UNIVERSIDAD DE MURCIA

http://revistas.um.es/analesderecho

ANALES de DERECHO

THE INTERNATIONAL LAW PRINCIPLE OF DUE DILIGENCE AND ITS APPLICATION TO THE CYBER CONTEXT

JUAN JORGE PIERNAS LÓPEZ

Profesor Titular de Derecho Internacional Público y Relaciones Internacionales de la Universidad de Murcia

El principio de diligencia debida en Derecho internacional y su aplicación al contexto cibernético

Resumen

Este artículo analiza la aplicación del principio de diligencia debida en Derecho internacional al contexto cibernético. Con este objetivo, el artículo describe en primer lugar los principales elementos de este principio en el contexto cibernético actual, marcado por la creciente amenaza que representan los ciberataques. A continuación, el artículo analiza la naturaleza jurídica del principio y su aplicación al ámbito cibernético a la luz de la práctica internacional de Estados y Organizaciones internacionales y concluye con una serie de consideraciones sobre su plena vigencia actual como obligación jurídica y su posible desarrollo futuro.

Palabras clave: *principio de debida diligencia, derecho internacional, práctica internacional, naturaleza jurídica*

"The international law principle of due diligence and its application to the cyber context"

Abstract

This article analyses the application of the principle of due diligence in international law to the cyber context. To this end, the article first describes the main elements of this principle in the current cyber context, which is marked by the growing threat posed by cyber-attacks. The article then analyses the legal nature of the principle and its application to the cyber domain in the light of the international practice of states and international organisations, and concludes with a series of considerations on its current full validity as a legal obligation and its possible future development.

Keywords*: principle of due diligence, international law, international practice, legal nature*

SUMARIO*: I. INTRODUCTION. II. THE CYBER CONTEXT: THE INCREASING THREATS ORIGINATING FROM CYBERSPACE. III. MAIN FEATURES OF THE DUE DILIGENCE PRINCIPLE IN THE CYBER CONTEXT. IV. THE LEGAL NATURE OF THE DUE DILIGENCE PRINCIPLE IN THE CYBER CONTEXT. V. THE POSITION OF THE EUROPEAN UNION AND ITS EVOLUTION. VI. CONCLUSIONS.

I. INTRODUCTION

According to the international law principle of due diligence, a state may incur in responsibility if it does not take all feasible measures, under the circumstances, to prevent conduct on or from its territory or in or from areas under its jurisdiction to the detriment of other States in violation of international law[1].

This principle has its origin in customary international law, it is usually linked to the principle of sovereignty. In this regard, for example, Ireland has linked the principle of due diligence to the principle of sovereignty and ranks it as a primary rule of international law, the breach of which generates international responsibility.[2] The principle was already mentioned by the International Court of Justice (ICJ) in the *Corfu Channel* case[3] as follows: [every State has the] "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States". To this extent, for

* Juan Jorge Piernas López, Profesor Titular de Derecho Internacional Público y Relaciones Internacionales y Titular de la Cátedra Jean Monnet (TEULP) en la Universidad de Murcia. Este trabajo ha sido realizado en el marco del proyecto de investigación titulado "La búsqueda de una regulación internacional para las actividades cibernéticas: ¿una ineludible necesidad? (CYBINREG)", ayudas a proyectos de I+D+i en el marco de los Programas estatales de generación de conocimiento y fortalecimiento científico y tecnológico del sistema de I+D+i orientada a los retos de la Sociedad (convocatoria 2020), Ref PID 2020 112577 RB-I00. El autor es IP2 del proyecto.

[1] GUTIERREZ ESPADA, C., *La Responsabilidad Internacional por el uso de la fuerza en el ciberespacio*, Aranzadi, 2020, in particular Chapter 3, section 3, paragraphs 48-50.

[2] Irish Department of Foreign Affairs, Position Paper on the Application of International Law in Cyberspace (6 July 2023) at p. 3: "Ireland considers the due diligence principle to be a primary rule of international law. Therefore, a breach of this international obligation, which is attributable to a state, engages state responsibility.", available at https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf

[3] Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)

(Judgment on the merits) [1949] ICJ Reports 4, 22.

instance, Switzerland regards the due diligence principle as customary international law and applicable to the cyber context.[4]

The principle of due diligence is also sometimes referred to as the duty or obligation of vigilance. The ICJ concluded in the *Armed Activities on the Territory of the Congo* case that Uganda was responsible "for any lack of vigilance preventing violations of Human Rights and International Humanitarian Law by other actors present in the occupied territory, including rebel groups acting on their own account".[5]

The due diligence principle has been particularly prominent in the environmental field.[6] To this extent, states introduced the main tenets of the due diligence obligation as principle 21 of the 1972 Stockholm declaration,[7] and as principle 2 of the 1992 Río declaration.[8]In this context, the ICJ held in the Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons* that "The existence of the general obligation of States to ensure that activities within their jurisdiction and control respect the environment of

[4] Federal Department of Foreign Affairs, 'Switzerland's position paper on the application of international law in cyberspace' (May 2021), available at file:///C:/Users/Jorge/Downloads/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN-1.pdf, at p. 7 "The principle of due diligence has evolved over a long period of time. Switzerland views due diligence as part of customary international law and applicable to cyberspace."

[5] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, ICJ Reports 2005, p. 168, [179]. See also Irish Department of Foreign Affairs, Position Paper on the Application of International Law in Cyberspace (6 July 2023), at p. 3, available at https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf

[6] See for these references OKWORI, E.O., "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States", in DESTA, Y., HAILU, M. (eds) Ethiopian Yearbook of International Law, vol 2018, Springer, at pp. 205–242, p. 209.

