly be regarded as a ‘fundamental’ human right, considering also that, under human rights treaties, it can be subject to limitations when necessary to pursue objectives of public interest. Finally, the restrictions imposed by the EU are not absolute, since the freezing may be derogated for the satisfaction of the basic needs of the affected persons, when the targeted assets are subject to arbitral, administrative or judicial decisions rendered prior to listing, or to make payments under contracts concluded before listing.

3. The legitimacy of preventive measures

As mentioned above, states rely on economic measures also to prevent transnational malicious cyber operations by precluding foreign companies from making a direct investment in their territory or from entering their markets to conclude commercial transactions for the supply of goods or services. Considering the extensive obligations under trade and investment agreements, these measures have raised several concerns. For instance, within the WTO China has voiced criticisms regarding the legitimacy of measures enacted by Australia, Sweden and the US de jure or de facto prohibiting Chinese companies from entering the public procurement market for information and communications technology (ICT) products or from participating in the construction of national 5G networks. At the same time, domestic measures affecting foreign

14 According to Regulation (EU) 2019/976, the freezing of assets prevents any use of funds and economic resources (art. 1, para. 8(e)–(f)). The full enjoyment of the right to property is re-established by the ‘delisting’ of the targeted individuals and entities.

15 According to the preamble to Regulation (EU) 2019/796, the purpose of the restrictive measures is to respond to cyberattacks with a significant effect on the EU and its members. See the definition of ‘significant effect’ provided in art. 2 of the Regulation. The argument that the proportionality of countermeasures must be assessed according to the aim sought has been explored by Enzo Cannizzaro, ‘The Role of Proportionality in the Law of International Countermeasures’, *EJIL*, vol. 12, no. 5 (2001), 889–916: 889.


17 In its commentary on art. 50 of the 2001 Draft Articles, the ILC identifies ‘fundamental human rights’, also referring to the rules of human rights treaties that isolate certain human rights that cannot be derogated from even in time of war or other public emergency: the right to property is not among them. See ILC Draft Articles, 132, para. 6, and Matthew Happold, ‘Targeted Sanctions and Human Rights’, in *Economic Sanctions and International Law*, ed. Matthew Happold and Paul Eden (Oxford: Hart, 2016), pp. 87, 94.

18 For our purposes, see art. 17, para. 1 of the EU Charter of Fundamental Rights.


20 See WTO docs G/C/M/133, sec. 32; G/C/M/135, sec. 25; G/C/M/136, secs 16–18; G/C/M/137, sec. 28; G/C/M/138, sec. 40; G/C/M/139, secs 13 and 38; G/C/M/140, sec. 36. The challenged US measures also concern restrictions on the exportation of ICT products. See also Shin-yi Peng, ‘Cybersecurity Threats and the WTO National Security Exceptions’, *Journal of International Economic Law*, vol. 18, no. 2 (2015), pp. 449–478: 449.
investments in the telecommunication sector have been challenged before investment tribunals.\textsuperscript{41}

In summary, depending on their specific features, preventive trade measures could amount to a violation of WTO law. Their illegitimacy could be affirmed on the basis of the prohibition of import restrictions established under art. XI of the WTO General Agreement on Tariffs and Trade (GATT) and of the obligations not to discriminate according to art. I and art. III GATT.\textsuperscript{42} Similar complaints could be raised under the WTO agreements on trade in services and on public procurement, should the preventive measure foreclose, respectively, the supply of foreign telecommunication services and the participation by foreign companies in public tenders for the supply of IT goods and services.\textsuperscript{43} Regarding international investment law, restrictions on the entry of foreign companies into the domestic ICT market could be inconsistent with entry requirements set out under bilateral investment treaties (BITs); likewise, it could be claimed that the exclusion of already established foreign investors from the construction of ICT networks and infrastructures amounts to the violation of BIT standards of protection on non-discrimination and fair and equitable treatment.\textsuperscript{44}

A comprehensive analysis of these measures under WTO law and BITs is beyond the scope of the present contribution. Rather, the following remarks delve into the arguments that could be invoked to justify them under the relevant treaty regimes. In particular, the reference is to the so-called security exception clauses included in most trade and investment agreements.

### 3.1 Security exception under international trade law

Under the multilateral trading regime, security reasons can be invoked to justify deviations from substantive discipline prescribed by the WTO agreements. In particular, the GATT does not prevent WTO members from embarking on any action they consider necessary to protect their ‘essential security interests’ relating to fissionable materials (art. XXI(b)(i)), the traffic in war materials and other goods carried out ‘for the purpose of supplying a military establishment’ (art. XXI(b)(ii)), or taken ‘in time of war or other


\textsuperscript{43} Ibid., pp. 359, 562 and 557.

\textsuperscript{44} On the scope of these standards, see Jeswald W. Salacuse, \textit{The Law of Investment Treaties}, 3rd ed. (Oxford: Oxford University Press, 2021), pp. 266 and 273.
emergency in international relations’ (art. XXI(b)(iii)). For almost 70 years this provision was rarely used as a defence before dispute settlement organs, and in no case was its interpretation the object of jurisdictional scrutiny. However, two recent WTO panels were mandated to settle disputes according to art. XXI(b)(iii). Even though this case law did not concern cybersecurity issues, it is particularly relevant for our purposes: indeed, national security reasons have been cited to exclude any possible discussion within the WTO on cyber-related restrictive trade measures.

As a premise, the two WTO panels held that, notwithstanding their text, WTO security exceptions are not self-judging. In Russia – Traffic in Transit, the panel emphasised that the terms ‘which it considers’ under art. XXI(b) must be understood in strict connection with the three sets of circumstances identified in the following subparagraphs (i) to (iii). Since the existence of these circumstances can be assessed in the light of objective criteria, they ‘qualify and limit the exercise of the discretion accorded to Members’. Against this background, the arguments whereby the WTO has no mandate to discuss the security interests that underpin cyber-related trade measures can be easily rejected: any justification under art. XXI is fully justiciable, and compliance with the requirements set out therein unquestionably comes under the jurisdiction of the dispute settlement organs.

A second issue to be explored is whether cybersecurity may be understood as a ‘security interest’ under art. XXI. In the case law under consideration, it was excluded that any security interests deserve protection under the WTO. Indeed, the panels asserted that ‘essential security interests’ are ‘a narrower concept than “security interests”’, generally referring to interests ‘relating to the quintessential functions of the state, namely, the protection of its territory and its population from external threats, and the maintenance of law and public order internally’. However, the panel in Russia – Traffic in Transit decided to formulate neither a list of ‘essential security interests’ nor a more detailed definition. After acknowledging the discretion of WTO members to identify their essential security concerns, and that these concerns may vary in time and space, it preferred to ground its arguments on the obligation of good faith in the interpretation and application of international treaties. Accordingly, the panel argued, on the one hand, that essential interests must not be invoked with the purpose of circumventing obligations

---

45 Similar provisions may be found in art. XIV bis GATS, art. 73 of the WTO Agreement on the Trade-Related Aspects of Intellectual Property Rights (TRIPs), and art. III:1 of the WTO Agreement on Government Procurement.
46 Russia – Measures Concerning Traffic in Transit, Panel Report, WT/DS512/R, adopted on 26 April 2019 (hereafter Russia – Traffic in Transit). The conclusions of this panel were confirmed in Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights, Panel Report, WT/DS567/R; however, this panel report was appealed before the WTO Appellate Body, and its adoption was therefore suspended.
47 See WTO doc. G/C/M/135, para. 25.6; G/C/M/136, paras 17.4 and 18.3; G/C/M/137, para. 28.9; G/C/M/138, para. 40.5. in general, see the positions of Russia and the US in the panel reports mentioned above, fn 28.
48 See art. XXI(b) GATT: ‘Nothing in this Agreement shall be construed ... to prevent any [WTO Member] from taking any action which it considers necessary for the protection of its essential security interests’ (emphasis added).
49 Russia – Traffic in Transit, para. 7.65.
50 Ibid., para. 7.130.
51 Ibid., para. 7.131.
under the GATT, and that the more the circumstances mentioned in art. XXI(b)(i)–(iii) can be ascertained, the easier it will be to consider the raised security interest as ‘essential’. On the other hand, the good faith obligation requires that ‘the measures at issue meet a minimum requirement of plausibility in relation to the proffered essential security interests, i.e. that they are not implausible as measures protective of these interests’.

Under this logic, nothing precludes a priori that concerns that are not strictly military, including cybersecurity, be deemed as a security interest, especially when we consider that the security threats and vulnerabilities states are exposed to have been widening in recent decades. Rather, the issue is whether cybersecurity is an ‘essential’ security interest. While this can be affirmed when the protection of military assets and information systems is at stake, cybersecurity matters could also relate to the protection of ‘civil’ infrastructures. This could be particularly true for infrastructures whose operativity relies on ICT (e.g. transport, energy and telecommunication networks, electoral and health systems), and which store sensitive non-public data or whose alteration or destruction may endanger the proper functioning of social and economic life within a state. Coherently with the panel report in *Russia – Traffic in Transit*, the vulnerabilities of these infrastructures cannot be invoked to veil protectionist or discriminatory intents (i.e. to exclude foreign competitors from the domestic market to the benefit of national businesses), but the more cyber-threats arise within the context of a war or an emergency in international relations under art. XXI(b)(iii), the easier it will be to establish that the protection of an essential security interest is at stake. Should this test be passed, restrictions on the sale of foreign goods or services that could pave the way to harmful cyber-intrusions could easily have a ‘plausible link’ with essential security interests.

Ultimately, the critical question is whether a situation of war or another emergency in international relations occurs when measures aiming at preventing harmful cyber operations are implemented. In *Russia – Traffic in Transit*, ‘war’ was meant to refer to an ‘armed conflict’, which may occur between states, between governmental forces and private armed groups, or between such groups within the same state. The category of ‘emergency in international relations’ indicates, besides war, ‘a situation of ... latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state’, giving rise to ‘particular types of interests for the Member in question, i.e. defence or military interests, or maintenance of law and public order interests’. Therefore, art. XXI applies where cyber-related trade restrictions are adopted in time of war or another emergency in international relations, even when these situations

---

52 Ibid., para. 7.133.
53 Ibid., para. 7.135.
54 Ibid., para. 7.138.
56 *Russia – Traffic in Transit*, para. 7.72.
57 Ibid., para. 7.76.
result from coordinated cyberattacks or systemic use of cyber-weapons. However, the issue is also whether cyber-threats constitute per se an emergency in international relations justifying the invocation of art. XXI GATT as a defence for preventive, not remedial, trade restrictions. If political or economic differences between states are not sufficient, in themselves, to constitute an emergency, except in the case of striking tensions, the threshold to justify measures intended to prevent cyberattacks is set very high, as what must be objectively observed is a situation of breakdown of law and public order in the invoking member (or in its immediate surroundings). Hence, the justification under art. XXI GATT of trade measures aimed at reducing a state’s vulnerability to foreign cyberattacks is conditional on the fulfilment of strict requirements.

It should be remembered that the text of art. XXI GATT was agreed upon in 1947. Hence it does not mirror the current challenges states are exposed to in their international relations. During the negotiations for the WTO agreements between 1986 and 1994, no amendment of the GATT security exception was discussed; rather, states agreed to mostly replicate it in other WTO agreements.

