UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Due diligence in cyberspace

Normative expectations of reciprocal protection of international legal rights

ANDRAZ KASTELIC

ACKNOWLEDGEMENTS

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This study was produced by the Security and Technology Programme, which is funded by the Governments of Germany, the Netherlands, Norway and Switzerland and by Microsoft. The author wishes to thank the following individuals for their invaluable advice and assistance on this paper: Giacomo Persi Paoli (UNIDIR), Nicholas Tsagourias (University of Sheffield, School of Law), Pablo Rice (UNIDIR), Robin Geiss (UNIDIR), Robin Geraerts (The Netherlands), Samuele Dominioni (UNIDIR), Wieteke Theeuwen (The Netherlands); and the participants in the UNIDIR multi-stakeholder dialogue, "Due Diligence in Cyberspace: Multi-Stakeholder Dialogue on the Norms of Responsible State Behaviour," held on 12 May 2021: Anastasiya Kazakova (Kaspersky), Camille Gufflet (European External Action Service), Johanna Weaver (Australia), Marco Roscini (Westminster Law School), Masahiro Kurosaki (National Defense Academy, Japan), Nemanja Malisevic (Microsoft), Talita de Souza Dias (University of Oxford), Wieteke Theeuwen (The Netherlands), and Zhixiong Huang (Wuhan University).

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

ABOUT THE AUTHOR

Andraz Kastelic is the lead Cyber Stability Researcher of the Security and Technology Programme at UNIDIR. Prior to joining UNIDIR, he held various research positions at international organizations and research institutions around the world.

Table of contents

Executive summary 1

1. Context and content 2

1.1. Norm C of the UN Group of Governmental Experts 2

1.2. Purpose of this paper 3

1.3. Structure of the paper 3

2. Due diligence and normative standards 5

2.1. Norm or rule or principle? 5

2.2. Due diligence principle 6

2.3. Standards of compliance 6

2.4. Primary and secondary rules of international law 7

3. Scope of normative expectations 9

3.1. Prevention, termination or mitigation? 9

3.2. Capacity building and possible minimum standards of compliance 10

4. Normative conditions 13

4.1. Actual or constructive knowledge 13

4.2. The concept of an internationally wrongful act 14

4.3. Any cyber operation contrary to the rights of another State? 16

4.4. States of origin versus the States of transit 16

5. Possible consequences of the divergent interpretations 19

6. Conclusions and recommendations 21

References 23

Executive summary

Cyber operations may pose a challenge to the international legal rights of States and, by extension, to international peace and security. To promote adherence to international law in the cyber era, the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security put forward a framework of mutual international assurance. This includes a voluntary norm according to which "States should not knowingly allow their territory to be used for internationally wrongful acts using [information and communications technologies (ICTs)]".

This expectation, included in the norm C of the 2015 GGE report, derives from the due diligence principle of international law but contains several elements of contention and is subject to divergent interpretations. In order to facilitate the implementation of the norm and operationalize the mutual international assurance of the legal rights of States, the following issues should be resolved by the international community.

- One of the main points of contention among States is the question of whether the reciprocal protection norm is in fact an expectation of voluntary behaviour of States in cyberspace or whether it is an obligation, the violation of which entails legal consequences as per the inter-national customary law of State responsibility.
- Other elements of the norm deserve the attention of future multilateral processes dedicated to international ICT peace and security. What should be clarified is the scope of expected behaviour and the standard of compliance with the norm. Accordingly, it remains to be seen whether States should do their utmost to terminate and mitigate a cyber operation that stems from their territory and is to the detriment of the legal rights of other States, or whether they should also do their utmost to prevent such operations from ever materializing in the first place.
- Another divergent interpretation appears to relate to the concept of an internationally wrongful act. The language of the norm currently limits expectations related to acts by non-State actors. It also creates a doctrinal discrepancy between the norm, the bulk of national positions, and the additional lawyer of understanding provided by the 2021 GGE report.
- It also cannot be said with certainty whether the nowrm is triggered by all cyber operations in contravention to the legal rights of another State or whether the expectations related to termination, mitigation, and possibly prevention are limited to cyber operations that reach the threshold of serious adverse consequences. The latter concept is heavily circumstance-sdependent.
- National positions also remain divided on the question of whether the responsibility for failing to do the utmost to stop, mitigate, or prevent cyber operations in question is triggered only when the State of origin or transit knew or whether it also applies if it is established that the State should have known of the outgoing malicious traffic.
- A related outstanding interpretation issue is of the relative expectations of the State of origin and of the States of transit. It appears that the norm lays down the same expectations and standards for both, although from technical and practical standpoints, their abilities to in fact do their utmost to, for example, terminate a malicious cyber conduct may not be equal.

It is hoped that this paper will facilitate future discussions on the various elements of the GGE norm C and help the international policy- and law-making community reach agreement on interpretation. This would enable States to operationalize the norm and therefore utilize the framework of mutual international assurance also in the context of conduct involving ICTs.

1. Context and content

International law is the cornerstone of peaceful and stable international relations.[1] This was the case in 1945 and it continues to be so today, even in the context of cyberspace.[2] While the development of information and communications technologies (ICTs) has indeed endowed the world with many benefits, the proliferation of malicious uses of ICTs can pose a threat to the international legal rights and obligations of States. This may undermine international peace and security as well as increase the likelihood of conflict among nations.[3]

Although public international law generally only manages the relationships among States, the capacity to deprive other States of their legal rights by cyber means is not a monopoly of States.[4] The relative low cost of cyber operations and the interconnectedness of our networks provide opportunity for relatively small malicious groups to interfere with the sovereign prerogatives of a State. This could, for example, include interference with a State's choice of political governance system or the exploitation of its natural wealth and resources.[5]

In addition to democratizing the threat, ICTs allow for violation of international legal rights on a much larger scale and can remain undetected for several years. According to the Disarmament Agenda of the United Nations Secretary-General, "[g]rowth in global interconnectivity means that the frequency and impact of such attacks could be increasingly widespread, affecting an exponential number of systems or networks at the same time".[6]

A cyber operation named RedOctober, for instance, targeted various diplomatic establishments around the world and lasted for more than five years. It allowed the perpetrators to misappropriate what amounted to hundreds of terabytes of data.[7] The operation, which is suspected of having been carried out by non-State actors, deprived the targeted States of their legal right to the inviolability of diplomatic communication and archives, outlined in the articles 27 and 24 of the 1961 Vienna Convention on the Diplomatic Law, respectively.

1.1. Norm C of the UN Group of Governmental Experts

To reinforce the rule of international law in the cyber era and therefore cooperatively "reduce risks to international peace, security and stability",[8] in late 2015, the United Nations General Assembly adopted the recommendations of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, guiding States in their use of ICTs in the context of international relations.[9] One of the voluntary norms – norm C – submits that "**States should not knowingly allow their territory to be used for inter-nationally wrongful acts using ICTs**".[10] The significance of the norm

1 UNGA (2014).
2 United Nations Charter (1945, Art 1); UNGA (2019a). See also UNGA (2021a, para 69).
3 UNGA (2021c).
4 "States and non -State actors are rapidly increasing their cybercapabilities and developing increasingly sophisticated cyberarsenals." UNGA (2020a).
5 UNGA (1962, Art 1).
6 UN Secretary General (2018, 56).
7 Kaspersky GRAT (2013).
8 UNGA (2019a).
9 UNGA (2015a).
10 UNGA (2015b, para 13(c)).

in cyberspace has been recognized in the Disarmament Agenda of the United Nations Secretary-General, and the consensual 2021 GGE report provided an additional layer of understanding.

In accordance with the norm, States must not only comply with international law but are also expected to do their utmost to not allow their territory from being used for internationally wrongful acts. As such, the central purpose of the norm is to promote reciprocalprotection of the international legal rights of States and decentralized safeguarding of the rule of international law.

The notion of reciprocal protection of international legal rights is certainly not new in international relations and has previously found traction in, inter alia, the context of revolutionary activities by non-State actors against foreign States and of protection of aliens abroad.[11] The norm is in line with the good neighbourliness principle of international law, as found in the so-called Friendly Relations Declaration of 1970.[12]

1.2. Purpose of this paper

Research by the UNIDIR Security and Technology Programme aims to assist the international community in implementing the necessary measures needed for operationalizing the norms of responsible State behaviour in cyberspace. However, **to enable implementation, the content and scope of these norms need to be elaborated**. As presented in this paper, States have diverging opinions on several aspects of the norm C. This research attempts to address the need for clarity and identify open questions that are hindering further development of the norm and national implementation efforts.