[7] UNGA (1972) Declaration of the United Nations Conference on the Human Environment (16 June 1972). UN Doc A/RES/2994 (Stockholm Declaration), principle 21: States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own resources pursuant to their own environmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other State."

[8] UNGA (1992) Declaration on Environment and Development (12 Aug 1992). UN Doc A/CONF.151/26 (Rio Declaration), principle 2: "States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own resources pursuant to their own environmental and developmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction."

other States or of areas beyond national control is now part of the corpus of international law relating to the environment."[9]

The origins of the principle are even more distant, as revealed for example by references to it in the *Alabama* case of 1872[10]. Even before, the concept of due diligence bears resemblance with Grotius' notions of responsibility based on *patientia* and *receptus*. Indeed, as it has been noted, according to Grotius "Responsibility based on *patientia* would arise if a sovereign knew of a crime to be committed by an individual but failed to prevent it, even if measures of prevention were available. Responsibility based on *receptus* would arise if a sovereign failed to adequately punish the wrongdoer after a wrongful act had been committed"[11].

The duty of due diligence is applicable to cyberspace as international law applies to new technologies absent an explicit exclusion thereof.[12] As summarised by the Government of Norway, "a State may be held responsible under international law if it knows or should have known that cyber operations that target third States are being carried out from or via its territory, and fails to take adequate measures."[13] Other Governments such as Switzerland have expressed a similar view.[14]

---

[9] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996 (I), pp. 241-242, para. 29.

[10] Alabama claims of the United States of America against Great Britain (1872) 24 RIAA 125, 129-131, specifically at p. 129: "And whereas the "due diligence" referred to in the first and third of the said rules ought to be exercised by neutral governments in exact proportion to the risks to which either of the belligerents may be exposed, from a failure to fulfil the obligations of neutrality on their part".

[11] MONNHEIMER, M., *Due Diligence Obligations in International Human Rights Law*, Cambridge University Press, 2021, p. 80. For the original references see GROTIUS, H., De Jure Belli Ac Pacis 1646, translated by F. W. Kelsey (New York: William Hein & Co, 1995), vol. II, chapter XVII, § XX, 523, and Grotius, De Jure Belli Ac Pacis 1646, vol. II, chapter XXI, § III, 526.

[12] SCHMITT, M.N. (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rule 6, p. 30. The experts refer in this regard to the Nuclear Weapons advisory opinion of the International Court of Justice in, para. 39.

[13] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States' UNODA, A/76/136 (August 2021), at p. 71, available at https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

[14] Federal Department of Foreign Affairs, 'Switzerland's position paper on the application of international law in cyberspace' (May 2021), at p. 7 "The principle of due diligence is also applicable to cyberspace. Consequently, 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 minimise the risks of such incidents."

This article analyses the application of the principle of due diligence in international law to the cyber context. To this end, the article first describes the current cyber context, which is marked by the growing threat posed by cyber-attacks. The article then analyses the legal nature of the principle and its application to the cyber domain in the light of the international practice of states and international organisations and concludes with a series of considerations on its current full validity as a legal obligation and its possible future development.

II. THE CYBER CONTEXT: THE INCREASING THREATS ORIGINATING FROM CYBERSPACE

The European Union has since November 2018 considered cyberspace as the fifth area of action, along with the classic spaces of land, sea, air and outer space.[15] This equating of cyberspace with other physical spaces is not new, as other official texts such as the Dutch Cyber Defence Strategy of 2012 (revised in 2015 and 2018), or the National Security Strategy (2010 and 2015) of the United Kingdom already did so.[16]

Cyber-attacks have become one of the main threats to global security, as accredited by numerous international reports and warned by European and national institutions. In this regard, for example, a World Economic Forum report was presented at the Davos meeting at the beginning of 2023, which states that more than 93% of cybersecurity experts and 86% of business leaders believe that "a major catastrophic cyber event is likely to occur in the next two years".[17]

The situation is likely to be exacerbated by the increasing connection of devices to the internet through the Internet of Things (IoT), with more than 41 billion IoT devices expected to be connected by 2025.[18] Moreover, the situation in the European Union is particularly challenging, given that it is a net importer of cybersecurity products and

[15] EU Cyber Defence Policy Framework (2018 update), Brussels, 19 November 2018, 14413/18, p. 1.

[16] GUTIERREZ ESPADA, C., *La Responsabilidad Internacional por el uso de la fuerza en el ciberespacio*, Aranzadi 2020, in particular Chapter 1, section I, paragraph 1

[17] See the news item on the publication of the report, available at https://www.weforum.org/press/2023/01/geopolitical-instability-raises-threat-of-catastrophic-cyberattack-in-next-two-years/ (author's translation).

[18] See in this respect the information published by the European Commission, available at the following link: https://digital-strategy.ec.europa.eu/es/policies/internet-things-policy

services, and relies heavily on non-European suppliers,[19] which increases the risk of technological dependency and vulnerability.

Cyberattacks have increased significantly during the COVID-19 pandemic, having recently been directed against critical infrastructures, health centres, or energy facilities, such as the large-scale cyberattacks in Belgium that affected the Belnet telecommunications company and the Department of Home Affairs responsible for immigration policy and public order in 2021, or the cyberattack against Ukraine that preceded the Russian aggression of February 2022.[20]

In this context, as GUTIÉRREZ ESPADA has recently pointed out, Spain is the third country in the world to suffer the most cyberattacks, and cyberattacks against critical sectors in Europe doubled in 2021.[21] It is also worth recalling in this context the words of former European Commission President Juncker in his 2017 State of the Union address: "Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks "[22] .