However, some interesting evolutions can be observed in the trade agreements concluded more recently on a preferential basis. Indeed, they give evidence of states’ growing awareness of cybersecurity issues. In some cases, the scope of the security exception has been expanded, opening the possibility to legitimately invoke it as a justification for the measures here at issue. For instance, the provision of the EU–Singapore free trade agreement corresponding to art. XXI(b)(iii) GATT covers also measures taken to ‘protect critical public infrastructure (this relates to communications, power or water infrastructure providing essential goods or services to the general public) from deliberate attempts to disable or disrupt it’ (art. 16.11(b)(iv). Similarly, art. 17.13(b)(iii) of the Regional Comprehensive Economic Partnership Agreement expressly authorises the adoption of measures to protect critical infrastructures of public interest, ‘including communications, power, and water infrastructures’. Finally, states participating in the Comprehensive and Progressive Agreement for a Trans-Pacific Partnership have agreed on vague language, whereby the security exception applies to measures simply considered necessary for the protection of essential security interests (art. 29.2(b)): in contrast to art. XXI GATT, it is not required that these measures be

59 Russia – Traffic in Transit, para. 7.75.
60 Ibid., para. 7.135.
64 The text of the CPTPP is available at https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/tpp-text-and-associated-documents.aspx. The same text may be found in art. 32.2(b) of the United States–Canada–Mexico Agreement effective as from June 2020 (see https://ustr.gov/trade-agreements/free-trade-agreements/united-states-canada-mexico-agreement).
applied in time of war or other emergency in international relations. In conclusion, these normative approaches imply a higher deference towards states’ policy decisions, albeit to different degrees. However, while offering a higher protection to security concerns and better suited to cope with the new security challenges articulated by states, in principle these new texts could open the door for an abusive reliance on the exception, hiding protectionist or discriminatory intents behind security concerns.

3.2 Possible justifications of ‘preventive’ measures under international investment law

States pursue cybersecurity interests also through preventive measures affecting investments, either preventing the establishment of foreign investors in the domestic ICT sector or banning them, once established, from participating in public tenders or concluding commercial contracts for the supply of ICT equipment and services. In this case, international responsibility issues may arise for the violation of obligations established under treaties on the promotion and protection of foreign investments. This circumstance opens the possibility for the harmed foreign investor to bring a claim before international investment tribunals alleging the infringement of the BIT clauses on the establishment of foreign investment, fair and equitable treatment, full protection and security or non-discrimination. Here again, the purpose is not to assess the content of these clauses and in which circumstances cyber-related measures could be at odds with them. Rather, the following analysis will focus on the possible alternatives that could be exploited by the host state to avoid its international responsibility for an unlawful act and, thereby, to not be subject to any duty of reparation of the damages suffered by the foreign investor. As a premise, it is worth emphasising the high degree of fragmentation of international investment law. Indeed, lacking a universal treaty, the topic is mostly ruled by investment treaties concluded on a bilateral or plurilateral basis, which nevertheless share some common features.

In general, measures precluding the entry of foreign investors might be covered by carve-out clauses, whereby the parties to a BIT agree on excluding some sectors from the scope of the agreement. This technique could be particularly relevant in case of BITs granting foreign investors a right of admission, based in most cases on a national treatment clause extending to foreign investors the treatment accorded to national investors for the establishment or acquisition of an economic activity. Closing to foreign investments

65 These allegations were put forward before two ICSID tribunals in Global Telecom Holding SAE v. Canada and Huawei Technologies Co., Ltd. v. Kingdom of Sweden, fn 23 above.
66 See Eric de Brabandere, International Investment Law, fn 23 above, 14 ff.
67 See for instance art. 3.1 of the 2012 US Model BIT, https://investmentpolicy.unctad.org/international-investment-agreements/model-agreements. Provisions on the admission of foreign investments are not established in all BITs. Under an alternative model, usually resorted to by European states, admission or establishment is granted only to the extent it is foreseen by national legislation. In this circumstance, bans on foreign investments would be lawful and the host state enjoys a large degree
critical sectors particularly exposed to cyber vulnerabilities could be a means to reserve this activity to domestic producers, at least mitigating the possibility of transnational harmful cyberattacks, albeit at the cost of not benefiting from capital inflows from third countries and the technology transfer that might be associated with it.68

Under a less restrictive approach, an alternative could be to include specific treaty language, whereby states would retain the right to exercise the powers established under their respective national laws and regulations on security matters. This approach has been adopted under the EU–Japan Economic Partnership Agreement, where Japan has reserved the right to conduct the screening of foreign investments in some sectors (e.g. heat supply, telecommunication services, medicines production, water supply or railway services) for the purposes of ascertaining whether they would cause a ‘situation in which national security is impaired, the maintenance of public order is disturbed, or the protection of public safety is hindered’.69 Likewise, under the same agreement Italy has retained the exercise of its ‘special powers’ (including the right to veto or to impose specific conditions) for security and public interest purposes with respect to acts or transactions involving strategic assets in the areas of energy, transport and telecommunication.70

Finally, breaches of the standards of protection of foreign investments may be justified under the security exception clause, when this is provided for in the BIT. In some instances, this clause is specifically tailored to cybersecurity vulnerabilities, as observed under trade agreements. For example, art. 33, para. 1(ii)(d) of the 2015 Norway Model BIT preserves the parties’ right to take any action they consider necessary ‘to protect critical public infrastructure including communication, power and water infrastructures from deliberate attempts intended to disable or degrade such infrastructure’.71

In other BITs, security clauses are formulated in vague terms, granting the right to exercise enough leeway for the protection of the parties’ security concerns. However, similarly to art. XXI GATT, these clauses may raise interpretative issues pertaining to their self-judging nature, their reviewability before an investment tribunal and the identification of the circumstances where they can be legitimately relied on by the host state. The arbitral awards on the measures adopted by Argentina in the 2000s to address its economic and financial crisis have extensively explored these issues, in some instances reaching conflicting solutions.72 Similar matters have been discussed in two more recent claims brought against India involving foreign investments in the telecommunication sector of discretion in reserving the construction and management of critical infrastructures to domestic investors.

68 Alternatively, states may decide to agree that commitments on admission are not subject to the investor–state dispute settlement mechanism. Accordingly, any infringements of the right of admission would be subject exclusively to the jurisdiction of the national tribunal of the wrongdoing state. This choice has been made under the Comprehensive Economic and Partnership Agreement between the EU and Canada, OJ L 11 (14 January 2017), 23, art. 8.18, para. 1.
69 See the Japanese schedule included in Annex 8-B to the Agreement, in OJ L 330 (27 December 2018), 757 ff.
70 Ibid., 786.
71 Available at https://investmentpolicy.unctad.org/international-investment-agreements/model-agreements.
sector. Here, the relevant BIT security exception was not formulated as a self-judging clause. Nevertheless, the tribunals pointed out that a margin of deference has to be granted to the host state to determine what its security interests are and whether they are ‘essential’. This would imply a higher burden of proof on the foreign investor alleging a violation of the BIT at issue, but also the need to avoid the substantive standards of protection being rendered ‘wholly nugatory’. In short, this case law helps us to acknowledge that, as observed for trade law, the invocation of general security exceptions established under international investment law can eventually be demanding. More tailored rule-making solutions would be better suited to provide states with leeway to preventively counter malicious foreign cyberattacks.

4. Conclusions

While states do not overlook the importance of economic measures to respond to or to prevent harmful cyberattacks, the legitimacy of this practice raises several doubts under international economic law. This contribution has first scrutinised some response measures, through the lens of the customary rules on the responsibility of states for internationally wrongful acts. While the retorsions considered are not critical under international trade law, the same could not be said for countermeasures implying a violation of the right to property enjoyed by the targeted individuals or entities. However, the customary requirements set out in the 2001 ILC Draft Articles can be satisfied, albeit under some specific conditions (primarily, the existence of conclusive evidence on involvement in wrongful cyberoperations).

Moving to preventive measures, their inconsistency with substantive obligations established under trade or investment agreements calls into question the scope of so-called ‘security exceptions’, where an equilibrium is crystallised between the pursuit of the objectives of trade liberalisation and investment promotion and protection, on the one hand, and the achievement of collective security interests on the other. Against this background, the degree of flexibility enjoyed by states to achieve cybersecurity interests by trade restrictions or the violation of commitments on admission and protection of foreign investments depends on the deference reserved to their policy decisions and the substantive conditions whose fulfilment is necessary in order to legitimately invoke security reasons. Albeit limited, the case law that has developed to date under both WTO law and investment law highlights some constrictions that could restrain states’ margin of manoeuvre. In this regard, interesting evolutions can be observed in some recent preferential trade agreements and investment treaties and models. An extensive

---

73 CC/Devas (Mauritius) Ltd et al. v. India, PCA case No. 2013-09, Award on Jurisdiction and Merits (25 July 2016) and Deutsche Telekom v. India, PCA case No. 2014-10, Interim Award (13 December 2017).
74 CC/Devas (Mauritius) Ltd et al. v. India, fn 55 above, para. 245.
75 Deutsche Telekom v. India, fn 55 above, para. 238. Also on this basis, the Tribunal reached the conclusion that the relevant security exception clause did not cover non-military interests.
application of this practice by the EU and in other regional contexts, in the relations between states representing diverse economic and political systems, could be conducive to a clearer delimitation of the legitimate boundaries between economic and cyber-related interests, and, it is hoped, to an open and frank debate on these issues within multilateral economic institutions and fora.
1. Introduction

This paper examines the existing and potential role of human rights within ongoing discussions on the international law applicable to cyber operations taking place within the UN General Assembly First Committee. For this purpose, the paper is structured in four parts.

> It begins by clarifying the meaning of human rights (Section 2).
> It then turns to explore the extent to which the First Committee has already engaged with human rights, with a particular focus on the work of the UN Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) (Section 3).
> Next, the paper examines the potential for the First Committee to engage with human rights in the future (Section 4). It argues that the First Committee has to date devoted minimal attention to human rights in its discussion of the applicability of international law to cyber operations, an approach that represents a missed opportunity given the pervasive relevance of human rights to the cyber threat landscape, various concepts of international law, and accountability and participation processes in the cyber governance context.
> Finally, the paper outlines some of the risks of centring human rights within the discussions of the First Committee, in particular the potential co-option of the language of human rights to legitimate repressive state practices under the banner of addressing different types of perceived threats at the intersection of international security and the cyber domain (Section 5).

2. Human rights defined: obligations, responsibilities and principles

For the purposes of this paper, human rights are understood as a set of obligations, responsibilities, and principles.\(^76\)

Human rights obligations: Human rights law (HRL) comprises a set of obligations on states rooted in both international treaty law and customary international law. Pursuant to HRL, states are subject to ‘negative’ obligations to respect human rights, i.e. to refrain from taking any measures that result in the violation of a given right. In addition, states are subject to ‘positive’ obligations to protect human rights, i.e. to take reasonable measures to ensure that persons within their jurisdiction do not suffer from human rights violations brought about by third parties or broad phenomena such as preventable environmental catastrophes, and to fulfil human rights, i.e. to take positive steps to bring about the effective enjoyment of human rights.

Human rights responsibilities: As Nehal Bhuta has noted, at their inception, human rights treaties took for granted the so-called ‘Westphalian frame’, presupposing that the legal framework for the realisation of human rights ‘depended upon and was expected to act through functioning political communities organized as sovereign states’. In recent decades, moves have been made to subject certain non-state actors to human rights responsibilities. Pursuant to the United Nations’ Guiding Principles on Business and Human Rights (UNGPs), in particular, business actors are subject to a corporate responsibility to respect human rights by avoiding infringing on the human rights of others and addressing adverse human rights impacts with which they are involved. This responsibility constitutes a non-binding ‘global standard of expected conduct’ applicable to business enterprises, which exists independently of states’ abilities and/or willingness to adhere to their human rights obligations.