First, this paper outlines the convergences and divergences in interpretations of the normative expectations and elaborates the legal and conceptual roots of the diverging national positions. Convergences in interpretation signal a consolidating approach to the understanding of the norm.[13]

Moreover, the exposition of the interpretation divergences offers guidance to future international negotiations of relevance. These processes have the potential to reduce the normative ambiguity, narrow the interpretation gap, and therefore to facilitate the implementation of necessary national measures and ultimately promote compliance with the norm.

The exposition of divergent views also represents a collection of State practices as well as the relevant underlying principles of international law; as such, the paper should therefore be valuable to the part of the international community that has yet to take an individual position on interpretation of the norm.

1.3. Structure of the paper

The structure of the paper follows the spectrum of the national interpretations of the norm C. Generally speaking, the interpretations of the normative elements can be classified as narrow or broad. **Narrow interpretation** restricts the scope of the norm and reduces the extent of expectations imposed on States and consequentially the burden of compliance. A limited extent of expectations imposed by the norm means that compliance will be, in theory, easier to attain. This is particularly important given the spectrum of national capacities related to cybersecurity and the fact that compliance with every

11 Lauterpacht (1928, 105–130).
12 UNGA (1970).
13 Chayes and Chayes (1993, 175–205).

individual normative expectation, even when a compliance standard is flexible and commensurate with the capacities of a State, incurs certain costs.[14] The smaller burden imposed by the narrow interpretation of the norm may also promote higher levels of compliance. At the same time, and as seen in the following sections, a narrow interpretation imposing a smaller burden has limited potential for effective reciprocal protection of the international legal rights of States in cyberspace.

Conversely, a **wide interpretation** of normative expectations is more ambitious. By increasing expectations, it increases the costs and burden of compliance on States. As such, a wide interpretation has the potential to amplify the effectiveness of the norm and enhance protection of the rule of law. However, it may also be seen as too ambitious and too taxing on States, thus discouraging adherence.

To this end, and beyond this introductory section, this paper is structured as follows:

Section 2 provides thoughts on classification of the norm and sets the methodological limitations of the paper.

Section 3 addresses interpretations of the conditions embedded in the norm, namely the conditions of knowledge of the origin and actor and potential thresholds.

Section 4 focuses on possible specific requirements of the norm, including emerging (international minimum) standards of conduct.

Section 5 envisions some of the possible issues arising from the divergent interpretations of the norm.

Finally, **section 6** offers concluding thoughts and suggestions for ways forward.

14 "[I]mplementation and compliance require monetary and bureaucratic resources." Jacobson and Weiss (1995, 127).

2. Due diligence and normative standards

2.1. Norm or rule or principle?

A first divergence among the positions related to the aforementioned norm is one of classification. While some States have made it clear that they believe that reciprocal protection of international legal rights is an expectation of voluntary behaviour,[15] a number of States argue that the norm in fact reflects a rule of customary international law.[16] Given the consensual nature of the GGE reports of 2015 and 2021, this paper does not scrutinize the issue of classification and does not question the nature of the norm. Instead, it rests on the consensual conclusions of the GGE, accepting the voluntary nature of the norm.

What is the difference?

In brief (and consciously deficient of legal nuances), norms of responsible State behaviour in cyberspace can be seen as pronouncements of acceptable behaviour or declarations of expectation about the conduct of States in the context of the use of ICTs in international affairs.[17] As such, they are voluntary in nature, which is reiterated by the GGE reports of 2015 and 2021.[18]

Thus, non-compliance with the norms, in principle, carries no legal consequences. Norms, sometimes seen a soft law,[19] can nonetheless attract political reaction from the international community and, in the worst case, retorsion (which is unfriendly reactions that remain well within the limits of international law).[20]

15 For example, as stipulated by New Zealand, "[w]hether this norm also reflects a binding legal obligation is not settled. … New Zealand is not yet convinced that a cyber-specific 'due diligence' obligation has crystallized in international law." New Zealand (2020, para 16 & 17). A similar argument was put forward by the United Kingdom: "[T]he fact that States have referred to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace." UNGA (2021b, 117).

16 See, for example, the position of Finland: "It is clear that States have an obligation not to knowingly allow their territory to be used for activities that cause serious harm to other States, whether using ICTs or otherwise." *Statement by Ambassador Janne Taalas at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security* (2018). Similar positions adopted by, for example, the Netherlands (The Netherlands (2019, Appendix 1); France (Ministère des Armées (2019)); Germany (German Federal Foreign Office and the German Federal Ministry of Defence (2021)); Chile, Ecuador, Guatemala, Guyana, and Peru (Inter-American Juridical Committee (2020, 33)). Czech Republic even suggested the norm should be included in the International Law section of the 2021 report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security. Ministry of Foreign Affairs of the Czech Republic (2020, para V).

17 For a succinct overview on the instrumentality of norms and international law, see Finnemore (2017).

18 UNGA (2015b, para 10); UNGA (2021a, para 15).

19 The soft versus hard law dichotomy can sometimes be too simplistic. See for example Pronto (2015).

20 On retorsion, see for example Giegerich (2020).

Conversely, international legal rules represent the obligations of States, as found in sources of international law such as treaties, customary international law, general principles of law recognized by civilized nations,[21] judicial decisions, and the writings of the most prominent scholars.[22]

Principles of international law are more general pronouncements of the fundamental objectives of law.[23] They lack technical precision, methods, or criteria related to the attainment of these objectives.[24] Principles of international law can therefore serve a different purpose and may be useful for systematizing or interpreting legal rules.[25] They do not automatically impose legal obligations,[26] even if they give rise to specific legal obligations.[27]

2.2. Due diligence principle

The norm in question is based on the due diligence principle of international law. Although this argument has not been completely devoid of controversy,[28] is has been in fact supported by a number of the individual national statements[29] as well as by the plethora of conceptualisations of the due diligence principle provided in the past by international judiciary entities.

Several decisions of international judiciary entities have revolved around the due diligence principle. For instance, in the Island of Palmas case of 1928, the Permanent Court of Arbitration was tasked to decide on a territorial dispute between the Netherlands and the United States of America. The arbitration rejected the notion of absolute territorial sovereignty; the arbitrator, Max Huber, argued that "[t]erritorial sovereignty ... has as corollary a duty: the obligation to protect within the territory the rights of other States".[30] Another oft-publicized conceptualization of the due diligence principle of international law can be traced back to a seminal case of the International Court of Justice (ICJ), which argued in the Corfu Channel Case that a State is "not to allow knowingly its territory to be used for acts contrary to the rights of other States".[31] The resemblance between the language of the ICJ and the GGE norm C is apparent.

2.3. Standards of compliance

Standards of compliance with the international obligations and expectations deriving from the due diligence principle are flexible and commensurate with the capabilities of a State. It is therefore expected that States do their utmost to not allow their territory to be used for internationally wrongful cyber operations. This was clearly expressed in the 2021 GGE report.[32] It has also been promoted by some States in their individual positions related to the due diligence principle.[33]

21 Not to be conflated with the principles of international law. See, for example, Wood (2019); UNGA (2020b).
22 *Statute of the International Court of Justice* (1945, Art 38).
23 ICJ (1984, para 79).
24 ICJ (1984, paras 79–81).
25 Wolfrum (2010).
26 ICJ (2018, para 93).
27 The example here being the prohibition of the use of force. See, for example, Paulus (2012, 121). In the context of cyberspace, some States take the position that sovereignty is not only an applicable legal principle but also a rule of international law. See, for example, Ministry of Foreign Affairs of Japan (2021, para 2) suggesting that "[i]n some cases, a violation of sovereignty constitutes a violation of international law even when it does not fall within the scope of unlawful intervention."
28 UNDIR (2021).
29 See, for example, Republic of Korea (2020a); Ministry of Foreigsn Affairs of Japan (2021, 5).
30 *Island of Palmas case (Netherlands v USA)* (1928).
31 ICJ (1949, 22). See also ICJ (2010, para 101).
32 "The norm raises the expectation that a State will take reasonable steps within its capacity". UNGA (2021a, para 30(a)). On possible minimum standards, see section 3.1.
33 Japan, for example, argued that, in determining compliance with the due diligence obligations, "it seems necessary to consider on a case-by-case-basis the scope of the obligation taking into account such factors as the seriousness of the cyber operations in question and the capacity of the territorial States to influence a person or group of persons conducting the attacks." UNGA (2021b, 48).