Cyber-attacks are also targeting European institutions, and in response to this growing phenomenon, the Commission presented in March 2022 a proposal for a Regulation of the European Parliament and of the Council establishing measures to ensure a high common level of cybersecurity within the institutions, bodies, offices and agencies of the Union, based on Article 298 TFEU on an "open, effective and independent" European administration. The Regulation provides, among other measures, for the creation of an Interinstitutional Cybersecurity Board. The Council and the European

[19] See on this point the Proposal for a Regulation of the European Parliament and of the Council establishing the European Centre of Industrial, Technological and Research Competence in Cybersecurity and the Network of National Coordination Centres, Brussels, 12.9.2018 COM(2018) 630 final 2018/0328 (COD), p. 1.

[20] See on these cyber-attacks, among others, MIADZVETSKAYA, Y. and WESSEL, R.A., "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox", European Papers, Vol. 7, 2021, No 1, pp. 413-438, p. 413.

[21] GUTIÉRREZ ESPADA, C., "La creciente necesidad de legislación contra las amenazas cyberneticas, fuentes de graves daños transnacionales", Cuadernos de Derecho Transnacional (October 2022), Vol. 14, No. 2, pp. 10-46, at pp. 11 and 15. See also for a recent account of the cybersecurity context SEGURA SERRANO, A. *El desafío de la ciberseguridad global*, Aranzadi, Cizur menor, 2023.

[22] State of the Union Address 2017, available at the following link: https://ec.europa.eu/commission/presscorner/detail/es/SPEECH_17_3165

Parliament reached a provisional agreement on this proposal on 26 June 2023 and the European Parliament adopted it at first reading on 21 November 2023. The regulation will therefore enter into force shortly.

On the other hand, the involvement of state actors, such as Russia, China and North Korea, in malicious cyber activities significantly increases the gravity of the situation. In this regard, the Council of the European Union has expressed concern about the growing ability of state and non-state actors to carry out malicious cyber activities[23]. For example, the *WannaCry* cyber-attack launched in May 2017 and attributed by the United States and the United Kingdom to North Korea[24], affected more than 300,000 computers in 150 countries, causing damage estimated at hundreds of millions of euros. Furthermore, a report by the Panel of Experts established pursuant to UN Security Council Resolution 1874 (2009), concerning the nuclear test conducted by the Democratic People's Republic of Korea on 25 May 2009, has concluded that North Korean government entities systematically conduct large-scale cyberattacks to finance North Korea, having already raised up to $2 billion[25].

III. MAIN FEATURES OF THE DUE DILIGENCE PRINCIPLE IN THE CYBER CONTEXT

The principle of due diligence can be anchored in Article 2 of the Draft articles on Responsibility of States for Internationally Wrongful Acts which clarifies that State conduct may take the form of "action or omission",[26] the principle of due diligence falling

[23] Council Conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ("cyber diplomacy toolkit"), 7 June 2017, CYBER 91 RELEX 482 POLMIL 58 CFSP/CFSP 476, p. 3.

[24] See in this regard the news published in December 2017 by the BBC: https://www.bbc.com/news/world-us-canada-42407488

[25] Report of the Panel of Experts established pursuant to Security Council resolution 1874 (2009), S/2019/691, 30 August 2019.

[26] International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2001. Text adopted by the International Law Commission at its fifty-third session, in 2001, and submitted to the General Assembly as a part of the Commission's report covering the work of that session (A/56/10), Article 2, p. 34: "Elements of an internationally wrongful act of a State: There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State."

in the latter category.[27]It has also been argued that the due diligence principle could be breached by action if a state adopts some ineffective measures to prevent harm where other, more effective, measures were available.[28]

The Czech Republic has also referred in this regard to Article 12 of the ILC's 2001 Draft articles on Responsibility of States for Internationally Wrongful Acts, which clarifies when an international obligation (in our case the principle of due diligence) is breached: "There is a breach of an international obligation by a State when an act of that State is not in conformity with what is required of it by that obligation, regardless of its origin or character."[29]

The due diligence principle applies primarily to the territory of a State but also extraterritorially, provided that such territory is under the control of the government (e.g., platform overseas). The experts of the Tallin Manual 2.0. also clarified that "transit States", that is, a State through which data transits (e.g. fibre cable) bear the due diligence obligation "when it (1) possesses knowledge (on actual and constructive knowledge, see below) of an offending operation that reaches the requisite threshold of harm and (2) can take feasible measures to effectively terminate it."[30] Some states, such as Costa Rica, Romania and Italy, have also accepted the responsibility of the "transit state".[31]

---

[27] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States' UNODA, A/76/136 (August 2021), at p. 71, available at https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

[28] OKWORI, E.O., "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States", in DESTA, Y., HAILU, M. (eds) Ethiopian Yearbook of International Law, vol 2018, Springer, at pp. 205–242, p. 211.

[29] International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2001. Text adopted by the International Law Commission at its fifty-third session, in 2001, and submitted to the General Assembly as a part of the Commission's report

covering the work of that session (A/56/10), at p. 54.

[30] Id., p. 33.

[31] Ministry of Foreign Affairs of Costa Rica, "Costa Rica's Position on the Application of International Law in Cyberspace" (21 July 2023), available at https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf, at p. 8-9 "Under customary international law, States have a general obligation 'not to allow knowingly its territory to be used for acts contrary to the rights of other States'. This duty is a corollary of State sovereignty and requires States to protect the rights of other States in their territory. It may be breached when a State knows or should have known that an act contrary to the rights of another State originates or transits through its territory, and yet fails to take reasonable action to stop or prevent it, and the harm materializes. This means that States must strive to

Rule 6 of the Tallinn Manual 2.0 stipulates that states should not, based on the principle of due diligence, allow their territory or infrastructure to be used for cyber operations that produce "*serious adverse consequences*". The Tallinn Manual does not specify how serious these consequences should be for other states and admits that this is a question not yet resolved by international law[32]. In our opinion, the "significant effect" that the 2019 EU Decision and Regulation require for the adoption of sanctions is likely to meet the standard required by this principle, given the characteristics required for its accreditation (the scope, scale, impact, or seriousness of the disruption caused, the number of natural or legal persons, entities or bodies affected, etc.).