Human rights principles: Viewing human rights through the prism of a ‘human-rights-based approach’, it is also possible to identify a number of principles that perveade the human rights enterprise. According to Land and Aronson, for example, these norms and principles include ‘universality/inalienability, indivisibility, interdependence/interrelatedness, equality and nondiscrimination, participation/inclusion, and accountability/rule of law’. Although there may be a temptation to view human rights as a commonly defined set of obligations, responsibilities and principles, it is important to emphasise that in practice human rights also tend to be dynamic and fluid. As Balakrishnan Rajagopal has observed, human rights is ‘a language ... of hegemony and counter-hegemony, and we need to recognise the multiple uses to which it is put and the fact that it is a terrain of

---

80 Ibid., Commentary to Principle 11.
contestation... for multiple deployments of power and resistance’. Discussions relating to human rights in the cyber domain, in particular, are evolving as existing sources are interpreted in a new context by a diversity of actors within the field.

3. Human rights deferred: the current role of human rights in the work of the UN General Assembly First Committee

In the most recent consensus report of the UNGGE and the final substantive report of the OEWG, human rights received minimal attention.

The UNGGE's 2021 report confirms that respect for human rights and fundamental freedoms remains ‘central’ to the promotion of information and communication technologies (ICTs) for peaceful purposes. The report also acknowledges that respect for and observance of human rights promotes ‘an open, secure, stable, accessible and peaceful ICT environment’, and that ICT vulnerabilities may pose a risk to human rights and fundamental freedoms.

Against this background, the UNGGE’s 2021 report reaffirms Norm 13(e)—initially recommended within the UNGGE's 2015 consensus report—which provides that states should respect particular Human Rights Council resolutions on the promotion, protection and enjoyment of human rights on the Internet, as well as particular General Assembly resolutions on the right to privacy in the digital age. With respect to this norm, the 2021 report explains that special attention should be placed on the right to freedom of expression and that observance of this norm can contribute to promoting non-discrimination and narrowing the digital divide, including with respect to gender. The report also draws attention to the especially negative impacts of arbitrary or unlawful mass surveillance on human rights, particularly the right to privacy.

In terms of implementing Norm 13(e), the UNGGE’s 2021 report invites states to consider specific guidance in relevant resolutions of the Human Rights Council and General Assembly and to advance new resolutions in light of ongoing developments in the field. The report also invites states to consider investing in and advancing ‘technical and legal measures’ to guide the development and use of ICTs in a human-rights-compliant manner, takes note of ‘dedicated fora’ within the UN that specifically address human

---

83 UNGGE Report (2021), para. 5.
84 Ibid., para. 39.
85 Ibid., para. 62.
86 Ibid., para. 36.
87 Ibid., para. 37.
88 Ibid., para. 38.
rights issues, and acknowledges the importance of engaging with the variety of stakeholders that contribute to the protection and promotion of human rights online.  

Finally, the UNGGE’s 2021 report also expressly reaffirms the commitments of states under international law to respect human rights and fundamental freedoms. In this regard, it is notable that the report reaffirms the assessments and recommendations on international law of the reports of previous UNGGEs, which include the confirmation in the UNGGE’s 2015 report that ‘States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms’.  

Turning to the final substantive report of the OEWG, the report opens by reaffirming states’ ‘faith in fundamental human rights’, acknowledging that developments in ICTs have implications for all three pillars of the UN’s work, including the human rights pillar, and emphasising that negative trends in the digital domain could ‘hinder the full enjoyment of human rights and fundamental freedoms’. The report also notes that states are increasingly concerned about the implications of the malicious use of ICTs for human rights. Yet, beyond these background references, the only other mention of human rights in the report is an acknowledgement that capacity-building ‘should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory’.  

What emerges from this brief overview of the recent work of the First Committee on the international law applicable to cyber operations is a sense that human rights are considered as merely a background issue—the general approach being one of deference to other fora more specialised in human rights within the UN, such as the Human Rights Council.  

In this regard, it is clear that other fora within the UN are devoting significant attention to the application of human rights in the cyber domain. Examples include:

> resolutions of the Human Rights Council on the Internet, new and emerging digital technologies, freedom of expression, the right to privacy, and peaceful protests;
> reports by Special Rapporteurs on the right to privacy,101 freedom of expression,102 freedom of association and assembly,103 violence against women,104 and racism;105

> reports by the Office of the High Commissioner on Human Rights on the right to privacy, freedom of assembly and peaceful protests, and artificial intelligence,106 as well as those produced as part of the B-Tech Project, which provides guidance for implementing the UNGPs in the technology space;107

> the ongoing work of human rights treaty bodies, including, for example, a new General Comment on children’s rights in relation to the digital environment.108

While this work is important, the apparent reluctance of the UN General Assembly First Committee to engage with human rights represents a missed opportunity given the clear and direct relevance of human rights to its mandate. In particular, the general assumption that human rights should be left for specialised fora represents a somewhat siloed perspective which negates sustained reflection of the pervasive relevance of human rights to questions of international security in the cyber domain.

4. Human rights recognised: the potential role of human rights in the work of the UN General Assembly First Committee

Human rights obligations, responsibilities and principles are relevant to the work of the UN General Assembly First Committee on the application of international law to the cyber domain in at least three respects:109 first, human rights offer an important frame for identifying and addressing several of the cyber threats identified by the UNGGE and OEWG; second, human rights are relevant to the interpretation of a number of international law concepts recognised and/or discussed by the First Committee in its work on the cyber domain; and finally, the human rights principles of participation/inclusion and accountability/rule of law are also of particular importance to the future orientation of the work of the First Committee in this context.

101 The reports are accessible here: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx
102 The reports are accessible here: https://www.ohchr.org/en/issues/freedomopinion/pages/annual.aspx
103 See, in particular, A/HRC/47/24/Add. 2 (on ending Internet shutdown).
104 See, in particular, A/HRC/38/47 (on online violence against women and girls).
105 See, in particular, A/HRC/44/57 (on racial discrimination in the design and use of emerging digital technologies), A/75/590 (on the discriminatory impact of emerging digital technologies on migrants, stateless persons, refugees and other non-citizens) and A/HRC/48/76 (on digital technologies deployed to advance xenophobic and racially discriminatory treatment and exclusion of migrants, refugees, and stateless persons).
106 The reports are accessible here: https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalReports.aspx
107 The resources are accessible here: https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx
4.1. Human rights and the cyber threat landscape

Both the UNGGE and OEWG reports identify a range of existing and potential threats posed by the malicious use of ICTs for the maintenance of international peace and security.\textsuperscript{110} Yet, while important references are made to ‘economic development and livelihoods, and ultimately the safety and wellbeing of individuals’,\textsuperscript{111} as well as the fact that threats may have ‘a different impact on different groups and entities, including on youth, the elderly, women and men, people who are vulnerable, particular professions, small and medium-sized enterprises, and others’,\textsuperscript{112} there is a noticeable lack of emphasis on risks to human security or the value of a human-rights-based approach to addressing security threats in the cyber domain.

Going forward, the adoption of a human rights perspective would enable the First Committee to better navigate and frame the relevant threats that exist at the intersection of international security and the cyber domain.

\hspace{0.5em}> Dispelling technological neutrality: First, it is notable that the OEWG’s report concludes that ‘it is the misuse of... technologies, not the technologies themselves, that is of concern’.\textsuperscript{113} The phrasing of this statement is unfortunate since it risks giving the misleading impression that it is only the use of technology that may have consequences for the enjoyment of human rights, neglecting the fact that it is also the very design of technology that can make those consequences more or less likely.\textsuperscript{114} As McGregor, Murray and Ng have observed, human rights establishes obligations on states and expectations on businesses to protect human rights across ‘the full algorithmic life cycle from conception to deployment’.\textsuperscript{115} Moreover, the OEWG’s statement neglects the possibility that there may be certain ICTs that should be prohibited due to their appreciable adverse human rights impacts.\textsuperscript{116}

\hspace{0.5em}> Elevating private actor responsibilities: Second, it is significant that the reports by the OEWG and UNGGE recognise the malicious use of ICTs by ‘non-State actors, including terrorists and criminal groups’,\textsuperscript{117} as well as the fact that critical infrastructure and critical information infrastructure ‘may be owned, managed or operated by the private sector’.\textsuperscript{118} In addition, the OEWG report recognises that

\textsuperscript{112} OEWG Report (2021), para. 21.
\textsuperscript{113} Ibid., para. 23.
\textsuperscript{114} Land and Aronson, fn 6 above, pp. 1, 2.
\textsuperscript{118} OEWG Report (2021), para. 18.
‘all stakeholders have a responsibility to use ICTs in a manner that does not endanger peace and security’. However, these statements substantially underplay the extent to which private actors have managed to amass control over the cyber domain. As a result of their outsize influence in the cyber domain, private actors ranging from social media companies to the private surveillance industry not only have the potential to substantially affect the human rights of individuals around the world, but may also be at the forefront of responding to human rights violations committed by third parties. By adopting a human rights perspective of international security in the cyber domain, the First Committee could direct greater attention towards identifying and clarifying the relevant positive obligations on States to address the adverse human rights impacts of private actors, as well as how the corporate responsibility to respect under the UNGPs may be better operationalised in this context.

Identifying and addressing specific cyber threats: Third, it is notable that a number of cyber threats identified in the reports by the OEWG and UNGGE would benefit from being framed in human rights terms. For example, mention is made of:

1. ‘States’ malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another State’;

2. ‘harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally’, including ‘critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet and health sector entities’;

3. ‘the use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure’.

Adopting a human rights perspective would enable the First Committee to specify the ways in which particular cyber threats may cause different types of harms to humans by interfering with and potentially violating particular human rights. For example, information campaigns potentially implicate the rights to freedom of expression, political participation, privacy and self-determination, while hostile cyber operations against critical infrastructure such as health facilities potentially implicate the rights to life and health.
At the same time, adopting a human rights perspective would also require the First Committee to make clear that it is not only the malicious design and use of ICTs that may pose a threat to human rights, but also the repressive measures that are sometimes adopted by states in their attempts to address perceived threats. The UNGGE’s 2021 report recognises this to a certain extent when it confirms that ‘arbitrary or unlawful mass surveillance may have particularly negative impacts’ on human rights, particularly the right to privacy. While such a statement is welcome, it would be useful to make clear the more general value of human rights in establishing criteria and thresholds that states must satisfy when addressing perceived cyber threats. For example, in conducting surveillance measures, states may not interfere with the right to privacy unless they can demonstrate that the interference is provided for by law, undertaken in pursuance of a legitimate aim, and necessary to the achievement of that aim. Applying these criteria requires states to establish a publicly accessible and sufficiently precise legal basis for the measures in question, as well as to demonstrate an evidential basis for the connection between the measures and the legitimate aim, why alternative less intrusive measures are inadequate, and the safeguards that have been put in place to ensure that the measures are not too broad.

Ultimately, rather than a limited and vague reference to ‘specific guidance’ contained in General Assembly and Human Right Council resolutions, it is suggested that the work of the First Committee could benefit from devoting greater attention to recognising the links between human rights and specific cyber threats, including specifying the human rights that may be violated by particular threats and explaining how human rights can guide and restrict the responses of states seeking to address them.

4.2. Human rights and concepts of international law

Human rights are also of relevance to the interpretation of a number of concepts of international law that have been discussed within the ongoing work of the First Committee on the application of international law to cyber operations.