Additionally, States should take preparatory steps enabling them to meet the expectations imposed by the norm. In other words, the "all appropriate and reasonably available and feasible steps"[34] suggests that States should keep abreast of advancements in technology and science and strive to build capacity prior to the disturbing situation which would require them to act.[35] This is a well-established notion of the due diligence obligations in the context of international environmental law and beyond,[36] which some States have introduced into the discourse on due diligence in the context of the GGE norm in question.[37] Past international arbitration decisions suggest that more diligence is expected from States with more resources and capacities relevant to cybersecurity.[38]

What is appropriate and reasonable depends not only on capacity but on wider context, including the state of technology.[39] Thus, the standard of due diligence expectations "may change over time";[40] actions not seen as reasonable a decade ago may very well be considered prudent today. Developments in the fields of artificial intelligence (AI) and quantum computing and the eventual proliferation of related cybersecurity tools are among some of the developments that may affect the normative expectations of compliance in the future.[41]

2.4. Primary and secondary rules of international law

Where appropriate, primary rules of international law are brought to attention by this paper to illustrate the origins of the divergent positions of interpretation of the norm. In fact, as indicated throughout this paper, established international law provides the foundation for many of the interpretation attempts; of particular interest is, for example, ICJ jurisprudence, which has served as an inspiration for many national positions related to the due diligence expectations in cyberspace.

The paper also elaborates the relevant parts of the secondary rules of international law, namely the international customary law of State responsibility. In this, it pays particular attention to the provisions of an internationally wrongful act, the concept which is at the heart of the norm C.

However, this paper does not attempt to delve into the primary rules of international law in cyberspace and does not seek to explain tangibly which specific acts or omissions using ICTs should be considered as a breach of international obligations. This paper also disregards the larger context of international legal rights. As the norm C is a product of a process that considers the use of ICTs in the context of international peace and security, cyber operations which could have a negative impact on the international legal rights of individuals are beyond the scope of this paper.

34 UNGA (2021a, para 29).
35 "[D]ue diligence in ensuring safety requires a State to keep abreast of technological changes and scientific developments". ILC (2001a, 146, art 3 cmt 11).
36 See e.g. ILC (2001a, 146, art 3 cmt 11); *L. F. H. Neer and Pauline Neer (U.S.A.) v United Mexican States* (1926, 62): the lack of diligence can stem from "the insufficiency proceeds from deficient execution of an intelligent law or from the fact that the laws of the country do not empower the authorities to measure up to international standards".
37 Finland (2020, 4).
38 "[D]iligence is proportioned to the magnitude of the subject and to the dignity and strength of the power which is to exercise it." *Alabama case (United States of America v Great Britain)* (1872, 572). Note also Principle 11 of UNGA (1992): "Standards applied by some countries may be inappropriate and of unwarranted economic and social cost to other countries, in particular developing countries."
39 According to Japan, the due diligence principle imposes flexible standard of compliance, which is based on "factors as the seriousness of the cyber operations in question and the capacity of the territorial States to influence a person or group of persons conducting the attacks." Ministry of Foreign Affairs of Japan (2021, 5).
40 ITLOS (2011, para 117).
41 Chan et al. (2019); IBM Institute for Business Value (2018).

3. Scope of normative expectations

This section explores what is in fact expected of States in order to comply with the norm C, which sets the expectations that States will not allow their territories to be used for internationally wrongful cyber acts. Negative expectations leave a certain level of ambiguity and discretion as to the methodology of compliance. The following subsections thus elaborate on the developing national views on the possible venues of compliance and potential international minimum standards.

3.1. Prevention, termination or mitigation?

> "State should **not** knowingly **allow** their territory to be used for internationally wrongful acts using ICTs."

It remains to be elucidated what it means for States not to allow certain cyber activity on their territories or, in other words, whether a State is expected to do its utmost to act proactively or merely react to already-materialized malicious cyber operations contrary to other States' international rights.

Doctrinally, the principle of due diligence imposes expectations of prevention.[42] This thus suggests a **wide interpretation** of the norm. Indeed, this is the position of a number of States; according to Chile, for example, States "must exercise due diligence to *prevent* its sovereign territory, including the cyber infrastructure under its control, from being used to carry out cyber operations that affect another State's rights".[43] This expanded interpretation is not a unique proposition; a joint statement by the Group of Seven (G7) elaborating on implementation efforts argues that States have "taken active measures to *prevent and discourage*"[44] their territories from being used to commit cyber operations to the detriment of the international rights of other States.[45]

Wide interpretation promotes preventive and proactive protection of the international rule of law. However, it also requires additional activities related to prevention, which raises the compliance costs by necessitating, for instance, enacting and implementing law, policy, and technical solutions and maintaining an up-to-date capacity to monitor ICT activity in a particular territory as well as technical and legal mechanisms to react rapidly to an imminent outgoing cyber operation before it materializes. Wide interpretation also extends the temporal aspect of the expectations – prevention requires the State to act diligently well before the incident occurs, which is again more taxing on the State.

Be that as it may, the 2021 GGE report rejected such expansive interpretation, arguing that States are expected to attempt "*to end* the ongoing activity in its territory".[46] This **narrow interpretation** of the norm is in line

42 See, for example, *Alabama claims of the United States of America against Great Britain* (1871); ICJ (1949, 23); ICJ (2005, 187).
43 Inter-American Juridical Committee (2020, para 58).
44 G7 (2019, 2).
45 See also Croatia, Finland, France, and Slovenia: "States should be encouraged to take measures to prevent non-State actors, including the private sector, from conducting ICT activities for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State's territory."; Canada: "States should be encouraged to ensure that non-State actors, including the private sector, are prevented from conducting malicious ICT activities for their own purposes or those of State or other non-State actors to the detriment of third parties including those located on another State's territory." UNGA (2021d).
46 UNGA (2021a, para 30(a)) [emphasis added].

with the individual positions of several States.[47] It suggests that a State is expected only to react to an existing internationally wrongful cyber operation stemming from its territory and should therefore attempt to employ its best efforts to terminate that cyber operation.

A narrow interpretation of the norm restricts the scope of expectations of States whose territories serve as a launchpad for cyber operations contrary to the international rights of the targeted States. Accordingly, States are only expected to attempt to respond to an ongoing incident and not also to prevent the incident from occurring in the first place.

In accordance with the narrow interpretation of the norm, and in particular when attempting to terminate a cyber operation is not a reasonable expectation, States may also be expected to do their utmost to mitigate negative consequences of that cyber operation. In the context of compliance with the norm, Canada, for instance, vows "to take appropriate action *to contain* the harmful behaviour",[48] a view also expressed in their comment to the pre-draft report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG).[49] A number of other States have taken a similar position.[50]

3.2. Capacity building and possible minimum standards of compliance

Whether due diligence encompasses expectations of prevention or only of termination and mitigation, prudence dictates the building of the enabling capacities. Given that norm C does not expect States to actually stop or prevent internationally wrongful cyber operations stemming from their territory but only to employ their best efforts to do so, there is no expectation as to the methodology and therefore no prescription for specific capacities. To facilitate termination, mitigation, or prevention, States could invest in: [51]

- Developing incident-response plans and corresponding mechanisms
- Enacting and implementing domestic policy and normative frameworks
- Raising awareness
- Developing enabling structures and cooperative partnerships (domestic and international)
- Designating a national point of contact

Although due diligence dictates a flexible standard of compliance, certain activities may be reasonably expected from all States. The first of the standards is the expectation

47 See, for example, Australia (The Department of Foreign Affairs and Trade (2017)) "if a state *is aware* of an internationally wrongful act originating from or routed through its territory, and it has the ability *to put an end to the harmful activity*, that state should take reasonable steps to do so." [emphasis added]; Netherlands (The Netherlands (2019, Appendix 1) 4) "Netherlands may, on the basis of the due diligence principle, ask the other country to shut down the servers." [emphasis added]; Ecuador (UNGA (2021d) "this norm should not be interpreted as requiring a state […] *to take other preventive steps*." [emphasis added].