The violation of the due diligence principle must affect the rights of other States (or international organizations) and entail "serious consequences", which do not require damage to objects or injuries to individuals and could involve "for instance, interference with the operation of critical infrastructure or a major impact on the economy".[33]

Rule 7 of the Tallin Manual 2.0 states that "The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other

prevent State or non-State actors, including cybercriminals, from conducting cyber operations against the rights of other States." Costa Rica refers in this regard to Article 14(3) of the 2001 ILC's Draft Articles of State Responsibility. Regarding Italy see Italian position paper on "International law and cyberspace", Italian Ministry for Foreign Affairs and International Cooperation, available at https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf, at p. 7: "Due diligence is an obligation of conduct, not one of result. Accordingly, as long as it makes its best efforts, a State cannot be held liable if ultimately unable to prevent, mitigate, or terminate wrongful cyber activities launched from or in transit through its territory."; see also, for Romania: Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, at p. 76.

[32] SCHMITT, M.N. (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rule 6.25, pp. 36-37: "The precise threshold of harm at which the due diligence principle applies is unsettled in international law. All of the Experts agreed that the due diligence requirement arises when the situation involves a cyber operation that results in 'serious adverse consequences', although they could identify no bright line threshold for the identification of such consequences. They adopted this standard by analogy from application of the due diligence principle in the context of international environmental law. Some of them supported a lower threshold of application for the Rule, for instance, by proposing the term 'significant' or 'substantial' in lieu of 'serious'".

[33] Id., p. 38.

States."[34] As the Government of Canada has recently argued, "The precise threshold that triggers this expectation will depend on the totality of the circumstances in that situation. This would include whether the State has knowledge of the wrongful acts, its technical and other capacities to detect and stop these acts, and what is reasonable in that case. For example, a State with limited technical capabilities would not likely be expected to respond if it failed to detect a malicious cyber activity emanating from or through cyber infrastructure on its territory. However, once aware, the State would be expected to respond."[35]

Similarly, the Government of Norway has held that "if a State possesses knowledge of a cyber operation being carried out from or via its territory causing serious adverse consequences with respect to a right of the target State under international law, it is required to take adequate measures to address the situation."[36]

Indeed, the malicious cyber operations might be carried out by state or non-state actors, or even by a third state,[37] from the territory of the state that bears responsibility under the due diligence principle. In this regard, Switzerland has recently stated that the due diligence principle may indeed act as a palliative in cases where attribution for a cyber-attack may not be clearly established to a state in application of the international norms of attribution, a view shared by Japan.[38] Switzerland has also added that

[34] SCHMITT, M.N. (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rule 7, p. 43.

[35] Government of Canada, International Law applicable in cyberspace (April 2022) para. 27, available at https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a5

[36] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States' UNODA, A/76/136 (August 2021), at p. 71, available at https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

[37] Government of Denmark, "Denmark's Position Paper on the Application of International Law in Cyberspace"(4 July 2023), available at https://brill.com/view/journals/nord/92/3/article-p446_007.xml?ebody=pdf-89805 at p. 7: "Denmark is of the view that a State may bear international responsibility where a State fails to take adequate measures against a non-State actor - or third State - that conducts harmful cyber operations against another State from its territory or other cyber infrastructure under its effective control."

[38] Ministry of Foreign Affairs of Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (28 May 2021), available at https://www.mofa.go.jp/files/100200935.pdf at p. 5 "One characteristic of cyber operations is the difficulty of making judgment as to attribution to a State. In this respect, the due diligence obligation may

countermeasures may be adopted against the state that breaches its due diligence obligation, irrespective of whether the malicious cyber operation at stake was conducted by state or non-state actors.[39]The Government of Denmark has also recently expressed a similar position.[40]

Notwithstanding, the precise content of the due diligence principle is not clear, although it requires states to take reasonable and appropriate steps, under the circumstances, to end cyber malicious activities of which they are aware, or "should have" been aware, although not all states agree as to the latter, so-called, constructive knowledge.[41] To this extent, in the *Corfú Channel* case the ICJ found that it is not enough for a state to simply state that it ignored that certain conducts were taken place, and added that the state at issue may be required to give explanations as to the information that was available to it and of the use it made of this information.[42]To this extent, it has been

provide grounds for invoking the responsibility of the State from the territory of which a cyber operation not attributable to any State originated. It is possible at least to invoke the responsibility of such a State for a breach of its due diligence obligation, even if it is difficult to prove the attribution of a cyber operation to any State."

[39] Federal Department of Foreign Affairs, 'Switzerland's position paper on the application of international law in cyberspace' (May 2021), at p. 7 "Due diligence applies in particular to actions by private individuals that violate the rights of other states (e.g. hackers) and cannot be (clearly) attributed to the state in accordance with the rules of attribution […]. If the aforementioned conditions exist and the state in question fails to fulfil due diligence requirements, the injured state may take countermeasures in accordance with the rules governing state responsibility in order to induce the responsible state to meet its obligations. Possible countermeasures outlined above may be taken both outside and inside the cyber domain. The responsible state may also be required to make reparations."