> **Due diligence:** The UNGGE’s 2021 report recognises the expectation that ‘States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs’, and reaffirms that states ‘should seek to ensure that their territory is not used by non-State actors to commit [internationally wrongful]..."
acts’. The status of due diligence under international law remains contested by states, with Israel and Argentina publicly rejecting the existence of the rule, while others such as Estonia, Finland, France, the Netherlands, Germany, the Republic of Korea and Brazil taking the opposite position. While the UNGGE’s report does not resolve the status of due diligence under international law, it does provide helpful guidance as to how a non-binding norm of due diligence should be understood. In this regard, the work of the First Committee might benefit from further deconstructing the concept of due diligence in the cyber domain by unravelling what Coco and de Souza Dias have recently referred to as ‘a patchwork of duties to prevent, stop and redress harm’ that apply by default to the cyber domain. Importantly, these protective obligations are grounded in a diversity of primary rules of international law, including the obligation of states to protect human rights within their jurisdiction. Unravelling the different but overlapping protective obligations requiring diligent behaviour in cyberspace, including those rooted in HRL, could help advance the debate on the concept of due diligence in the work of the First Committee.

> **Countermeasures:** Neither of the reports by the UNGGE or the OEWG directly addressed the concept of countermeasures, namely ‘measures that would otherwise be contrary to the international obligations an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation’. The status of countermeasures in the cyber domain has proved contentious among states in previous UNGGEs. The UNGGE’s 2021 report merely acknowledges that ‘an affected State’s response to malicious ICT activity attributable to another State should be in accordance with its obligations under … international law, including those relating to … internationally wrongful acts’. In advancing its work on the issue of countermeasures, the First Committee should bear in mind that one of the limitations that apply to their use is that they shall not affect ‘obligations for the protection of fundamental rights’. Since little guidance is provided on the meaning of ‘fundamental rights’ in the Articles on State Responsibility or its accompanying commentaries, were the First Committee to advance its discussions on the status of countermeasures in the

---

130 UNGGE Report (2021), para. 71(g).
133 Ibid., pp. 771, 795–800. See also Milanovic and Schmitt, fn 51 above, 247, 270–282.
135 Schmitt, fn 56 above.
cyber domain more generally, clarifying the meaning of fundamental rights limitations in this context might usefully form part of its work.

4.3. Human rights and proposals for advancing responsible state behaviour in ICTs

Finally, the human rights principles of participation/inclusion and accountability/rule of law could also inform the First Committee’s consideration and design of proposals for advancing responsible state behaviour in ICTs. In this regard, it is notable that the UNGGE’s 2021 report and the OEWG’s report recognise ‘the value of further strengthening collaboration, when appropriate, with civil society, the private sector, academia and the technical community’, including via ‘dialogue through bilateral, sub-regional, regional and multilateral consultations and engagement’. Mention is also made of ensuring the continuation of efforts to further the framework of responsible State behaviour within the UN and other regional and multilateral forums ‘in an inclusive, consensus-driven, action-oriented and transparent manner’.

One possibility specifically mentioned in the reports by both the UNGGE and the OEWG is the proposal for a Programme of Action (PoA) on advancing responsible state behaviour in cyberspace. Although the modalities of a PoA remain subject to further discussion, such an initiative has the potential not only to improve the inclusiveness of the current debate by providing a more sustained and structured basis for multistakeholder participation, but also to provide an avenue for accountability through, for example, some form of state-led ‘cyber peer review mechanism’ supported by input from the broader stakeholder community.

---

139 UNGGE Report (2021), para. 79.
5. Human rights contested: the risks of pursuing a human rights-based approach in the UN General Assembly First Committee

While human rights offers an important frame and vocabulary for examining the intersection of international security and the cyber domain, it is also important to recognise the risk that arises of the co-option of the language of human rights to legitimate repressive state measures. A recent illustration of the legitimation function of human rights is found in the majority judgment of the Grand Chamber of the European Court of Human Rights in the case of *Big Brother Watch and Others v. the UK*, which concerned the compatibility of the UK’s bulk surveillance programme with the European Convention on Human Rights. The judgment is grounded in what Zalnieriute refers to as ‘procedural fetishism’—endorsing the legality of bulk surveillance operations as ‘valuable’ and of ‘vital importance’ to state security provided a set of ‘end-to-end’ procedural safeguards are satisfied. The result, as Milanovic explains, is ‘a grand, definitive normalization of mass surveillance by a virtually unanimous Grand Chamber for decades to come’. Or as Judge Pinto de Albuquerque put it in his Partly Concurring and Partly Dissenting Opinion in the case, ‘for ill more than for good, with the present judgment the Strasbourg Court has just opened the gates for an electronic “Big Brother” in Europe’.

In the context of the First Committee, recent decades have witnessed the emergence of a division of emphasis among states concerning the role of human rights in discussions of international security in the cyber domain. On the one hand, while affirming the importance of ensuring respect for human rights, some states have placed emphasis on such respect being premised on compliance with relevant national laws and regulations. For instance, in a letter to the UN Secretary-General in 2011, Russia, China, Tajikistan and Uzbekistan proposed an international code of conduct for ‘information security’, which included a call for states ‘to fully respect rights and freedom in information space, including rights and freedoms to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulations’. By contrast, several other states have placed greater emphasis on the principle of free flow of information.

---

144 *Big Brother Watch and Others v. the United Kingdom*, Applications Nos 58170/13, 62322/14 and 24960/15, ECtHR Grand Chamber, Judgment (25 May 2021), para. 59.
145 Zalnieriute, fn 45 above.
147 *Big Brother Watch and Others v. the United Kingdom*, Applications Nos 58170/13, 62322/14 and 24960/15, ECtHR Grand Chamber, Partly Concurring and Partly Dissenting Opinion of Judge Pinto de Albuquerque (25 May 2021), para. 59.
The UK, for example, has previously declined to recognise the validity of the term ‘information security’ to the extent that ‘it could be employed to legitimate further controls on freedom of expression beyond those agreed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights’. 149

Against this background, it is notable that a recent UN General Assembly resolution, co-sponsored by the US and the Russian Federation, invites states to continue to inform the Secretary-General of their views and assessments on ‘efforts taken at the national level to strengthen information security and promote international cooperation in the field’. 150 Although it is not free of ambiguity, the inclusion of the term ‘information security’ in the resolution—which was adopted without a vote—risks legitimizing the notion that information itself can pose a security threat and endorsing an approach that places emphasis on restricting human rights in the cyber domain. 151 In this way, the resolution may also be considered a warning sign for how human rights might be interpreted and understood were the First Committee to centre such questions in its future work at the intersection of international security and the cyber domain.

149 A/68/156, 15. See similarly A/69/112/Add. 1, 3 (France).
150 A/RES/76/19 (emphasis added).
Application of Sovereignty to Information and Communications Technologies

**Vera Rusinova**, National Research University Higher School of Economics

1. Introduction

This paper’s arguments on the application of sovereignty to information and communications technologies (ICTs) under international law proceed in four steps. The first part outlines the current status quo. The second one aims to unify different approaches with respect to the normativity of the principle to respect sovereignty. The third part discusses five main legal obstacles arising in the current process of law-making aimed at the designation of the scope of ICT acts breaching sovereignty as a rule. The fourth one represents an attempt to overstep the limits of the ‘territorial sovereignty’ concept by considering the application of sovereignty to ICT through the prism of function theory.

2. Setting the scene

The role of the principle of non-interference in internal affairs with respect to malicious ICT activities is rather modest, and, at the current moment, intervention in elections serves as the sole example illuminating attempts to modify the scope of this principle. This brings to the forefront of normative discourse the principle of sovereignty. Although the principle of sovereignty is closely connected with the principle of non-interference, as it was clarified by the International Court of Justice (ICJ) in the Nicaragua case, their content is not identical, and the former still can be violated by actions not outlawed by the latter. In particular, the flights of US aircraft over the territory of Nicaragua were qualified as such a breach. Further similar conclusions were made by the ICJ in other cases, and the range of violations included marine as well as terrestrial intrusions. Nonetheless, apart from separate rules, such as the prohibition of interference in domestic affairs, state immunity, jurisdiction and territorial integrity, a general scope of this principle in non-cyber-specific relations—in contrast to the

---

153 Nicaragua v. US, paras 251, 292.
principle of non-interference—does not exist either in state practice and opinio juris of states or in the doctrine.

Although the UN Group of Governmental Experts (GGE) has confirmed the applicability of the principle of sovereignty in the ICT context,\(^\text{156}\) it confined itself to highlighting the relevance of the principle of sovereign equality, the applicability of ‘state sovereignty and international norms and principles that flow from sovereignty’ to ‘the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory’, and a necessity for states to ‘observe’ state sovereignty in their use of ICTs. The Open-Ended Working Group (OEWG), in its final report, was even more cautious.\(^\text{157}\) Application of the principle of sovereignty in ‘cyberspace’ encounters not only the problem of the indeterminacy of its content, including elements of outlawed behaviour, their threshold and the scope of protected (‘critical’) infrastructure,\(^\text{158}\) but also a split in the official positions of different states with respect to the legal nature of this principle as giving rise to a rule or merely being a fundamental principle. The US and the UK articulated their positions that sovereignty is solely a principle, not a rule.\(^\text{159}\)

Among the states that in their official positions defended the sovereignty-as-a-rule approach, one can find a variety of views on the parameters of its scope. The Netherlands, Finland and Switzerland relied on the approach reflected in the 2017 Tallinn Manual, according to which this rule is breached if there is an ‘infringement upon the target State’s territorial integrity’ and ‘an interference with or usurpation of inherently governmental functions’.\(^\text{160}\) Some states, such as Brazil, Norway and France, tried to reserve the widest possible approach to the content of this principle. The Defence Ministry of France indicated that its sovereignty can be breached by any attack against ‘the information systems located on its territory’, including ‘equipment and infrastructure located on national territory; connected objects, logical components … content operated or processed via electronic communication networks which cover the national territory or from an IP address attributed to France’ and ‘domains belonging to national

---

\(^{156}\) GGE Report, 2015, paras 26, 27, 28(b).
\(^{157}\) The final OEWG Report, 2021, paras 19, 56.
\(^{158}\) Please note that experts of the Tallinn Manual 2.0 were strongly divided in respect of these issues (see Tallinn Manual 2.0, pp. 20–27).
registers’. A comparable position was taken by Norway, and the fact that Brazil has referred to ‘interceptions of telecommunications’ as an example of a violation of sovereignty gives an indication of its very wide approach to what is protected by this rule.

3. Sovereignty as a rule or as a principle: a unity of opposites

The sovereignty-as-a-principle approach presupposes that at the current moment neither general (non-cyber) nor specific (cyber) rules exist in international law. At first glance, it seems to ignore ‘territorial sovereignty’ as a strand of the sovereignty approved by the ICJ as a standalone rule, and clearly stands for a lack of lex lata regulation. Relevant rules are, therefore, to be created by states.

The sovereignty-as-a-rule approach seems to overestimate the ‘territorial’ aspect of sovereignty and in the absence of any standards faces the limitations and shortcomings of deduction. A mélange of tools to overcome them consists of building up an ‘extended non-interference principle’ linking its scope (at least, in a part) with the exercise of state functions or of reliance on the lack of the opposite opinio juris (a Nicaragua-like argumentative pattern). It is, however, true, that in air, space and sea, ‘sovereignty has been applied differently by the international community depending on the practice of states across these domains, resulting in disparate legal paradigms’.

A search for the possible criteria and the articulation of any version of the scope of this principle are of a norm-creative character. The examples dealt with by the ICJ as breaches of territorial sovereignty can confirm only a very narrow reading of this rule with respect to ICT activities, making it almost inapplicable. Thus, the two approaches arguing against each other inevitably meet in the lawmaking. The only difference is that it is explicit for sovereignty-as-a-principle and implicit for its opponents.