48 Canada (2019) [emphasis added]. A similar position was taken by the Republic of Korea, which argued that "the notified State should, in accordance with international and domestic law and within their capacity, take all reasonable steps, within their territory, to cause these activities to cease, or to *mitigate its consequences*." Republic of Korea (2020, 5) [emphasis added].

49 OEWG (2020, 2).

50 Note also, for example, statements by Ecuador and the Republic of Korea. OEWG (2020, 6 & 8).

51 List inspired by norm-implementation reports of Republic of Korea (2020b); Canada (2019); UK (Foreign and Commonwealth Office (2019)) and Australia (2019).

of **notification**. The principle of due diligence suggests that a State whose territory is used for a cyber operation in contravention of international rights should at least notify the targeted States. This is well-established by the jurisprudence[52] as well as by expectations of analogues regimes, including international environmental law.[53] What is more, several States have emphasized the expectation of notification in their individual positions.[54] In line with the good faith principle,[55] the notification should be transferred to the targeted State without undue delay.[56]

Another related expectation is that of response to the notification. A State notified that its territory is used for cyber operations to the detriment of the international legal rights of another State should "**acknowledge** receipt of the notification"[57] before making an attempt to put a stop to the operation or to mitigate the operation in good faith. Once again, and in addition to the 2021 GGE report, this expectation seems to have support from certain individual national positions.[58]

In attempting to comply with the norm, a State lacking the capacity to terminate or mitigate a cyber operation stemming from its territory is encouraged to **seek help** from other States and the private sector.[59] While a suggestion to seek help from other entities is not a novel proposition and has been previously promoted by certain legal regimes,[60] the inclusion of the private sector would indeed appear to be unique to cyberspace.

As technology changes and State practice evolves, other minimum expectations may develop over time. What is clear at the time of writing is that States are not expected to monitor all ICT activities within their territory in order to proactively identify activity that may have a negative impact on international legal rights.[61]

52 For example, in the Corfu Channel case, ICJ decided Albania incurred international responsibility for its omission to notify and warn the British navy of the dangers of the mines laid in the Corfu straight. ICJ (1949, 10).
53 ILC (1994, 129 art 28); ILC (1996).
54 See, for example, similar statements by Canada and Ecuador. OEWG (2020, 1 & 7).
55 UNGA (2021a).
56 ILC (1996, 29 para 36).
57 UNGA (2021a, para 30).
58 For example, Canada and Ecuador. UNGA (2021d).
59 UNGA (2021a, para 30b).
60 "States concerned shall cooperate in good faith and, as necessary, seek the assistance of one or more *competent international organizations* in preventing significant transboundary harm or at any event in minimizing the risk thereof." ILC (2001a, 146 art 4) [emphasis added].
61 UNGA (2021a).


mirror_mod.use_y
mirror_mod.use_z
elif _operation == "MIRR
mirror_mod.use_x
mirror_mod.use_y
mirror_mod.use_z
#selection at the e
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.object
print("Selected" + str(
#mirror_ob.select

4. Normative conditions

The normative expectations outlined above are subject to several conditions. Just as in the of case the scope of the expectations, interpretation of the conditions triggering the norm are subject to divergent interpretations. Concepts in need of future discussion are the concepts of knowledge, threshold, the internationally wrongful act and territorial jurisdiction.

The following subsections elaborate the differences in interpretation of each of these terms in turn with a view to facilitating future international discussions on the norm in question.

4.1. Actual or constructive knowledge

> "State should not **knowingly** allow their territory to be used for internationally wrongful acts using ICTs."

The first condition limiting the applicability of the norm is that of knowledge. According to the norm, States are only expected to terminate or mitigate cyber operations of which they are aware or have actual knowledge. This is a **narrow interpretation** of the norm, creating the expectation that a State should only act or react in relation to a known cyber operation stemming from its territory.

Works of international legal scholarship have argued in favour of actual knowledge in the context of the principle of due diligence in cyberspace.[62] Past decisions of international judiciary bodies have also established State responsibility based on evidence of actual knowledge.[63] The individual positions of some States support this interpretation.[64]

However, this is not a universally accepted interpretation, and the norm could also be subject to a **wider interpretation**. Accordingly, it could be argued that a State fails to meet the normative expectation when it does not employ its best efforts to prevent a cyber operation about which it should know.

Jurisprudence labels this concept as constructive knowledge. The individual positions of Finland,[65] the Netherlands,[66] Norway,[67] Romania,[68] and Switzerland[69] related to due diligence in the context of State conduct using ICTs have all argued in favour of the constructive knowledge condition. Their position has also been endorsed by the scholarship.[70] It has its origins in ICJ jurisprudence, namely the Corfu Channel case and the Application of Genocide Convention case.[71]

62 Due diligence arises if organs of a State "have detected a cyber operation … originating from its territory or if the aggrieved party to the conflict has credibly informed the [State] that a cyber operation has originated from its territory". Schmitt (2013, rule 93 para 5).
63 *Alabama claims of the United States of America against Great Britain* (1871, 125–134); ICJ (1980).
64 "New Zealand considers it should apply only where states have *actual, rather than constructive, knowledge* of the malicious activity, and should only require states to take reasonable steps within their capacity to bring the activity to an end." New Zealand (2020, paras 16 & 17) [emphasis added]. Note also the remarks by the United States, arguing that "*[W]hen a state is notified* of harmful activity emanating from its own territory, it must take reasonable steps to address it." United States Mission to the United Nations (2021) [emphasis added].
65 Finland (2020, 4).
66 The Netherlands (2019, Appendix 1, 4).
67 "In addition to actual knowledge of the use of cyber infrastructure within its territory for harmful cyber operations against another State, a State may also violate its due diligence obligation if it is in fact unaware of the activities in question but objectively should have known about them and fails to address the situation." UNGA (2021b, 71).
68 UNGA (2021b, 75).
69 "[A] state that is or *should be aware* of cyber incidents that violate the rights of another state is obliged to take all reasonable measures that are appropriate to stop or minimize the risks of such incidents" Federal Department of Foreign Affairs (2021, 7) [emphasis added].
70 Akande et al. (2020).
71 ICJ (1949). "[F]or it to incur responsibility on this basis it is enough that the State was aware, or *should normally have been aware*, of the serious danger that acts of genocide would be committed". ICJ (2007, para 432) [emphasis added].

To establish whether a State should have known of a cyber operation stemming from its territory, one must take into account the capacity of that State to detect the outgoing malicious activity, the technical feasibility to do so, as well as its past performance related the monitoring of its networks for such activities.[72]

By placing the expectation of stopping or mitigating injurious cyber operations on the State that should have known of the malicious activities stemming from its territory, the wide interpretation has the potential to elevate the effectiveness of the norm. The wide interpretation would prevent a State from excusing non-diligent behaviour with arguments that it had no knowledge of an outgoing cyber operation in contravention to the rights of another State, particularly when the capacity to detect and past performance of the former are undisputed. What might be considered as a high normative burden is not particularly problematic in the light of the voluntary nature of the expectations and in the absence of legal consequences in the event of non-compliance.

On the other hand, at least three arguments may be advanced against the wide interpretation. First, the additional layer of understanding provided by the GGE in 2021[73] and a number of individual State opinions offer a possible convergence on the interpretation, this being that States are not expected to proactively monitor the ICT infrastructure under their jurisdiction in order to attain compliance with this norm.[74] Second, the international case law laying the foundation for recognition of the constructive knowledge condition was set in very particular contexts: interpretation of the due diligence obligations under the Genocide Convention;[75] and the responsibility for the material damage, and loss of human life in the Corfu strait.[76] Third, there seems to be an expectation that the States targeted by a cyber operation will inform the State of emanation or of transit and will request termination.[77] This would provide the latter State with the actual knowledge of the cyber operation but it does also raise questions on the capacity and the ability of the targeted State to determine the origin of a cyber operation.

4.2. The concept of an internationally wrongful act

> "State should not knowingly allow their territory to be used for **internationally wrongful** acts using ICTs."