[40] See for Denmark Government of Denmark, "Denmark's Position Paper on the Application of International Law in Cyberspace"(4 July 2023), available at https://brill.com/view/journals/nord/92/3/article-p446_007.xml?ebody=pdf-89805 at p. 7: "The lack of compliance with a State's due diligence obligations may lead another State to take countermeasures […]"

[41] See in favour, *e.g*., the position of Ireland: "Ireland considers that constructive knowledge, often described as a situation where a state "ought to have been aware", is capable of satisfying the knowledge component of the obligation of due diligence where this can be ascertained to an appropriate level." Irish Department of Foreign Affairs, Position Paper on the Application of International Law in Cyberspace (6 July 2023), at p. 3, available at https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf For the opposite view see, e.g., New Zealand Foreign Affairs and Trade, 'The Application of International Law to State Activity in Cyberspace', available at https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf , at point 17: "If a legally binding due diligence obligation were to apply to cyber activities, 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."

[42] Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)

suggested that a state whose cyber facilities, owned and controlled, have been breached repeatedly to carry out malicious cyber activities that harm other states, "should have known" that a similar attack will probably take place again.[43]

In any event, the principle of due diligence imposes on states an obligation of means ("must try") and not of result, as the International Court of Justice clarified in the *Genocide Convention Implementation* case:

"Secondly, it is clear that the obligation in question is one of conduct and not one of result, in the sense that a State cannot be under an obligation to succeed, whatever the circumstances, in preventing the commission of genocide: the obligation of States parties is rather to employ all means reasonably available to them, so as to prevent genocide so far as possible. A State does not incur responsibility simply because the desired result is not achieved; responsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide. In this area the notion of "due diligence", which calls for an assessment in concreto, is of critical importance".[44]

IV. THE LEGAL NATURE OF THE DUE DILIGENCE PRINCIPLE IN THE CYBER CONTEXT

The Tallinn Manual 2.0 is unambiguous as to the mandatory character of the due diligence principle: "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"[45].

(Substantive Judgment) [1949] ICJ Reports 4, 18: "It is also true that that State cannot evade such a request by limiting itself to a reply that it is ignorant of the circumstances of the act and of its authors. The State may, up to a certain point, be bound to supply particulars of the use made by it of the means of information and inquiry a t its disposal."

[43] OKWORI, E.O., "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States", cit., p. 215.

[44] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BOSNIA AND HERZEGOVINA v. SERBIA AND MONTENEGRO), Judgment of 26 February 2007, page 221, para. 430.

[45] SCHMITT, M.N. (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rule 6, p. 30.

Not all states, even within the European Union, have traditionally accepted the principle of due diligence as a rule of international law. Indeed, divergences among states, including some very relevant to cyberspace issues, might explain why the legal principle was seemingly diluted in the 2015 report of the UN Group of Governmental Experts on Advances in Information and Telecommunications in the Context of International Security into a political recommendation[46]. According to this report, states 'should not' allow their territory to be used by non-state actors for such purposes[47]. The G7 Lucca Declaration re-emphasised the validity of the due diligence obligation in the same terms[48], as did Resolution 73/266 of 22 December 2018 (adopted with 138 States voting in favour).

In this regard, the experts of the Tallin Manual acknowledged "a view, which no member held, that a general due diligence principle, and therefore its application in the context of cyber operations, has not achieved *lex lata* status. Advocates of this position point to the United Nations Groups of Governmental Experts' (UN GGE) exhortation that States 'should' engage in due diligence, as distinct from a statement that they 'must' engage as a matter of law."[49]

It is nevertheless advisable to be cautious about the value of the opinion of the Tallinn Manual which is not an official document but the opinion of independent experts acting solely in their personal capacity. In this respect, the Tallinn Manual does not codify international custom nor can it represent the *opinio iuris of* the States of nationality of the participating experts but constitutes an expression of the doctrine of the most competent publicists of the various nations, as an auxiliary means for the determination of the rules

[46] See also on this point the discussion in the Tallinn Manual 2.0. SCHMITT, M.N. (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rule 6.3, p. 30.

[47] See 2015 Expert Group Report (UN A/70/174), paragraph 13(c): "States should not knowingly allow their territory to be used for the commission of internationally wrongful acts through the use of ICTs.

[48] G7 Declaration on responsible states behavior in cyberspace Lucca, 11 April 2017, paragraph 4: "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs".

[49] SCHMITT, M.N. (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rule 6.3, p. 30

of law, in accordance with Article 38(d) of the Statute of the International Court of Justice[50].

On the other hand, the fact that the experts participating in the Tallinn Manual are mostly from states with a similar vision of international law, such as the United Kingdom, the United States or Australia, has facilitated progress in the drafting of the Manual, which is very detailed. This contrasts with the difficulties of the much more diverse United Nations Group of Experts in specifying general principles applicable to cyberspace and, in short, in reaching even a minimum consensus text in its last report. The Tallinn Manual 2.0 may, in this context, prove useful in pointing the way towards which the international community could be heading in the future[51].

In this context, as underlined by a study published by the Ministry of Defence of the Republic of Austria in 2018, funded by the EU and prefaced by the then High Representative '*Several major cyber powers, including Russia, China, the United States and the United Kingdom, appear hesitant to accept or even reject the legally binding nature of the due diligence obligation. However, numerous others, including France, Germany, Finland, the Netherlands and Spain, recognise due diligence as an international law* rule"[52].

This statement can be complemented, and to some extent nuanced, with the positions adopted by states in most recent years. For instance, the position of China, according to a 2021 official statement, seems to confer to the due diligence principle a mandatory character: “No State shall knowingly allow its territory, or territory or ICT

[50] BOOTHBY, WH, "Cyber Capabilities", in BOOTHBY, WH (ed.), *New Technologies and the Law in War and Peace*, Cambridge University Press, 2018, p. 89.