Whether or not the OEWG or alternative multilateral fora will deal with the clarification of the applicability of sovereignty to ICT acts, the lawmaking has already started by states that unilaterally articulate their legal stances.

---

163 GGE Compendium-2021 (Brazil), p. 18.
165 Tallinn Manual 2.0.
166 See: GGE Compendium-2021 (Brazil), p. 18.
4. Sovereignty as a prohibitive rule: legal obstacles for lawmaking

At least five legal obstacles can be summarised that arise in the process of lawmaking aimed at the designation of the scope of ICT acts breaching sovereignty-as-a-rule, and therefore identification of the criteria of the outlawed behaviour, whether through the functions and/or notion of the critical infrastructure or the search for the proper threshold.

The first obstacle consists in the necessity for states to make a shift from an egocentric (what a state considers as a violation of its sovereignty) to a self-transcending (what acts of this state will violate sovereignty of others) articulation of this rule. The indications of egocentricity can be found in the self-oriented formulations of the states\textsuperscript{168} or the use of the extended scope of malicious ICTs acts giving rise to the application of coercive measures (‘sanctions’).\textsuperscript{169} or avoidance of discussing the thresholds.\textsuperscript{170} A generous approach to sovereignty-as-a-rule in the ICT sphere may be well justified by various factors: it plays a deterrent role, it supports political attribution and the ‘name and shame’ tool, it enhances the legitimacy of the resort to unilateral or collective coercive measures in response to malicious ICT acts. However, such a stance does not necessarily presuppose a readiness to be bound by the same (synallagmatic) obligations. The same trap led to the crystallisation of a very narrow scope of the non-interference principle.

The second obstacle is a well-reported conundrum of compatibility of a sovereignty-as-a-standalone-rule approach, exceeding the scope of the non-interference principle, with the general permissibility of espionage (while being criminalised domestically, it is lawful under international law unless it violates a particular norm). The interception of information and intrusion into information systems fall under espionage, and, thus, it will make states face a difficult choice of international prohibition of espionage, which is rather an idealistic and utopian option, or of adopting a very thin version of interference outlawed by the rule of sovereignty. It should be not surprising that states that have articulated the widest stances on the scope of sovereignty in the ICT context have not expressed their views on the relationship with espionage.\textsuperscript{171} Thus, even the egocentric views on the scope of sovereignty-as-a-rule in a cyber context should be taken with a view of (still not prohibited) espionage.

\textsuperscript{168} For instance, see fn 10 above.


\textsuperscript{170} See for instance GGE Compendium-2021 (Switzerland), pp. 87–88; Ministry of Foreign Affairs (The Netherlands), Letter to the Parliament on the International Legal Order in Cyberspace, 26 September 2019, p. 2.

\textsuperscript{171} It is indicative that no state in the GGE Compendium-2021 mentioned the relationship between sovereignty-as-a-rule and espionage, and Norway specifically stressed that ‘This position paper does not contain any specific analysis of cyber espionage, that is cyber operations whose purpose and effect is limited to the mere collection of information for use by the authorities, which is not in itself illegal under international law. However, certain aspects of such intelligence operations could violate specific rules of international law’ (p. 66, n. 176).
The third legal problem arises from a double function of a notion of ‘critical infrastructure’. One of the approaches seems to be to delineate the scope of protected objects. In parallel, the same notion is used internally by states to bolster the protection of the most important infrastructure, and is an implication of sovereignty as a responsibility to defend one's own population and respectful infrastructure.\(^{172}\)

The fourth obstacle is that the ‘packing’ of ICT relations into ‘territorial sovereignty’ will require ‘cyber borders’,\(^{173}\) which, being crucial for cyber security, will ‘fire back’ by extension and legitimisation of the national control over communications.\(^{174}\) Notwithstanding its political connotation, this linkage has clear legal implications.

A rupture between ‘cyber borders’ technically related to the autonomous systems making up the Internet, on the one hand, and the concept of territoriality as a part of territorial sovereignty, on the other, constitutes the fifth problem. The post, telephone and telegraph paradigm to treat sovereignty with respect to ICT context is ineffective and will inevitably reach its objective (institutional and technical) limitations.

5. New ways for the formalisation of sovereignty in ‘cyberspace’\(^{175}\)

The resources for crystallisation of new approaches to the legal formalisation of sovereignty in ‘cyberspace’ can be found in the legal–philosophical theories conceiving of sovereignty on the basis of property, competencies or functions. Both the ‘sovereignty-as-a-rule’ and ‘sovereignty-as-a-principle’ approaches are underpinned by the object (property) theory of territory (which entails state territory as a possession of the state), and, therefore, fall into the ‘territorial trap’, taking for granted the spatial dimension of the state as a persistent mechanism that operates much the same over time.\(^{176}\) Another theory that is better designed to describe territory in contemporary international law in general, and to reconcile territorial sovereignty with cyberspace in particular, is the competence theory\(^{177}\) advanced by the ‘pure theory of law’.\(^{178}\) According to this approach, territory itself is not of a geographical nature, but the sphere

---

of validity of the coercive legal order called the state.\textsuperscript{179} The role of the territory is to limit, according to general international law, the exercise of jurisdiction by the internal organs of the authorities of the state.\textsuperscript{180} The exclusive nature of sovereignty requires that it should be considered through the plentitude of its competencies rather than their individual sum.\textsuperscript{181} The state exercises its sovereign competences in three spheres of application: spatial, personal and factual (material). The initially universal factual competence is limited by the domestic legislation of every state, by international law and by norms governing conflict of laws.\textsuperscript{182}

The monistic approach of this theory to the relation between international and national law yielded its main criticism\textsuperscript{183} and paved the way for the rise of a function theory that defined the state as an imperium endowed with a plurality of powers and competencies protected by international law. According to it, state competences do not derive from international law, but from the subjective right of the state to exercise its powers within the limits of the competences recognised by international law.\textsuperscript{184} The territory of the state is defined according to the function served by practising relevant sovereign power. The function theory, a sub-theory of the competence theory, allows the state to project the powers necessary to reach a definite object or to satisfy a definite interest.\textsuperscript{185} Most crucially, the function theory reconfigured the jurisdiction of the state in a competence theory that is not to be presumed to exist all the time.\textsuperscript{186} Aside from the spatial and personal connotations of competence, the functional competence of the state is aimed at individual and common interests. That is relevant when the collaborative efforts of the community of states are required for its fulfilment, as for example in environmental issues and combating piracy and terrorism, when no strict application of spatial or personal powers suffices.\textsuperscript{187}

The Tallinn Manual 2.0 adopted a rather hybrid approach, mixing the property and competence theories.\textsuperscript{188} At the same time, its authors added that any prospective normative concept of cyberspace should comply with the material notion of territory, embodied in the summa potestas conception of territorial sovereignty.\textsuperscript{189} The first edition of the Tallinn Manual in 2013 even tried to materialise cyberspace explicitly

\textsuperscript{186} Conforti, fn 33 above, p. 76.
\textsuperscript{187} Milano, fn 28 above, pp. 69 et seq.
\textsuperscript{188} Tallinn Manual 2.0, pp. 55, 61.
\textsuperscript{189} Ibid., p. 12, para. 5.
through the prism of state jurisdiction, by providing that ‘[A]ctual physical presence is required, and sufficient, for jurisdiction based on territoriality; spoofed presence does not suffice’. This metaphor was subject to criticism for failing to understand the ethereal nature of cyberspace, by presuming that the Internet will certainly exist ‘somewhere’.

A possible solution for this issue can be derived from the application of the function theory in cyberspace. Then a functional model of a non-presumed state competence can be deployed to read sovereignty in terms of ‘quantum superposition’; sovereignty – and, hence, competence – can exist and not exist in the same spatiotemporal setting, determining the existence of a state competence only to be recognised when passing certain legal–political thresholds agreed upon by the states.

The function theory also provides rather comfortable conditions for states to participate in cyber-governance with their sovereign capacity, instead of being on par with non-state actors in cyberspace. Nevertheless, the function theory in cyberspace requires further collaborative efforts to define rightful state interests worthy of protection by international law, and to determine the threshold for the violation of such interests. State functions in cyberspace should be defined not only as a matter of normative parameters, but also as demonstrating the intended outcomes of pursuing such objectives, and the methods necessary to delimit states’ functional jurisdiction against other subjects of international law.

The application of this approach has a number of practical tenets relevant for the development of lawmaking with respect to ICTs. Firstly, the competence and function theories shift the emphasis from the only partly objectifiable territorial borders in ‘cyberspace’ to the competences and functions of states. On the one hand, this exposes the limits of the deduction from sovereignty (be it taken as a principle or as a rule) alone, and highlights the necessity of lawmaking through induction (state practice accompanied by opinio juris) or drafting of international treaties. On the other hand, it leaves the articulation of the competences/functions in the realm of existing norms of international law. Secondly, sovereignty with respect to ICTs, seen through these lenses, does not presuppose existence of the exclusive sovereignty of one state over particular relations or acts, but allows overlapping and coexistence. Thirdly, this approach to sovereignty is focused on the rights of states in their own territory and abroad, but does not automatically ‘obligate other states to refrain from all activities that might infringe upon or operate to the prejudice of the territorial state’s internal sovereignty’, unless

---

it is prohibited by lex lata rules of international law, such as the non-interference principle, or will be prohibited in the course of international lawmaker.

6. Conclusion

This paper assumes that through the stereoscopic approach to the appreciation of the nature of sovereignty and the use of functional theory in addition to the concept of ‘territorial sovereignty’, it is possible to advance new ways for the formalisation of sovereignty in ‘cyberspace’. As the application of this theory allows cyberspace to remain in its present global sphere and does not diminish for states the realisation of their functions, such a stance can also pave the way for a possible change of the vector of the positivistic approach to the application of sovereignty in the ICT context.
1. Introduction

As a corollary to every state's sovereignty, states and scholars have long recognised an international law prohibition on intervention.\(^{195}\) Although it is not in the text of the UN Charter, states featured the non-intervention principle prominently in the 1970 Friendly Relations Declaration.\(^{196}\) It is codified in several regional organisations’ constituent instruments (e.g. the Organization of American States (OAS), African Union (AU), Association of Southeast Asian Nations (ASEAN)).\(^{197}\) And the International Court of Justice (ICJ) recognised it as ‘part and parcel of customary international law’ (while acknowledging that violations of ‘the principle are not infrequent’).\(^{198}\)

In terms of its contours, the ICJ’s *Nicaragua* opinion contains the now-canonical summary:

> [T]he principle forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of


\(^{196}\) Declaration on Principles of International Law, Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. Doc. A/RES/25/2625 (24 October 1970) (‘1970 Friendly Relations Declaration’) Principle 3 (‘No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State … No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State.’); see also *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion*, 2010 ICJ Rep. 403, para. 80 (characterising the 1970 Friendly Relations Declaration as customary international law). The 1970 Friendly Relations Declaration had UNGA antecedents. See e.g. *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty*, GA Res. 2131(XX) (21 December 1965).

\(^{197}\) Charter of the Organization of American States, 30 April 1948, Art. 3(e); Constitutive Act of the African Union, 11 July 2000, Art. 4(g); The ASEAN Charter, 20 November 2007, Art. 2(2).

these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.\(^{199}\)

Thus, as a matter of general public international law, there clearly exists a principle of non-intervention and it prohibits (a) action attributable to a state (b) involving ‘methods of coercion’ (c) regarding the internal or external affairs of a state. Yet states have struggled to elaborate the prohibition further, leaving its contents ‘riddled with definitional ambiguity and conceptual uncertainty’.\(^{200}\) As a result, aside from ‘forceful’ coercion—i.e. uses of force—international law offers little consensus on what constitutes ‘methods’ of coercion, let alone what ‘affairs’ are protected from them.