This section attempts to outline possible interpretations of the characterization of a cyber operation as internationally wrongful. In other words, it determines which cyber operations stemming from its territory a State should attempt to terminate, mitigate, or possibly prevent.

An act or omission (or a combination of both) can be characterized as internationally wrongful when it constitutes a breach of international obligations and, consequentially, a violation of international rights corollary to those obligations.[78] Traditionally, international law governs the relationships between States and does not directly stipulate international obligations of individuals or natural persons.

72 This two-part test of constructive knowledge was developed by the ICJ in the Corfu Channel case. It remains to be seen whether the test will stand the test of time and can in fact accommodate the cyber environment. ICJ (1949, 20).
73 UNGA (2021a, para 30(a)).
74 See, for example, Ecuador arguing "this norm should not be interpreted as requiring a state to monitor proactively all ICTs within its territory, or to take other preventive steps". UNGA (2021d).
75 ICJ (2007).
76 ICJ (1949).
77 UNGA (2021a, para 30(c)).
78 Generally speaking, "there are no international obligations of a subject of international law which are not matched by an international right of another subject or subjects, or even of the totality of the other subjects." ILC (2001b, ch IV art 2 cmt 8).

Accordingly, an internationally wrongful act using ICTs can only be perpetrated by the principal bearer of international obligations – a State.

A **narrow interpretation** of the norm would thus suggest that States are not to allow their territory to be used for internationally wrongful acts of a State. The classification of conduct as an internationally wrongful act of a State is guided by the established customary international law, collected and elaborated upon by the International Law Commission in its *Articles on Responsibility of States for Internationally Wrongful Acts*.[79] In brief, a breach is considered to be internationally wrongful only when it is attributable to a State, be it directly or indirectly.[80]

This is, however, in contradiction to the additional layer of understanding provided by the 2021 GGE report, indicating that the norm expectations extend to internationally wrong-ful acts of independent non-State actors,[81] a view supported by a number of individual national positions.[82] It could be considered as a **wider interpretation** of the norm. Given the growing concern over the use of non-State proxy actors to conduct malicious ICT acts,[83] extending the expectation to do the utmost to constrain non-State actors from conducting malicious ICT acts would indeed strengthen the normative protection of the international rights of States.

Nevertheless, non-State actors bare no responsibility for internationally wrongful acts, the latter being a distinct doctrinal category of the international law of State responsibility. Certain acts contrary to international law that are conducted by non-State actors and not attributed to a State can amount to an international crime but strictly speaking do not constitute an internationally wrongful act.[84] Indeed, the progressive development of the law,[85] the outcomes of the Nuremberg trials,[86] and the establishment of the International Criminal Court[87] and the ad hoc international criminal tribunals for the former Yugoslavia[88] and Rwanda[89] suggest that non-State actors can be individually responsible for certain international crimes – such as war crimes, crimes against humanity, genocide, or aggression by use of armed forces not attributable to a State.[90]

To ensure that the norm covers the ICT acts of non-State actors contrary to the rights of the States and to synchronize the norm with the GGE's additional layer of understanding, reconceptualization of the norm is proposed by this paper. Using the language of the ICJ's Corfu Channel case, the norm could set the expectation of a State "not to allow knowingly its territory to be used for acts contrary to the rights of other States".[91] Such a norm would exhibit the expectations related to

79 UNGA (2002, Annex).
80 UNGA (2002, Annex, art 5); UNGA (2002, Annex arts 6–11).
81 "[A] State should not permit another State or non-State actor to use ICTs within its territory to commit internationally wrongful acts". UNGA (2021a, para 29)
82 For example, Romania argued "[t]he due diligence principle entails that a State may be responsible for the effects of the conduct of private persons, if it failed to take necessary measures to prevent those effects." UNGA (2021b). A similar position was taken by Canada (UNGA (2021d).
83 UNGA (2021a, para 71(g)).
84 Individual criminal responsibility and State responsibility are not mutually exclusive. See Nollkaemper (2003).
85 Clapham (2010, 25–30).
86 Nuremberg Military Tribunals (1946).
87 *Rome Statute of the International Criminal Court* (1998, arts 21 & 25).
88 International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991 (2009, art 1).
89 UNSC (1994).
90 "The term 'individual responsibility' has acquired an accepted meaning in light of the Rome Statute and other instruments; it refers to the responsibility of individual persons, including State officials, under certain rules of international law for conduct such as genocide, war crimes and crimes against humanity." ILC (2001b, art 58, cmt 4). See also *Rome Statute of the International Criminal Court* (1998, arts 5–8).
91 ICJ (1949, 22) [emphasis added].

ICT acts detrimental to the rights of States, performed by States as well as non-State actors. At the same time, it would cover any conduct that deprives another State of its international rights, not only the cyber conduct amounting to the gravest violations of the international law, such as genocide. The proposed reconceptualization would not only promote a robust normative protection of the international rights of States but would also harmonize the norm with the existing doctrinal understanding of internationally wrongful act.

4.3. Any cyber operation contrary to the rights of another State?

The norm C itself provides no additional qualifiers or thresholds in relation to cyber operations contrary to the international rights of other States. Accordingly, it would appear that the choice of words of the norm proposes a **wide interpretation** of the norm according to which States are to do their utmost to prevent any cyber conduct contrary to the international rights of other States stemming from their territory, regardless of the magnitude and intensity of the (likely) effects.

Some States favour a **narrow interpretation** of the normative expectations. The Netherlands, for instance, has argued that "it is generally accepted that the due diligence principle applies only if the State whose right or rights have been violated suffers sufficiently serious adverse consequences."[92] This threshold can also be traced back to several other official national positions.[93] It also has roots in the scholarship.[94]

The threshold, which originates in international environmental law,[95] is not well-defined in international law, let alone in the context of cyber operations. Nevertheless, it may be reasonable to argue that a cyber operation that is likely to result in damage to physical infrastructure or injury to human beings would reach the proposed threshold, putting the State of origin or transit under the expectation to terminate, mitigate, or possibly even prevent the operation. A cyber operation against critical infrastructure is another example of conduct that has the potential to produce serious adverse effects.[96] Beyond this, the proposed threshold of the narrow interpretation depends on the context, including but not limited to the type and resilience of the targeted infrastructure.

4.4. States of origin versus the States of transit

> "State should not knowingly allow **their territory** to be used for internationally wrongful acts using ICTs."

The fourth condition pertaining to the normative expectations relates to the concept of territorial sovereignty. A **narrow interpretation** of the norm would suggest that due diligence is only expected from the State

92 The Netherlands (2019, Appendix 1, 5).

93 Ecuador (UNGA (2021d)) argues States are expected to employ best efforts so that their territory is not used 93for an internationally wrongful act that is likely to produce serious adverse consequences in another State"; Finland (Finland (2020, 4)) argues "States may … not knowingly allow their territory, or cyber infrastructure within a territory under their control, to be used to cyber operations that produce serious adverse consequences for other States." See also similar positions advanced by Canada (UNGA (2021d)); Romania (UNGA (2021b, 75)); and Norway (UNGA (2021b, 71)).

94 Schmitt (2017, rule 6 cmts 29–31).

95 "[N]o State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, *when the case is of serious consequence* and the injury is established by clear and convincing evidence." *Trail smelter case (United States, Canada)* (1938 & 1941, 1965) [emphasis added].

96 See UNGA (2015b, para 5); Egypt (2020): "The most harmful abuse of ICTs is related to the targeting of critical civilian infrastructure and associated information systems.". Similar argument is made by the ICRC (2019).

whose territory is the origin of a cyber operation contrary to the rights of other States. "Territory" encompasses all of the objects and subjects under the territorial jurisdiction of a particular sovereign State.[97]

A **wider interpretation**, on the other hand, equates the State of origin with any State of transit, and thus imposes the expectations of due diligence also on any State whose territory is used merely as a transit for a cyber operation contrary to another State's international rights. Support for extending the normative expectations to States of transit may be found in the additional layer of understanding provided by the 2021 GGE report as well as in the prior individual position of France.[98] Other States do not appear to have taken a clear position regarding this issue of interpretation.