[51] Id., p. 133: "The UN GGE process can demonstrate that it is only by including experts from a representative selection of States that an inevitably less detailed, more generalised set of provisions can be achieved. It will then be those that consider that extant law goes further than the GGE experts have acknowledged that will be dissatisfied. Curiously, therefore, neither process generates unanimity of view in the short term. Arguably, it is the kind of process associated with the Tallinn Manuals that will set a more prescriptive legal agenda for the global community to, perhaps gradually, move towards.

[52] REHRL, J., *Handbook on Cybersecurity The Common Security and Defence Policy of the European Union*, Publication of the Federal Ministry of Defence of the Republic of Austria, 2018, p. 31.

facilities, data and information under the control of its government, to be used for ICT activities that undermine national security or interests of other States."[53]

By contrast, Israel features among the States that now oppose the mandatory character of the due diligence principle. In the words of Roy SCHÖNDORF, Israeli Deputy Attorney General (International Law), on December 8, 2020, "we have not seen widespread State practice beyond this type of voluntary cooperation [such as CERT], and certainly not practice grounded in some overarching *opinio juris*, which would be indispensable for a customary rule of due diligence, or something similar to that, to form."[54]

Similarly, New Zealand considers that a due diligence obligation is not settled in international law, and particularly in respect of cyber operations: "An agreed norm of responsible state behaviour provides that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. Whether 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 crystallised in international law."[55]

The United Kingdom has referred to the non-binding nature of the due diligence principle as mentioned in the UN reports to negate the emergence of a customary international law rule of due diligence: "the fact that States have referred to this as a non-

[53]China's Views on the Application of the Principle of Sovereignty in Cyberspace, Ministry of Foreign Affairs of the People's Republic of China, at pp. 2-3, available at https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf

[54] SCHONDORF, R., "Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations (Transcript of the keynote speech delivered at the Stockton Center for International Law", U.S. Naval War College's event on "Disruptive Technologies and International Law."), available at https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/

[55] New Zealand Foreign Affairs and Trade, 'The Application of International Law to State Activity in Cyberspace', at points 16 and 17. This Government has also added that "It is clear that states are not obliged to monitor all cyber activities on their territories or to prevent all malicious use of cyber infrastructure within their borders. If a legally binding due diligence obligation were to apply to cyber activities, 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." The position of New Zealand is available at https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

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".[56]

Interestingly, Canada has recently stated that the conclusions of the 2015 UN expert report do not obstruct the recognition of a mandatory due diligence rule, although this State has not done so and continue studying the issue: "Canada does not consider that the UN GGE consensus in 2015, and subsequently, on voluntary, non-binding norms touching on this matter precludes the recognition of a binding legal rule of due diligence under customary international law. Canada continues to study this matter."[57]

By contrast, a larger number of States support the binding character of the due diligence principle. In the case of France, the national cyber defence strategy is clear about the existence of the international principle, its customary nature and its content:

> "In accordance with the principle of the obligation of reasonable diligence, which is a principle of international humanitarian law, every State has the obligation not to allow its territory to be used for the purpose of acts contrary to the rights of other States. A State which would not have fulfilled this obligation (of means) could thus, in certain cases, incur its responsibility and be the object of counter-measures by the victim State, even if it is not the commander"[58] .

In another official document, France has also recently stated that: *"France exercises its sovereignty over the information systems located on its territory. In compliance with the due diligence requirement, it ensures that its territory is not used for internationally wrongful acts using ICTs. This is a customary obligation for States, which must (i) use cyberspace in compliance with international law, and in particular not use*

[56] United Kingdom Foreign, Commonwealth & Development Office, 'Application of international law to states' conduct in cyberspace: UK statement, policy paper, 2021, at point 12, available at https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement

[57] Government of Canada, International Law applicable in cyberspace (April 2022), para. 26 (footnote 20), available at https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a5

[58] GAUTIER, L. (Preface), *Stratégie nationale de la cyberdéfense*, Economica, Paris, 2018, p. 102.

proxies to commit acts which, using ICTs, infringe the rights of other States, and (ii) ensure that their territory is not used for such purposes, including by non-state actors."[59]

Similarly, the Czech Republic have supported the view that the above-referred 2015 UN expert report conclusions "reflect a general principle of international law obliging States to ensure that territory and objects over which they enjoy sovereignty are not used to harm other States' rights".[60]

In the same vein, Germany has also supported the mandatory nature of the due diligence principle in the following terms: "As a corollary to the rights conferred on States by the rule of territorial sovereignty, States are under an 'obligation not to allow knowingly their territory to be used for acts contrary to the rights of other States' – this generally applies to such use by State and non-State actors. The 'due diligence principle', which is widely recognized in international law, is applicable to the cyber context as well and gains particular relevance here because of the vast interconnectedness of cyber systems and infrastructures."[61]

Particularly clear are the positions of Japan and the Netherlands, which refer to the principle of due diligence as an international obligation.[62] The Dutch position, after recognising that not all states regard the due diligence principle as "an obligation in its own right under international law [affirms that] The Netherlands, however, does regard

[59] INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE, Paper shared by France with the Open-ended working group established by resolution 75/240, 2021, at p. 2, available at https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf

[60] 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, 2020, at p. 3, available at https://front.un-arm.org/wp-content/uploads/2020/04/czech-republic-oewg-pre-draft-suggestions.pdf

[61] Federal Government of Germany, 'On the Application of International Law in Cyberspace', Position Paper (March 2021), at p. 3, available at https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

[62] Ministry of Foreign Affairs of Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (28 May 2021) at p. 5: "States have a due diligence obligation regarding cyber operations under international law." This State refers not only to the ICJ Corfú Channel case but also to the Alabama arbitral decision.

the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act."[63]

Lastly, the Government of Sweden has depicted the due diligence principle as an obligation, with reference to the abovementioned Corfú Channel case, for states to not knowingly allow their territory to be used for acts contrary to the rights of other States.[64]

In our view, in line with the majority opinion, the obligation of due diligence is a "settled rule of international law"[65] and, like other international norms, applicable (in the absence of specific rules eliminating it) to activities in and from cyberspace. The text agreed in the abovementioned fora (that States "should not"...) contrasts with that included in Resolution 73/27 of 5 December 2018, entailing a clear obligation, which may explain why this second resolution was adopted with *only* 119 States voting in favour, and 46 States voting against, including EU Member States, the UK and the US[66].