This state of affairs has carried over into the cyber context. Unlike other areas (e.g. sovereignty, due diligence), there does not appear to be any debate over the existence of a non-intervention duty in cyberspace. The 2015 UN Group of Governmental Experts (GGE) acknowledged that ‘States must observe, among other principles of international law ... non-intervention in the internal affairs of other States.’\(^{201}\) The 2021 UN GGE indicated that ‘[i]n accordance with the principle of non-intervention, States must not intervene directly or indirectly in the internal affairs of another State, including by means of information and communication technologies.’\(^{202}\) At the same time, further elaborations on the principle’s application to cyber contexts remain sparse; as the Netherlands noted, a precise definition has ‘not yet fully crystalized’.\(^{203}\) The 2021 Open-Ended Working Group on Information Security—open to all UN member states—makes no mention of it.\(^{204}\) Many (if not most) of the states that reference non-intervention in official statements on international law’s application to cyberspace simply repeat earlier formulations of the principle (e.g. the 1970 Friendly Relations Declaration, the Nicaragua opinion).\(^{205}\)

Given this status quo, how can states elaborate what the non-intervention principle entails and apply it to current practices? Any progress will likely require attention to at

---


\(^{200}\) Helal, fn 1 above, p. 26.


\(^{203}\) Ibid., Annex, p. 56.


\(^{205}\) See generally 2021 GGE Report, fn 8 above, Annex (especially views of Australia, Brazil, China, Japan, Singapore, Switzerland, Russian Federation, UK).
least two sets of challenges for devising a cyber-specific manifestation of this duty, i.e. those involving (i) non-intervention’s corollaries and (ii) its contents.

2. Corollaries

As noted at the outset, the non-intervention principle is usually envisioned as a corollary to sovereignty. That linkage raises important questions for the principle’s future elaboration. For example, should further clarifications of non-intervention depend on sovereignty being accepted/rejected as a stand-alone rule governing cyber operations? How broadly a state defines coercion might, for example, depend on whether non-intervention operates as the only general prohibition on state behaviour below the use of force threshold, or if, instead, it forms an intermediate restriction lying between the prohibition on threats and uses of force and violations of a (lower) sovereignty threshold.

The latter possibility highlights that sovereignty may not be the only appropriate corollary for constructing the non-intervention principle—the use of force prohibition also warrants attention (indeed, the linkage is already evident in the ICJ’s *Nicaragua* opinion). States and scholars have spent two decades assessing whether and which cyber operations would cross the use of force threshold. The dominant view now depends on an ‘effects’ test, analysing to the outcomes of prior engagements with military or ‘armed’ force rather than depending on the use of military tools (or weapons) directly. Should non-intervention in cyberspace incorporate a similar effects test? At least some states (e.g. Germany) support that methodology. 206 Scholars such as Helal highlight, however, that such an approach risks excluding otherwise coercive interference in a state’s internal affairs simply because it proves ineffective. 207 Thus, gaining consensus on the right (or wrong) corollaries for non-intervention could open up opportunities for further elaborating its meaning or application.

3. Contents

The contents of non-intervention are currently convoluted and contested. Progress may thus depend on identifying additional layers of agreement on what the elements of the obligation entail and how to apply these in cyber contexts.

206 Ibid., p. 34 (Germany is of the opinion that cyber measures may constitute a prohibited intervention under international law if they are *comparable in scale and effect to coercion in non-cyber contexts* (emphasis added)).
207 Helal, fn 1 above, pp. 43–45.
3.1. Acts attributable to states

Attribution operates as a prerequisite for further delimitations of the non-intervention principle in cyberspace (just as it does for applying other international law restrictions on state behaviour). For the principle to operate effectively, therefore, states should continue to pursue greater consensus on the thresholds and evidentiary standards (if any) for assigning state responsibility to cyber-operations, not just technically but legally (and politically) as well.

3.2. Methods of coercion

According to the ICJ’s Nicaragua opinion, the presence of coercion forms ‘the very essence’ of a prohibited intervention. Yet the concept of coercion itself is remarkably indeterminate in both its scope and its nature. As a matter of scope, coercion may easily encompass cases of forceful or dictatorial (i.e. ‘do not do X, or else’) demands. But what if the acts are not designed to have the target state take a particular position, and simply deprive that state of its control over the matter (or, even more broadly, simply produce disruptions or chaos)? What if the targeted state does not even know of the acts in question? And how do traditional categories separating coercion from acts of ‘persuasion, criticism, public diplomacy, [and] propaganda’ operate in an online environment where states now readily deploy campaigns of disinformation, deception and disruption? Is a disinformation campaign in an election non-coercive because it seeks only to persuade a population (or certain decision-makers), or does its ultimate aim—targeting a state’s ability to decide its political system—convert otherwise persuasive acts into coercive ones? To call some (or all) such measures coercive will require states to agree on expanding its scope, or even (as scholars such as Kilovaty suggest) dispensing with coercion entirely. States must therefore devote more attention to coercion’s scope online to avoid ‘an excessively narrow definition … permitting coercive policies that undermine the political independence of states or impair the right of self-determination’, while not having so broad a definition as to

---

208 Kilovaty, fn 1 above, p. 103 (noting that cyber operations require a certain degree of control over non-state actors to satisfy international law’s requirement for state action).


210 Tallinn Manual 2.0, fn 1 above, p. 320 (noting that most experts would not require knowledge by the targeted states of an intervention to breach the obligation); Kilovaty, fn 1 above, pp. 109–110.


212 Ido Kilovaty, ‘The Elephant in the Room: Coercion’, AJIL Unbound, vol. 113 (2019), pp. 87–91: 87, 90 (calling for non-intervention to replace coercion with a prohibition of acts that prevent ‘a state from freely exercising functions associated with its internal and external affairs’).
‘prohibit legitimate forms of pressure that states exercise in the pursuit of their interests’.213

Alongside questions of scope, states have never fully resolved what the nature of coercion ‘is’ itself. Simply put, is the presence of coercion found in the intentions of the act’s authors, in the effects that result, or in some combination of the two?214 The differences are significant. Does the principle include significant yet unintended interventions in a state’s internal affairs or exclude intended disruptions that never achieve the desired effects? In the cyber context, for example, does the emplacement of malware in a state’s critical infrastructure constitute intervention if it is never activated? What about a large-scale, surreptitious cyber operation that was not intended to disrupt a state’s government networks but does so once discovered because the targeted state feels compelled to rebuild its systems? State views are, at present, divided. Several (e.g. Estonia, France, Norway, Romania) define non-intervention in the effects produced on the targeted state.215 Others (e.g. Germany, New Zealand) appear to require an intention to intervene as well.216 As such, the relevance of intentions to non-intervention appears a topic ripe for further inter-state dialogue.

3.3. Internal and external affairs

Intervention only exists when acts by a state constitute coercion regarding another state’s ‘internal or external affairs’. In other words, coercive acts will not trigger the non-intervention prohibition absent a connection to affairs of state. Thus, even if state-sponsored ransomware is by definition coercive (e.g. demanding payment in return for restoring access to a system, a network or data), it will only be prohibited where it concerns the state’s internal or external affairs. For many, internal affairs equate to the

---

213 Helal, fn 1 above, p. 30. In addition, states and other stakeholders might consider whether the existence of coercion depends, in part, on its severity. To do so could allow international law to incorporate an assessment of the target state’s capacity to resist or otherwise defend against intervention in calculating the existence of a violative intervention.

214 Measuring intentions of institutional entities such as states is, of course, difficult. But subjective elements are already prominent in other key areas of modern international law, whether they be the search for opiniō juris in identifying the existence of a customary international law rule or ascertaining the intentions of states to form a treaty.

215 See 2021 GGE Report, fn 8 above, Annex, p. 25 (for Estonia, non-intervention prohibits operations that affect a state’s internal or external affairs in such a manner that it coerces a state to take a course of action it would not voluntarily seek); ibid., p. 68 (for Norway, cyber operations that compel the target state to take a course of action, whether by act or omission, in a way that it would not otherwise voluntarily have pursued (coercion) in matters relating to its internal or external affairs (domaine réservé) will constitute an intervention in violation of international law); ibid., p. 77 (for Romania, ‘there has to be a causal nexus between the coercive act and the effect on the internal or external affairs of the target State’); Ministère des Armées, Droit international appliqué aux operations dans le cyberspace (9 September 2019) (for French Ministry of Defence, ‘interference which causes or may cause harm to France’s political, economic, social and cultural system, may constitute a violation of the principle of non-intervention’).

216 See 2021 GGE Report, fn 8 above, Annex at 34 (for Germany, ‘the acting State must intend to intervene in the internal affairs of the target State – otherwise the scope of the non-intervention principle would be unduly broad’ (emphasis added)); New Zealand, The Application of International Law to State Activity in Cyberspace (December 2020) (defining coercion in terms of ‘an intention to deprive the target state of control over matters falling within the scope of its inherently sovereign functions ... While the coercive intention of the state actor is a critical element of the rule, intention may in some circumstances be inferred from the effects of cyber activity’).
domaine réservé. This, however, has done little to resolve the definitional difficulties, as states have yet to decide if the domaine réservé is dynamic or immutable. Is the domaine réservé some sort of fixed (and objective) list of inherent sovereign functions or does the scope of the non-intervention protection recede once a state accepts the matter as one of international concern (e.g. by assuming treaty commitments with respect to it)? In the latter case, the non-intervention principle may only protect areas of ‘residual liberty retained by states’ and will not forestall efforts to enforce commitments that might otherwise have fallen within the domaine réservé (e.g. the EU’s capacity to make demands on member states’ political systems according to their EU Treaty commitments). 

Whether the domaine réservé is fixed or dynamic, there is also clearly room for states as a practical matter to identify the principle of non-intervention’s subjects beyond those listed in existing doctrine (e.g. the ‘choice of a political, economic, social, and cultural system, and the formulation of foreign policy’). The GGE’s solicitation of state views on the application of international law to cyberspace reveals some areas of potential consensus. Common candidates include elections (the voting process itself or perhaps even the broader information ecosystem involving electoral processes and campaigns), critical infrastructure and medical facilities.