There is a benefit to extending the normative expectation to transit States. Malicious cyber operations may utilize a dispersed network of intermediary infrastructures in order to obfuscate the origin of the operation.[99] Also, certain types of malicious cyber operations rely on a large number of distributed networks of machines located in different territories, overwhelming the target through orchestration and thus rendering it inoperable.[100] By extending the normative expectation, the theoretical potential to successfully terminate or mitigate a malicious cyber operation and therefore protect the legal rights of the targeted State is increased.

There are also concerns associated with the expanded interpretation of the norm. First, if the infrastructure of the State of transit enables only a small fraction of the functionality of a larger cyber operation, the extent to which the States of transit can become aware of the malicious cyber operation is unclear. What are the odds that a State of transit, which may not be expected to proactively monitor its territories for malicious activity transiting their territory,[101] can proactively acquire knowledge of such activity? Can States of transit be responsible for not meeting the normative expectations based on the constructive knowledge test and the proclamation that they should have known of the transiting cyber operation?

Second, it is not yet entirely clear whether the standard of expected behaviour is different for States of transit compared to the behaviour expected of the State of origin. From a technical standpoint, is it reasonable to expect that a transit State can meaningfully contribute to termination of cyber operations that deprive other States of their legal rights? Cyber operations can indeed be modular, flexible, and thus complex, and disabling one of the enabling, central command units in a web of infected machines may only make a dent in a malicious operation comprised of several hundred such units.[102] This is the case with distributed denial of service (DDoS) operations, which are highly decentralized; during the DDoS operation against the Estonian systems in 2007, the traffic was

97 "States have jurisdiction over the ICT infrastructure located within their territory". UNGA (2015b, para 28(a)). See also scholarship contribution by Goldsmith (1999).
98 UNGA (2019b, 24).
99 TrendMicro (2014).
100 See, for example, Kaspersky (2021).
101 See section 3.
102 See, for example, Sancho and Link (2011).

coming from infected computers in 178 countries.[103] Given the nature of the DDoS operation, not all of the 178 transit States could have known that their outgoing traffic was malicious in nature and not a legitimate visit, nor would blocking outgoing traffic from one network node have made any tangible impact on the DDoS operation, which could have included several hundred thousand participating malicious servers.[104]

Regardless of the interpretation that prevails in the future, the additional layer of understanding provided in 2021 is explicit: the mere fact that the territory of a particular State is being used for a cyber operation to the detriment of the international rights of another State does not involve automatic responsibility of the former State for the operation itself.[105] Indeed, responsibility for internationally wrongful acts is a matter of the secondary rules of international law and specific frameworks guiding the attribution.[106]

103 Heickerö (2010, 41).
104 For example, 2017 DDoS attack on Google involved 180.000 servers. Menscher (2020).
105 UNGA (2021a, para 30(d).
106 UNGA (2002, Annex, arts 2–4).

5. Possible consequences of the divergent interpretations

Norms outline expectations of the international community in relation to the behaviour of States in cyberspace. By outlining the frameworks of behaviour, norms facilitate the predictability of the conduct of States in cyberspace, thus providing a level of security. Specifically, norm C aims to provide a framework of reciprocal protection of the international legal rights of States and decentralized safeguarding of the rule of international law.

Although the 2021 GGE consensus report provides an additional layer of understanding and therefore adds a degree of normative precision, the norms remain a product of a negotiation process. This inherently leaves room for interpretation. There is no institutionalized, international body authorized to interpret and specify the normative expectations outlined by the GGE. In the absence of a judicial body providing interpretation or of any extensive commentary by the drafters providing the precision desired, the future of the norm is in the hands of the States.

The issue, as elaborated in this paper, is that the individual national interpretations are diverse, which may hinder implementation of measures needed for operationalization of the norms as well as compliance with the norms. Divergent interpretations foster ambiguity and may diminish the normative security as they do not steer the behaviour of States towards the predictable spectrum, thus jeopardizing the utility of the normative framework. In order to implement and therefore operationalize the norms of responsible State behaviour in cyberspace, the normative expectations need to be elaborated if not synchronized.

According to the scholarship on rational choice theory, reciprocity is one of the driving forces behind cooperation and, more specifically, compliance with norms.[107] Divergent interpretations can, however, reduce the potential for reciprocity in international relations. Although reciprocity is not the only agent of compliance, divergent interpretations can reduce the incentive to adhere to a norm if the scope of the expected conduct is not shared among the States and if reciprocity cannot reasonably be expected. For instance, the incentive to employ capacities to prevent a cyber operation to the detriment of another State's legal rights may be reduced if it is unclear whether reciprocity – that is, efforts to prevent – can be expected from the other State. The same compliance hesitation can be expected to arise from the differences surrounding the condition of knowledge: Should a State aim to develop the capacity to detect cyber operations stemming from its territory? Or should it only focus on cyber defence of its infrastructure and wait to be notified that its territory is the origin of a cyber operation on another State in contravention of international law?

Moreover, a reaction by the targeted State to conduct by another State that does not fit the latter's interpretation of the norm can in fact have a negative impact on international peace and security. Consider the following peacetime scenario. State A and State B have divergent views on the scope of the reciprocal protection norm: State A considers the norm to be applicable to both the State of origin and States of transit; State B has consistently favoured the narrow normative

107 See, for example, Axelrod (1984); Keohane (1984); Keohane (1986); Guzman (2010).

interpretation, arguing that diligence in relation to cyber operations depriving a State of its rights is only expected from the State whose territory is considered to be the origin of a cyber operation.

State A is targeted by a complex malicious cyber operation, effectively forcing it to scrap plans to sign a free trade agreement with a third State, thus depriving it of the sovereign prerogative to set its economic policy.[108] Technical investigation indicates that the origin of the operation cannot be reliably established. Evidence, however, dispels any doubt that the operation is traversing government-owned ICT infrastructure located in territory under the jurisdiction of State B.

State A notifies State B of the ongoing cyber operation and reminds it of the normative expectations. State B now has an actual knowledge of the cyber operation but refuses to respond to the notification. Given its narrow interpretation and the fact that the malicious act does not originate on territory under its jurisdiction, State B makes no meaningful attempts to stop or mitigate the malicious cyber operation in question.

For the sake of argument, envision that the targeted State A considers the norm to have in fact a character of an obligation under existing international law. Accordingly, it invokes the State responsibility of State B for acting in violation of its due diligence obligation vis-à-vis State A to not knowingly allow its territory to be used for acts contrary to the rights of State A. State A then takes what it believes to be lawful countermeasures, and demands (assurance of future) diligent behaviour and reparations from State B.[109]

In the eyes of State B, accused of non-diligent conduct, there was no international wrongdoing on its part, because State B only sees due diligence as a non-binding norm of responsible state behaviour. In the absence of any internationally wrongful act, countermeasures taken by State A are deemed to be a violation of the international rights of State B. The latter is now legally entitled to take countermeasures against State A, which may either trigger or escalate conflict between the two States.

108 Heickerö (2010, 41).
109 "Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State." UNGA (1970). See also ICJ (1986, para 205).

6. Conclusions and recommendations

Noting the ability of voluntary norms to strengthen peace, security, and stability in international relations, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security proposed a normative framework of mutual international assurance, based on the due diligence principle of international law. This paper provides an exposition of the divergences and convergences in national interpretations of the norm C, as formulated in the 2015 GGE report and later elaborated in the 2021 report, which suggests that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs".[110]

States are yet to reach an agreement on the scope of the norm, knowledge conditions, standards, and thresholds of the norm. What is more, States have divergent positions on whether it is a voluntary norm, a rule or a principle of international law imposing certain obligations.

Regardless, to enhance the predictability of behaviour of States and thus increase the normative security and enable the reciprocal protection of the international legal rights of States, States should take a number of mitigating steps.

1. **States should share and discuss the issues arising from the divergent interpretative positions** as to the content, scope, and conditions of the norm C. This will support the need to reduce the divergences in interpretation.

2. To enhance the predictability of international relations in cyberspace, **States that have not yet developed an interpretation of the norm should do so**, paying particular attention to the areas of significant interpretation divergences elaborated in this paper, among other things. The national interpretations of the norm should take into account the state of ICT and the object and purpose of the normative framework established by the GGE.[111] They should focus on the principles and (primary and secondary) rules of international law, serving as a foundation for the norm C.