[63] Dutch Ministry of Foreign Affairs, 'Letter to the parliament on the international legal order in cyberspace' (5 July 2019), Appendix "International law in cyberspace", at p. 4, available at 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

[64] Government office of Sweden, Position Paper on the Application of International Law in

Cyberspace, 2022, available at https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf, at p. 4: "As a corollary to their sovereignty, States have an obligation to not knowingly allow their territory to be used for acts contrary to the rights of other States."

[65] CERVELL HORTAL, M.J., *La legítima defensa en el derecho internacional contemporáneo: (nuevos tiempos, nuevos actores, nuevos retos)*, Tirant lo Blanch, Valencia, 2017, p. 128. See also in this regard Government office of Sweden, Position Paper on the Application of International Law in

Cyberspace, 2022, available at https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf, at p. 4: "As a corollary to their sovereignty, States have an obligation to not knowingly allow their territory to be used for acts contrary to the rights of other States. This well-established rule of international law, described by the ICJ in the Corfu Channel case, also applies to cyber operations. A State's obligation to ensure that its territory is not used to harm other States has often been referred to as an obligation of due diligence."

[66] A/RES/73/27, Advances in the Field of Information and Telecommunications in the Context of International Security, paragraph 1.3: "States should not knowingly allow their territory to be used to commit internationally wrongful acts using ICTs. States should not rely on third parties to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-state actors to commit such acts". The 46 votes against were from the following countries: Albania, Andorra, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Marshall Islands, Monaco, Montenegro, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain,

Indeed, as underlined by the experts of the Tallin Manual 2.0 “the GGEs' comments do not definitively refute the existence of such a principle. Indeed, the due diligence principle derives from the principle of sovereignty (Rule 1), and the UN GGEs have themselves acknowledged that principles of international law that 'flow' from that of sovereignty are binding in the cyber context.”[67]

V. THE POSITION OF THE EUROPEAN UNION AND ITS EVOLUTION

On 11 February 2015 the Council of the European Union adopted its *conclusions on cyber diplomacy*[68], as a response to the increase in the number of cyber-attacks and the deadlock in international negotiations on international law and state responsible behaviour in cyberspace.[69] The conclusions on cyber diplomacy were updated in 2017 with the so-called Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").[70]

The Framework was developed in October 2017 through the adoption of the Toolkit’s implementing guidelines.[71]The 2017 Cyber Toolkit implementing Guidelines provided, in particular, that in the event that a State knowingly allows its territory to be used for malicious cyber activities, including internationally wrongful acts using ICTs, against a Member State or against the EU, the Framework's measures could be triggered to induce that State to ensure that its territory is not used for such activity[72]. The 2017 guidelines added that, in accordance with voluntary standards, states should not

Sweden, The former Yugoslav Republic of Macedonia, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America.

[67] SCHMITT, M.N. (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rule 6.3, p. 30.

[68] Council Conclusions on Cyber Diplomacy, CYBER 5 RELEX 114 JAIEX 6 TELECOM 32 COPS 42, Brussels, 11 February 2015.

[69] See to this extent Y. MIADZVETSKAYA, AND R.A. WESSEL, “The Externalisation of the EU’s Cybersecurity Regime: The Cyber Diplomacy Toolbox”, European Papers, 2022, forthcoming, at page 15.

[70] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 7 June 2017, CYBER 91 RELEX 482 POLMIL 58 CFSP/CFSP 476.

[71] Ibid.

[72] *Ibid.*

knowingly allow their territory to be used for internationally wrongful acts, and should respond to appropriate requests for assistance from another state.

The 2017 guidelines did not explicitly mention the existence of a "due diligence" obligation or principle under international law, and emphasized the non-binding character of the UN norms in this respect. The guidelines appeared to refer to the abovementioned 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which recommended that States should deliberately not allow the use of their territory and "advocated" that States should assist each other[73]. Similarly, the 2019 Council decision setting up the EU sanctions regime in response to cyberattacks noted that "States […] should seek to ensure that their territory is not used by non-State actors to commit such acts" with reference to the 2015 UN Report.[74]

However, and remarkably in this context, the 2023 Revised Implementing Guidelines of the Cyber Diplomacy Toolbox, still non-adopted, provide that States have "a due diligence obligation under international law to not knowingly allow their territory to be used for acts contrary to the rights of other States and may also call on other States to cooperate in managing cyber incidents, in accordance with the UN framework for responsible state behaviour in cyberspace".[75]

The revised guidelines clearly distinguish the previous statement from the non-binding norms cited in the 2017 guidelines by holding that "In addition, agreed norms of responsible State behaviour affirm, inter alia, that states should not knowingly allow their

[73] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, p. 2: "[...] The Group recommended that States should work together to prevent harmful practices in the field of ICTs and that they should not knowingly allow their territory to be used for the commission of internationally wrongful acts using ICTs. It also called for increased information sharing and assistance in prosecuting the use of ICTs for terrorist and criminal purposes, stressing that states should ensure full respect for human rights, including the right to privacy and freedom of expression.