4. Forward path(s)?

The complexities of non-intervention’s corollaries and contents require further attention. And several states appear amenable to pursuing efforts to forge ‘common understandings’ on this topic. But where should such dialogues occur? UN processes—specifically the new Open Ended Working Group—provide a platform for achieving a universal approach. Yet, if past is prologue, UN processes have had decades to engage with the principle of non-intervention with limited success in further elaborations beyond those in the 1970 Friendly Relations Declaration or endorsements of the ICJ’s reasoning. Moreover, given that the most recent OEWG did not even

---

217 Tallinn Manual, fn 1 above, p. 314; but see Moynihan, fn 1 above, pp. 33–34 (arguing that the duty of non-intervention protects a state’s ‘inherently sovereign functions’ rather than the domaine réservé, which involves a sphere of activity that is not otherwise regulated by international law).
218 Helal, fn 1 above, p. 38.
219 Nicaragua, fn 4 above, para. 205.
220 On elections, see generally 2021 GGE Report, fn 8 above, Annex (Australia, Brazil, Estonia, Germany, Netherlands, Norway, Romania, Singapore, UK and US all list elections as among the affairs protected by the non-intervention principle with several—e.g. Germany, Norway—including disinformation campaigns). States such as Estonia, Norway, Japan and New Zealand expressed support for protecting critical infrastructure, while others such as Japan, New Zealand, the UK and the US would add medical services (with New Zealand including disinformation campaigns that significantly undermine a state’s public health efforts during a pandemic). Ibid; New Zealand statement, fn 22 above.
221 See 2021 GGE Report, fn 8 above, Annex, p. 47 (Japan); ibid., p. 35 (Germany notes that discussions on this topic are ongoing); Italy, Ministry of Foreign Affairs, Italian Position Paper on International Law and Cyberspace (November 2021) (‘Italy sees merit in continuing to deepen the study of possible violations of the principle of non-intervention in cyberspace’ including information operations involving public health and voting behaviour).
222 In 1982, for example, the UN General Assembly passed a Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, but unlike the unanimity that characterised the 1970 Friendly Relations Declaration, it generated significant opposition from major Western powers, with a final vote of 120 in favour, 22 against, six abstentions, with nine states
address non-intervention, it seems most likely that efforts would (at least initially) only reproduce past elaborations of the obligation. This is not to suggest that states should avoid the topic entirely, but only to temper expectations.

Regional approaches, in contrast, could produce broader or deeper elaborations of the principle of non-intervention. The history of specific regions (e.g. the Americas) may afford the topic the expertise (and priority) necessary to address one or more of the challenges identified above. It is also important to recognise that such efforts need not be limited to the cyber context. The proposed EU regulation on coercion, for example, offers member states an opportunity not only to further define that concept but to actually establish a framework for its application (applications that could include both cyber and non-cyber cases). Such opportunities may trade off the lack of universality with expanded (or deeper) understandings of the principle of non-intervention than witnessed to date.

What about the International Court of Justice? After all, non-intervention owes its present contours and contents to the Court’s Nicaragua formulation. Could the ICJ (or some other international court or tribunal) use a future case to further elaborate non-intervention’s application to cyberspace? Certainly, states and other stakeholders should carefully consider the prospects of such an approach given the (increasing) role of international courts and tribunals in the formulation of international law. At the same time, however, there are reasons to be cautious here given the need for a dispute, jurisdiction and expertise. For starters, an international case addressing non-intervention will require a dispute. To date, however, states have been reluctant to invoke international law generally in their accusations of state-sponsored cyber operations. But even if two or more states did have a dispute over non-intervention’s application to a cyber operation, the number of cases where the ICJ (or some other tribunal) will have compulsory jurisdiction is likely to be limited (as will be the circumstances where disputing states contemporaneously agree to present an issue to an international court or tribunal). And even if the ICJ took on such a case, we should not ignore the challenges technology may pose to the Court’s considerations. Will the judges have sufficient capacity to


225 Finnemore and Hollis, fn 15 above, p. 971. In surveying 11 cyber-incidents, Efrony and Shany found that states avoided invoking international law generally, let alone non-intervention specifically. Dan Efrony and Yuval Shany, ‘A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber-operations and Subsequent State Practice’, American Journal of International Law, vol. 112, no. 4 (2018), pp. 583–657: 583, 594. Kilovaty (fn 1 above, p. 106) suggests that this may be due to the absence of coercion. It is possible, however, that states’ reluctance stems from other rationales such as divergences over what coercion ‘is,’ lack of interest in giving constitutive effect to a particular episode, evidentiary issues in establishing the relevant facts, or concerns about the lack of effective enforcement mechanisms even if a violation could be found. See Finnemore and Hollis, fn 15 above, pp. 999–1000.

226 At the same time, it might be interesting for like-minded states to consider whether to refer a case inter se to the ICJ pursuant to Article 36(1) of the Court’s statute. However, doing so would require a like-minded state to have conducted a cyber operation against an ally or partner state that it is willing to admit to authoring and accepting the need to document and justify its behaviour: steps that states have not shown any willingness to pursue so far.
understand the technological architecture and its effects to produce well-reasoned and justified outcomes? Such challenges suggest that—at least for now—states will most likely need to elaborate the appropriate corollaries and contents of non-intervention on their own.

Finally, where states and other stakeholders do address the principle of non-intervention themselves, there may be real value in supplementing conceptual and doctrinal exchanges with methodologies that ask participants to assess the obligation in the context of past cases or hypotheticals. Such efforts can reveal areas of convergence (and divergence) about which particular behaviours may trigger the prohibition and in what contexts they actually would do so. Such efforts will not, of course, resolve every question, let alone generate universal agreement. Limited progress is probably the best-case outcome. Yet limited progress is still progress. Given the more existential challenges facing international law’s application to cyberspace, the opportunity to elaborate (and strengthen) the principle of non-intervention in cyber contexts is well worth exploring.
1. Introduction

This contribution discusses the application of ‘due diligence’ to information and communications technologies (ICTs) under international law. It does so by briefly addressing three key questions: (1) why, as a matter of law and policy, due diligence matters in the cyber context; (2) what exactly it means in international law; and (3) whether it applies to states’ use of ICTs. The paper concludes that due diligence is a standard of conduct found in a variety of existing international obligations, some of which apply by default to ICTs. Moving forward, it proposes that discussions on the matter should focus on specific measures of implementation, to dispel misconceptions and induce compliance.

2. Why does due diligence matter in the cyber context?

The concept of due diligence has recently gained prominence in the cyber context, where its application has been advanced by several scholars, states and international institutions. In general terms, due diligence encapsulates ideas of reasonable care and...
harm or risk prevention. As a limit to state and non-state uses of ICTs, its importance is fourfold.

First, by focusing on a state’s lack of care rather than the harmful act or result itself, due diligence avoids the notoriously difficult problem of factual and legal attribution in cyberspace. In short, due diligence would apply to a state insofar as it allowed a harmful cyber operation to originate from or transit through its territory or jurisdiction.

Second and relatedly, a finding of lack of due diligence may be less confrontational or antagonistic than a finding that a state is responsible for a harmful cyber operation. Again, due diligence is not about attributing responsibility to states for harmful acts or results, but about calling out states for failing to behave diligently or responsibly to prevent, halt or redress such acts. As such, both victim and origin/transit states may feel more comfortable coming forward.

Third, due diligence looks forward, not backwards. At the heart of the concept is the tried and tested assumption that prevention is better than cure. Thus, due diligence contributes to the prevention of cyber harms and their significant impact on states and non-state entities.

Fourth, due diligence is flexible. It is about taking steps that are reasonable in the circumstances, rather than successfully preventing or remedying all harms. In this way, due diligence gives effect to the idea of common but differentiated responsibilities and caters to different levels of state development in the cyber environment.

3. What exactly is due diligence in international law?

That due diligence in the ICT environment is a great idea as a matter of policy and common sense is beyond doubt. Duties of care have been imposed on states and individuals for centuries in different legal systems around the world. However, one of

---

the most hotly debated questions in cyber-governance circles is whether due diligence is binding on states as a matter of international law.  

3.1. A general principle?

Some scholars and states have argued that due diligence is a general principle of law derived from domestic legal systems around the world, within the meaning of Article 38(1)(c) of the Statute of the International Court of Justice (ICJ). This may well be the case. Nevertheless, it is difficult to prove this assumption. Challenges include the high number of states currently in existence, the variety of domestic legal systems and concepts to be surveyed, and the non-availability of translated legal documents. To date, a comprehensive comparative study of due diligence in domestic legal systems is yet to be carried out.

3.2. A cyber-specific rule?

According to Rule 6 of the *Tallinn Manual 2.0*:

A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.

This raises the question of whether due diligence is a rule of customary international law developed specifically for ICTs or in the cyber context. There is indeed widespread evidence that states have behaved diligently in their use of ICTs. However, there is insufficient *opinio juris* to date to the effect that there is a cyber-specific customary rule of due diligence. Existing manifestations of *opinio juris* have been limited to general due diligence obligations and their applicability to ICTs. Thus, Rule 6 of the *Tallinn Manual 2.0* is simply an articulation or ‘application’ of an existing due diligence obligation in

---


238 See above, fn 235.


242 See above, fn 228.
cyberspace. Nevertheless, it is open to states to develop such a cyber-specific rule under treaty or customary international law.

3.3. A standard of conduct?

While a cyber-specific due diligence obligation could be useful in laying down specific standards of state behaviour in their use of ICTs, such a rule is not strictly necessary. There is already a patchwork of international obligations of general applicability under conventional and customary international law that require states to behave with due diligence in a variety of circumstances, online or offline. Although ‘due diligence’ is often used as a shorthand for those various ‘protective duties’, it is best described as a flexible standard of conduct found in each of those rules. Though different, the following protective duties containing a due diligence standard share certain similarities. They are chiefly obligations of conduct, triggered by some level of actual or constructive knowledge of a certain risk or harm, and subject to a state’s capacity to act in the circumstances. They require a state to put in place the minimum necessary governmental apparatus and exercise its best efforts to prevent, stop or redress certain harms to another state or non-state actor.

3.3.1. The Corfu Channel principle

The most well-known version of due diligence was articulated by the ICJ in its 1949 Corfu Channel case. There, it found that: a ‘well-recognized’ principle under customary international law requires a state ‘not to allow knowingly its territory to be used for acts contrary to the rights of other States’. Though most of these acts will amount to an internationally wrongful act, they need not be committed by a state or violate a rule of international law per se. For instance, whether or not sovereignty is a self-standing rule of international law applicable in cyberspace, a state might violate the Corfu Channel principle if it knowingly allows its territory or jurisdiction to be used by other states or non-state actors to perpetrate acts contrary to another state’s sovereign rights, such as its right to hold elections and determine its health and national security policies. For a breach of this principle to ensue, there is no threshold of gravity or intensity. The origin

---

244 See Coco and de Souza Dias (fn 240).
246 See Coco and de Souza Dias (fn 240), pp. 804–805.
247 Ibid.
249 Coco and de Souza Dias (fn 240), pp. 778, 804–805.
250 Corfu Channel Case (United Kingdom v Albania), Judgment, 9 April 1949, ICJ Reports (1949) 4, p. 22 (emphasis added).
251 Coco and de Souza Dias (fn 2404), pp. 784–785.
252 Ibid., pp. 786–787.
or transit state must have actual or constructive knowledge of the act in question, have the capacity to prevent or halt it, and fail to do so by allowing the act to materialise.\textsuperscript{253}

### 3.3.2. The no-harm principle

A similar but different version of the due diligence standard in international law is found in the so-called ‘no-harm’ principle. Support for this principle under customary international law comes from treaties,\textsuperscript{254} landmark international cases such as Pulp Mills\textsuperscript{255} and Trail Smelter,\textsuperscript{256} and the work of the International Law Commission (ILC) on the prevention of transboundary harm.\textsuperscript{257} According to Article 3 of the ILC’s Draft Articles on the topic: ‘[t]he State of origin shall take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof.’\textsuperscript{258} The scope of the ILC’s Draft Articles was, for practical reasons,\textsuperscript{259} limited to activities having physical consequences.\textsuperscript{260} Nevertheless, the no-harm principle is arguably broader, covering physical and non-physical harm\textsuperscript{261} to persons, property or the environment,\textsuperscript{262} including where the activity in question is not wrongful under international law.\textsuperscript{263}

In the context of ICTs, this could potentially include online misinformation and disinformation campaigns, especially those taking place during elections, public health crises or armed conflict. Unlike the Corfu Channel principle, the no-harm principle first imposes liability on a state that fails to exercise due diligence in the prevention of harm. It is only if this state does not compensate for the harm to which it is liable that international responsibility for a breach of the principle will ensue.\textsuperscript{264}