3. To facilitate transparency and trust, **States should share their interpretations of the norm and the implementation practices with the international community** via confidence-building measures and other processes dedicated to international ICT peace and security.[112]

4. To reduce divergences and thus facilitate compliance with the norm, the **international community should continue to discuss the norm**, focusing on reducing divergences in interpretation of the expectations of State behaviour in cyberspace.

Even if a universal interpretation of the norm remains an aspirational goal and even if the suggestions above are in fact implemented, divergences of interpretation are likely to persist. There is hardly any rule or principle of international law that faces no reservation by States or is not subject to a variety of interpretations. After all, interpretation of normative frameworks "is to some extent an art, not an exact science".[113] Moreover, divergences of interpretation are more likely to arise with the emergence of new norms or with application of existing norms to a new reality.

110 In this instance, countermeasures are a distinct category of the international law of State responsibility. See ILC (2001b, Ch II).
111 UNGA (2021a, para 15).
112 One such example is the Cyber Policy Portal, a confidence-building tool, recognized by the GGE and OEWG in their final consensual reports in 2021. UNGA (2021a, para 86); UNGA (2021c, para 50).
113 ILC (1966, 218).

References

Akande, Dapo Antonio Coco, Talita de Souza Dias, Duncan Hollis, Harold Hongju Koh, James O'Brien and Tsvetelina van Benthem. 2020. 'The Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means'. *European Journal of International Law:Talk!*, 28 October 2020. https://www.ejiltalk.org/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through-digital-means

Alabama case (United States of America v Great Britain) (decision of 14 September 1872). In Moore, John. 1898. *History and Digest of the International Arbitrations to which the United States has been a Party* (vol I, Washington DC, US Government Publishing Office).

Alabama claims of the United States of America against Great Britain. UNRIAA XXIX (8 May 1871) 125. https://legal.un.org/riaa/cases/vol_XXIX/125-134.pdf

Australia. 2019. *Australian Implementation of Norms of Responsible State Behaviour in Cyberspace*. https://www.dfat.gov.au/sites/default/files/how-australia-implements-the-ung-ge-norms.pdf

Axelrod, Robert. 1984. *The Evolution of Cooperation.* New York: Basic Books.

Canada. 2019. *Canada's implementation of the 2015 GGE norms*. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/canada-implementation-2015-gge-norms-nov-16-en.pdf

Chan, Leong, Ian Morgan, Hayden Simon, Fares Alshabanat, Devin Ober, James Gentry, David Min, Renzhi Cao. 2019. *'Survey of AI in Cybersecurity for Information Technology Management'. 2019 IEEE Technology & Engineering Management Conference (TEMSCON)*: 1–8. https://ieeexplore.ieee.org/abstract/document/8813605

Chayes, Abram and Antonia Handler Chayes. 1993. 'On Compliance'. *International Organization* 47(2): 175–205.

Clapham, Andrew. 2010. 'The Role of the Individual in International Law'. *European Journal of International Law* 21(1): 25–30.

Department of Foreign Affairs and Trade. 2017. *Australia's Position on the Application of International Law to State Conduct in Cyberspace*. https://www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf

Egypt. 2020. *Working Paper submitted by the Delegation of Egypt to the Open-Ended Working Group on Developments in The Field of Information and Telecommunications in The Context of International Security*. 30 January 2020. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/Egypt-Working-Paper-OEWG-ICTs1.pdf

Federal Department of Foreign Affairs. 2021. *Switzerland's position paper on the application of international law in cyberspace*. https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf

Finland. 2020. *International law and cyberspace–Finland's national positions*. 15 October 2020. https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859

Finnemore, Martha. 2017. 'Cybersecurity and the Concept of Norms'. *Carnegie Endowment for International Peace*, 30 November 2017. https://carnegieendowment.org/files/Finnemore_web_final.pdf

Foreign and Commonwealth Office. 2019. *Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015*. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf

G7. 2019. *Cyber Norm Initiative Synthesis of Lessons Learned and Best Practices*. https://www.diplomatie.gouv.fr/IMG/pdf/_eng_synthesis_cyber_norm_initiative_cle44136e.pdf

German Federal Foreign Office and German Federal Ministry of Defence, *On the Application of International Law in Cyberspace*. March 2021. https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

Giegerich, Thomas. 2020. 'Retorsion'. *Max Planck Encyclopedias of International Law*, September 2020. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e983

Goldsmith, Jack. 1999. 'Against Cyberanarchy'. *University of Chicago Law Occasional Paper* 40: 1–40.

Guzman, Andrew. 2010. *How International Law Works: A Rational Choice Theory*. Oxford: Oxford University Press, 2010.

Heickerö, Roland. 2010. 'Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations'. *Swedish Defence Research Agency*. 30 March 2010.

IBM Institute for Business Value. 2018. *Wielding a double-edged sword: Preparing cybersecurity now for a quantum world*. https://www.ibm.com/downloads/cas/5VGKQ63M

Inter-American Juridical Committee. 2020. *Improving Transparency: International Law and State Cyber Operations – Fifth Report*. OAS document CJI/doc. 615/20 rev.1 (7 August 2020).

International Court of Justice (ICJ). 1949. *Corfu Channel case*. Merits, ICJ Reports 1949: 4. https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf

–––. 1980. *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)*. Judgment, ICJ Reports 1980: 3. https://www.icj-cij.org/public/files/case-related/64/064-19800524-JUD-01-00-EN.pdf

–––. 1984. *Delimitation of the Maritime Boundary in the Gulf of Maine Area (Canada v United States of America)*. Judgment, ICJ Reports 1984: 288–290, para. 79. https://www.icj-cij.org/public/files/case-related/67/067-19841012-JUD-01-00-EN.pdf

———. 1986. *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)*. Merits, Judgment, ICJ Reports 1986: 14. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

———. 2005. *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)*. Judgment, ICJ Reports 2005: 168. https://www.icj-cij.org/public/files/case-related/116/116-20051219-JUD-01-00-EN.pdf

———. 2007. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*. Judgment, ICJ Reports 2007: 43. https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf

———. 2010. *Pulp Mills on the River Uruguay (Argentina v Uruguay)*. ICJ Reports 2010: 14. https://www.icj-cij.org/public/files/case-related/135/135-20100420-JUD-01-00-EN.pdf

———. 2018. *Immunities and Criminal Proceedings (Equatorial Guinea v France)*. Preliminary Objections, Judgment, ICJ Reports 2018: 292. https://www.icj-cij.org/public/files/case-related/163/163-20180606-JUD-01-00-EN.pdf

International Committee of the Red Cross (ICRC). 2019. 'International Humanitarian Law and Cyber Operations during Armed Conflicts'. https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

International Law Commission (ILC). 1966. *Draft Articles on the Law of Treaties with commentaries*. UN Document A/CN.4/SER. A/1966/Add. 1. II Ybk of the ILC: 187. https://legal.un.org/ilc/texts/instruments/english/commentaries/1_1_1966.pdf

———. 1994. *The law of the non-navigational uses of international watercourses*. UN Document A/CN.4/SER.A/1994/Add.l (Part 2). II(2) Ybk of the ILC: 88. https://legal.un.org/ilc/publications/yearbooks/english/ilc_1994_v2_p2.pdf

———. 1996. *International liability for injurious consequences arising out of acts not prohibited by international law*. UN Document A/CN.4/475 and Add.1 (13 May 1996) II(1) Ybk of the ILC: 29. https://legal.un.org/ilc/publications/yearbooks/english/ilc_1996_v2_p1.pdf

———. 2001a. *Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries*. UN Document A/CN.4/SER.A/2001/Add.1 (Part 2) (2001) II(2) Ybk of the ILC: 146. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_7_2001.pdf

———. 2001b. *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. UN Document A/CN.4/SER.A/2001/Add.1 (Part 2). II(2) Ybk of the ILC. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

International Tribunal for the Law of the Seas (ITLOS). 2011. *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area.* Advisory opinion, ITLOS Reports 2011: 10. https://www.itlos.org/fileadmin/itlos/documents/cases/case_no_17/17_adv_op_010211_en.pdf

International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991. 2009. *Updated Statute of the International Criminal Tribunal for the Former Yugoslavia*. September 2009. https://www.icty.org/x/file/Legal%20Library/Statute/statute_sept09_en.pdf

Island of Palmas case (Netherlands v USA). UNRIAA II (4 April 1928) 829. https://legal.un.org/riaa/cases/vol_II/829-871.pdf

Jacobson, Harold and Edith Brown Weiss. 1995. 'Strengthening Compliance with International Environmental Accords: Preliminary Observations from a Collaborative Project'. *Global Governance* 1(2): 119–148.

Kaspersky, 'What is a DDoS Attack? - DDoS Meaning'. https://www.kaspersky.com/resource-center/threats/ddos-attacks

Kaspersky Global Research & Analysis Team (Kaspersky GRAT). 2013. 'The "Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies'. Kaspersky, 14 January. https://securelist.com/the-red-october-campaign/57647

Keohane, Robert. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.

–––. 1986. 'Reciprocity in International Relations'. *International Organization* 40(1): 1.

L. F. H. Neer and Pauline Neer (U.S.A.) v United Mexican States. UNRIAA IV (15 October 1926): 60.

Lauterpacht, Hersch. 1928. 'Revolutionary Activities by Private Persons Against Foreign States'. *American Journal of International Law* 22(1): 105–130.

Menscher, Damian. 2020. 'Exponential growth in DDoS attack volumes'. Google Cloud. 16 October 2020. https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks

Ministère des Armées, *Droit international appliqué aux operations dans le cyberspace*. 9 September 2019. https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international

Ministry of Foreign Affairs of Japan. 2021. *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*. 28 May 2021. https://www.mofa.go.jp/files/100200935.pdf

Ministry of Foreign Affairs of the Czech Republic. 2020. *Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security*. April 2020. https://front.un-arm.org/wp-content/uploads/2020/04/czech-republic-oewg-pre-draft-suggestions.pdf

New Zealand. 2020. *The Application of International Law to State Activity in Cyberspace*. https://dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace

Nollkaemper, Andre. 2003. 'Concurrence between Individual Responsibility and State Responsibility in International Law'. *International and Comparative Law Quarterly* 52(3): 615–640.

Nuremberg Military Tribunals. 1946. *United States of America vs Karl Brandt, Siegfried Handloser, Paul Rostock et al.* Office of Military Government for Germany (US) Nuremberg 1946. Case No 1, count 2 and 3. https://www.loc.gov/rr/frd/Military_Law/pdf/NT_Indictments.pdf

Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG). 2020. *Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions and comments on the initial pre-draft of the OEWG report (as of 27 May 2020.* https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Non-paper-rules-norms-and-principles-19-01-2021.pdf

Paulus, Andreas. 2012. 'Purposes and Principles, Article 2'. In *The Charter of the United Nations: A Commentary, Volume I*. edited by Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus, Nikolai Wessendorf. 3rd Edition, Oxford: Oxford University Press.

Pronto, Arnold. 2015. 'Understanding the Hard/Soft Distinction in International Law'. *Vanderbilt Journal of Transnational Law* 48: 941–956.

Republic of Korea. 2020a. *Comments on the pre-draft of the OEWG Report*. 14 April 2020. https://front.un-arm.org/wp-content/uploads/2020/04/200414-rok-comment-on-pre-draft-of-oewg.pdf

–––. 2020b. *Implementation of the 2015 UNGGE Norms*. https://front.un-arm.org/wp-content/uploads/2020/03/rok-implementation-of-2015-gge-norms.pdf

Rome Statute of the International Criminal Court (Rome, 17 July 1998) UNTS vol. 2187, No. 38544.

Sancho, David and Rainer Link. 2011. 'Sinkholing Botnets'. *Trend Micro Technical Paper. 31 March 2011*. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp__sinkholing-botnets.pdf?_ga=2.255495307.282598821.1623832502-271237131.1623832499

Schmitt, Michael, ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

–––. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Statement by Ambassador Janne Taalas at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security. 2018. 10 & 11 February. https://ccdcoe.org/uploads/2018/10/Statement-on-International-Law-by-Finnish-Ambassador-Janne-Taalas-at-2nd-session-of-OEWG.pdf

Statute of the International Court of Justice. 1945. San Francisco, 24 October 1945.

The Netherlands. 2019. *Letter to the parliament on the international legal order in cyberspace*. 5 July 2019, Appendix 1. https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace

Trail smelter case (United States v Canada). UNRIAA III (16 April 1938 and 11 March 1941) 1905.

TrendMicro. 2014. 'Utilising Island Hopping in Targeted Attacks'. 25 September 2014. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/utilizing-island-hopping-in-targeted-attacks

United Nations Charter. 1945. San Francisco, 26 June 1945.

United Nations General Assembly (UNGA). 1962. *Permanent sovereignty over natural resources.* UN Document 1803 (XVII) (14 December 1962).

–––. 1970. *Declaration on Principles of International Law Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United Nations*. UN Document A/RES/2625(XXV) (24 October 1970).

–––. 1992. *Rio Declaration on Environment and Development*. UN Document A/CONF.151/26 (Vol. I) (12 August 1992).

–––. 2002. *Responsibility of States for Internationally Wrongful Acts*. UN Document A/RES/56/83 (28 January 2002) Annex.

–––. 2014. *The rule of law at the national and international levels*. UN Document A/RES/69/123 (18 December 2014).

–––. 2015. *Developments in the field of information and telecommunications in the context of international security*. UN Document A/RES/70/237 (30 December 2015).

–––. 2015a. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. UN Document A/70/174 (22 July 2015).

–––. 2019a. *Advancing responsible State behaviour in cyberspace in the context of international security*. UN Document A/RES/74/28 (18 December 2019).

–––. 2019b. *Developments in the field of information and telecommunications in the context of international security*. UN Document A/74/120 (24 June 2019). https://undocs.org/A/74/120

–––. 2020a. *Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation*. UN Document A/74/821 (29 May 2020). https://undocs.org/A/74/821

–––. 2020b. *Second report on general principles of law by Marcelo Vázquez-Bermúdez, Special Rapporteur.* UN Document A/CN.4/741 (9 April 2020).

———. 2021a. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. UN Document A/76/135 (14 July 2021). https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

———. 2021b. *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266.* UN Document A/76/136 (13 July 2021). https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

———. 2021c. *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. UN Document A/75/816 Annex 1 (18 March 2021). https://undocs.org/en/A/75/816

———. 2021d. *Chair's Summary: Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Third substantive session*. UN Document A/AC.290/2021/CRP.3 (10 March 2021). https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

United Nations Institute for Disarmament Research (UNIDIR). 2021. *Due Diligence in Cyberspace: Multi-Stakeholder Dialogue on the Norms of Responsible State Behaviour*. Proceedings (12 May 2021) [on file with the author].

United Nations Secretary-General. 2018. *Securing Our Common Future: An Agenda for Disarmament*. UN Office for Disarmament Affairs, New York. https://www.un.org/disarmament/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf

United Nations Security Council (UNSC). 1994. Resolution 955. UN Document S/RES/955 (8 November 1994).

United States Mission to the United Nations. 2021. *Remarks by Ambassador Linda Thomas-Greenfield at a UN Security Council Open Debate on Cybersecurity*. 29 June 2021. https://usun.usmission.gov/remarks-by-ambassador-linda-thomas-greenfield-at-a-un-security-council-open-debate-on-cybersecurity

Wolfrum, Rüdiger. 2010. General International Law *(Principles, Rules, and Standards)*. The Max Planck Encyclopedia of International Law, December 2010. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1408

Wood, Michael. 2019. 'Customary International Law and the General Principles of Law Recognized by Civilized Nations'. *International Community Law Review* 21: 307–324.

Due diligence in cyberspace

Normative expectations of reciprocal protection of international legal rights

Noting the ability of voluntary norms to strengthen peace, security, and stability in international relations, the United Nations Group of Governmetal Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security proposed a normative framework of mutual international assurance, based on the due diligence principle of international law. This paper provides an exposition of the divergences and convergences in national interpretations of the norm C, as formulated in the 2015 GGE report and later elaborated in the 2021 report, which suggests that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs". As elaborated by this paper, States are yet to reach an agreement on the scope of the norm, knowledge conditions, standards, and thresholds of the norm. What is more, States have divergent positions on whether it is a voluntary norm, a rule or a principle of international law imposing certain obligations.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

@unidirgeneva @UNIDIR un_disarmresearch