\textsuperscript{256} Trail Smelter Case (USA v Canada) (1941) 3 RIAA 1911, at 1963.
\textsuperscript{257} ILC, Draft Articles on Prevention (n 233).
\textsuperscript{258} Ibid., at 153.
\textsuperscript{259} Ibid., at 151, Commentary to Art. 1, para. 16.
\textsuperscript{260} Ibid., at 149, Art. 1.
\textsuperscript{261} Examples of state practice and/or opinio juris supporting the applicability of the no-harm principle to non-physical harms, including in the ICT context, include (a) Art. 10, para. 2 of the 1927 International Radiotelegraph Convention; (b) Art. 35(1) of the 1932 International Telegraph Convention; (c) Arts 1–4 of the 1936 International Convention concerning the Use of Broadcasting in the Cause of Peace; and (d) Arts 38(5) and 45(3) of the 1992 Constitution of the International Communications Union, 1825 UNTS 331.
\textsuperscript{262} 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, 144, at 152, Commentary to Art. 2, para. 4 (hereafter ‘Draft Articles on Prevention’).
\textsuperscript{263} ILC, Draft Articles on Prevention (n. 233), at 150, Commentary to Art. 1, para. 6.
3.3.3. Positive human rights obligations

Universal and regional human rights treaties, as well as customary international law, impose on states both negative obligations to respect human rights and positive duties to protect them from arbitrary interference. It is these positive duties that require states to exercise due diligence in preventing, halting or redressing human rights violations by other states or non-state entities, including corporations. Insofar as jurisdiction over the individual victim is required by the relevant treaty, it is submitted that physical or non-physical control over the enjoyment of the right in question suffices to trigger it. In the digital world, due diligence to protect the rights to privacy, non-discrimination, freedom of expression, freedom of opinion and participation in democratic processes is particularly important.

3.3.4. Positive obligations under international humanitarian law

Lastly, several obligations under international humanitarian law (IHL) contain a due diligence standard, requiring states to take different steps in the context of international or non-international armed conflict to protect different persons or objects. Most notably, Common Article 1 of the 1949 Geneva Conventions, along with Article 1(1) of Additional Protocol I, codifies states’ customary obligation to respect and ensure respect for the provisions of the conventions. This erga omnes obligation requires all states to do ‘everything in their power to ensure that the humanitarian principles underlying the Conventions are applied universally’, including in peacetime. In the

266 UN Human Rights Committee (HRC), ‘General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant’, UN Doc. CCPR/C/21/Rev.1/Add.13, 26 May 2004, para. 8. See also Coco and de Souza Dias (fn 2404), pp. 799–800.
268 Coco and de Souza Dias (fn 14), pp. 800–804.
269 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.
270 Article 1(1), 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.
273 Ibid., paras 127–128 and 185.
ICT environment, this may require states to take reasonable steps to prevent or mitigate online content and operations that encourage or facilitate violations of IHL, such as attacks against civilians and medical or religious personnel.

4. Due diligence at the UN GGE and OEWG: does it apply to ICTs?

In its 2015 report, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) recognised that: ‘States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs’. This norm has been endorsed and fleshed out in the GGE’s 2021 report. Similarly, in its 2021 substantive report, the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) recognised the need to protect critical infrastructure and critical information infrastructure supporting essential services to the public, especially healthcare, as well as to ensure the general availability and integrity of the Internet. However, that the GGE and OEWG framed due diligence as a non-binding norm of responsible state behaviour has been taken to mean that it is not a binding rule applicable to ICTs. In the same vein, some states have argued that due diligence lacks specific state practice and opinio juris in cyberspace.

These lines of argument fail for at least three fundamental reasons. First, as the OEWG has itself recognised, ‘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’. Second, as seen earlier, due diligence standards and their respective obligations apply generally to state behaviour under customary and conventional law in a wide range of circumstances. Third, these circumstances or activities include the use of ICTs insofar as these do not make up a ‘separate’ or ‘exclusionary’ domain that is carved out from existing

---

278 OEWG Final Substantive Report (n. 276), para. 25 (emphasis added). See also OEWG Zero Draft (n. 234), para. 54.
international law. Whether or not ICTs are virtual or have physical manifestations, existing general obligations under international law apply to them by default, without the need to prove specific state practice or opinio juris. The applicability of duties featuring a due diligence standard to ICTs has been explicitly recognised by several states and over 180 international lawyers in the five Oxford Statements on International Law Protections in Cyberspace.

5. Conclusion: the way ahead

In summary, due diligence is an important standard of conduct that binds states in their use of ICTs under different rules of international law. These rules do not require states to successfully prevent, stop and redress all kinds of malicious cyber operations, or to do the impossible to achieve that. As seen earlier, different conditions or thresholds, such as knowledge of the harm, jurisdiction and, most importantly, the capacity of each state to act in the circumstances, limit the operation of different standards of due diligence in cyberspace and beyond. All due diligence asks from states is that they behave carefully online as they must offline, insofar as feasible. This is arguably not too much to ask from any state but the bare minimum condition for a secure and stable ICT environment.

Moving forward, more efforts are needed to clarify the nature and scope of due diligence and dispel all misconceptions that have hampered its full acceptance and implementation in the ICT environment. To this end, future academic and policy discussions on the matter should focus on specific due diligence measures that may be put in place to discharge different protective duties in the cyber context. These discussions would benefit from the multidisciplinary input of lawyers, computer scientists and experts in public governance and administration.
About the authors

**Giovanna Adinolfi** is Full Professor of International Law at the University of Milan. Her research interests include international economic law, international trade law, law of international responsibility, cybersecurity, immunity of states and international organisations, and international disaster law. She is author of three monographs, co-editor of four volumes (one published by Springer) and author of articles and chapters in international volumes. She is a member of the Editorial Board of Questions of International Law – QIL (online) and of the Yearbook of International Disaster Law (Brill). In 2018–2019 she was consultant for the World Trade Organization on the research project ‘Trade and Natural Disasters’. She is member of the Committee of the International Law Association on Sustainable Development and the Green Economy in International Trade Law. In 2022 she was appointed to the position of arbitrator and trade and sustainable development expert for bilateral disputes under the EU preferential trade agreements.

**François Delerue** is a Senior Researcher in Cyber Security Governance at the Institute of Security and Global Affairs at Leiden University and Team Leader on International Law for the EU Cyber Diplomacy Initiative (EU Cyber Direct). He is also an Associate Fellow of the GEODE Center (Paris 8 University) and the Hague Program on International Cyber Security. He co-chairs the International Law Association (ILA) Committee on Digital Issues for International Law as part of the ILA’s 150th anniversary. François regularly lectures at Sciences Po (Paris), the International Institute for Humanitarian Law at Sanremo and the French War College (École de Guerre), and in the master in cybersecurity programme of the French Military Academy of Saint-Cyr. His book Cyber Operations and International Law was published by Cambridge University Press in 2020 and was awarded the 2021 Book Prize of the European Society of International Law.

**Talita Dias** is the Shaw Foundation Junior Research Fellow in Law at Jesus College, University of Oxford, as well as a Research Fellow with the Oxford Institute for Ethics, Law and Armed Conflict (ELAC). She is a founding member of the Oxford Process on International Law Protections in Cyberspace and co-authored the Oxford Statements on International Law Protections in Cyberspace. Prior to that, Talita was a Postdoctoral Research Fellow at Oxford’s Blavatnik School of Government, where she led ELAC’s Cyber Due Diligence project. Her current research focuses on the application of international law to new technologies and the international regulation of information operations, including disinformation and hate speech. Talita teaches international law & public policy on the Master of Public Policy Programme and has previously taught English criminal law, international criminal law, and public international law in Oxford. She has a DPhil
and a master’s degree in Law from the University of Oxford and a bachelor’s degree in Law from the Federal University of Pernambuco in Brazil. She is a qualified lawyer in Brazil.

**Aude Géry** is a post-doctoral fellow at GEODE, a research and training centre on the geopolitics of the datasphere hosted at the University of Paris 8. Her research focuses on the international regulation of digital space and more particularly on the external legal policies of states, multilateralism in the field of ICTs in the context of international security, and the normative issues flowing from the adoption of instruments on digital issues. She co-chairs the International Law Association (ILA) Committee on Digital Issues for International Law as part of the ILA’s 150th anniversary. She has participated in several high-level dialogues on digital issues (Sino-European Dialogue on Cybersecurity, Track 1.5 dialogues organised by EU Cyber Direct, Global Commission on the Stability of Cyberspace, Paris Call for Trust and Security in Cyberspace). For her PhD dissertation on international law and the proliferation of offensive cyber capabilities, she was awarded the PhD thesis prize of the French branch of the ILA, a special mention from the Léon Bourgeois Award, and the third thesis prize of the Institut des Hautes Etudes de Défense Nationale (IHEDN).

**Duncan B. Hollis** is Laura H. Carnell Professor of Law at Temple Law School and a co-convenor of The Oxford Process on International Law Protections in Cyberspace. His scholarship engages with issues of international law, interpretation and cybersecurity, with an emphasis on treaties, norms and other forms of international regulation. He is a non-resident scholar at the Carnegie Endowment for International Peace and an elected member of the American Law Institute, where he served as an adviser on its project to draft a Fourth Restatement on the Foreign Relations Law of the United States. In 2016, he was elected by the General Assembly of the Organization of the American States to a four-year term on the OAS’s Inter-American Juridical Committee. There, he has served as the rapporteur on binding and non-binding agreements as well as the rapporteur on improving the transparency of state views on international law’s application to cyberspace. Duncan’s books include the award-winning Oxford Guide to Treaties (OUP, 2nd ed., 2020), International Law (with Allen Weiner) and (with Jens Ohlin) Defending Democracies: Combatting Foreign Election Interference in a Digital Age (OUP, 2020).

**Vera Rusinova** is a Professor at the Faculty of Law of the National Research University Higher School of Economics, where she heads the School of International Law. The main fields of her research activities comprise international human rights law, international humanitarian law, use of force, the theory of international law, and application of international law to information and communications technologies. Vera has published more than 85 scientific articles and book chapters on international law. She is a co-chair of the ILA Committee on Use of Force: Military Assistance on Request, and a member of the editorial groups/boards of International Justice, Journal of
International Humanitarian Legal Studies and International Cybersecurity Law Review. Her lecture on ‘Human Rights in Armed Conflicts’ was placed in the UN Audiovisual Library of International Law. She also led the research project ‘Reshaping Public International Law in the Age of Cyber: Values, Norms and Actors’.

Barrie Sander is Assistant Professor of International Justice at Leiden University—Faculty of Governance and Global Affairs. His research and teaching focuses on the fields of international criminal law, international human rights law, and the intersection between digital technology and international law. He is the author of Doing Justice to History: Confronting the Past in International Criminal Courts (OUP, 2020) and recipient of the ICLQ Young Scholar Prize for his 2018 International & Comparative Law Quarterly article ‘History on Trial: Historical Narrative Pluralism Within and Beyond International Criminal Courts’.
About EU Cyber Direct

**EU Cyber Direct – EU Cyber Diplomacy Initiative** supports the European Union’s cyber diplomacy and international digital engagements in order to strengthen rules-based order in cyberspace and build cyber resilient societies. To that aim, we conduct research, support capacity building in partner countries, and promote multistakeholder cooperation. Through research and events, EU Cyber Direct regularly engages in the discussions about the future of international cooperation to fight cybercrime and strengthen criminal justice systems globally.