[74] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I , 17.5.2019, p. 13–19, preamble at 4.

[75] Revised Implementing Guidelines of the Cyber Diplomacy Toolbox, Brussels, 8 June 2023 (OR. en) 10289/23, at point 12.

territory to be used for internationally wrongful acts using ICTs, and should respond to appropriate requests for assistance by another State."[76]

In any event, as it has been held "in debates about diligent state behavior in cyberspace, doubts about a general principle or a cyber-specific protective obligation should not be presented as an alternative to a legal vacuum. For international law already provides more than meets the eye: a patchwork of protective duties that, together, require states to do their best to prevent, halt and respond to a wide range of online harms."[77]

Moreover, the revised guidelines make clear that requesting a State to prevent or address a cyber-incident does not, of itself, constitute the imputation of international responsibility: "The EU and its Member States can request States to take appropriate measures to prevent or address cyber incidents that originate from their territory, bearing in mind that the indication that a cyber-attack emanates from the territory or the infrastructure of a State does not, of itself, imply responsibility of that State for the incident, or that notifying a State that its territory is being used for a wrongful act does not, of itself, imply that it is responsible for the act itself."[78]

In the case of a violation of the principle of due diligence, the imputation of the cyber-attack to a state or non-state actor is irrelevant since, as has been stated since the 1930s, this principle can be violated by acts committed by non-state actors (economic criminals, terrorists...). This was already noted in the *Trail smelter* case.[79]

[76] Ibid.

[77] COCO, A. & DIAS, T. "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law, European Journal of International Law, Volume 32, Issue 3, August 2021, Pages 771–806, at p. 806.

[78] Ibid.

[79] See in particular *Trail smelter case* (United States, Canada), 16 April 1938 and 11 March 1941, Reports of International Arbitral awards, pp. 1905-1982, at p. 1963: "A State owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction. A great number of such general pronouncements by leading authorities concerning the duty of a State to respect other States and their territory have been presented to the Tribunal. These and many others have been carefully examined. International decisions, in various matters, from the Alabama case onward, and also earlier ones, are based on the same general principle, and, indeed, this principle, as such, has not been questioned by Canada"

It is therefore the conduct of the state from whose jurisdiction a cyber-attack has been launched, in particular to prevent or stop it, that must be analysed[80], without it being necessary to prove the existence of an internationally wrongful act or to identify the state responsible for it. Indeed, as it has been observed "Instead of putting the emphasis on the legal qualification of a malicious activity, this concept [due diligence] makes it possible to focus on what could have been done by a state, and on what the state did not do in order to prevent transboundary cyber-harm"[81].

Notwithstanding, tracing a cyber-attack to a certain territory might be very difficult in some instances. In addition, the knowledge that can be imputed to States will depend on the State's cyber capabilities (since, as stated above, not all States, even in the European Union, have the same capacity to protect against cyber-attacks), and on the sophistication of the cyber-attack in question (which may be very difficult to detect, prevent or nullify). In this regard, as summarised by the position of Switzerland "Due diligence is a variable standard and depends on the capacities and capabilities of a state as well as the particular circumstances of each case. Territorial states are obliged to use all reasonable means to prevent serious harm being caused to another state by activities taking place within their territory or in an area under their effective control. This makes due diligence an obligation of conduct, not of result. If the aforementioned conditions exist, the state in question is obliged under international law to close any loopholes immediately and assist in intercepting and tracing the incident."[82]

In addition, some states, even among those that support the mandatory character of the due diligence obligation, have clearly stated that a general obligation to prevent cyber attacks does not exist under international law, and therefore that "States are consequently not under an obligation to monitor all cyber activities on their territories."[83]

[80] SCHMITT, M.N. (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rule 7, p. 43: "The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States".

[81] PAWLAK, P. and BIERSTEKER, T. (eds.), *Guardian of the Galaxy, EU cyber sanctions and norms in cyberspace*, Chaillot Paper 155, European Union Institute for Security Studies, 2019, p. 66.

[82] Federal Department of Foreign Affairs, 'Switzerland's position paper on the application of international law in cyberspace' (May 2021), at p. 7.

[83] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States' UNODA, A/76/136

In any event, it must at least be established that the cyber-attack was launched from a certain territory, that the state knew, or should have known about it -although this is more controversial as mentioned before-, and that it did not do enough to prevent or stop it. In this regard, as the International Court of Justice noted in the *Corfu Channel* case, it cannot be concluded from the mere fact of a state's control over its territory and waters that the state necessarily knew, or ought to have known, of any unlawful act perpetrated there, nor that it necessarily knew, or ought to have known, of the perpetrators[84].

The reference to the need for the State whose territory is being used for malicious computer activity to be aware of this fact and to deliberately allow it, also finds support in another paragraph of the 2015 expert group report, which recalls that "a determination that certain ICT-related activity has been launched or otherwise originated in the territory or ICT infrastructure of a State may not in itself be sufficient to attribute such activity to that State"[85] . This paragraph was further inspired, as regards infrastructure, by Rule 7 of the original Tallinn Manual, which is also mentioned in version 2.0, and which adds that while the above may not be considered as sufficient evidence to impute responsibility to the State in question, it does constitute an indication of responsibility[86] .

In this context, the European Union has adopted legal framework of allowing the adoption of restrictive measures in response to cyber-attacks. This framework is composed of Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (hereinafter

(August 2021), at p. 72, available at https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

[84] Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)

(Substantive Judgment) [1949] ICJ Reports 4, 18: "it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known the authors".

[85] Id., para. 28(f).

[86] SCHMITT, M.N. (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, cit. p. 91: "Accordingly, the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure, or that malware used against hacked cyber infrastructure is designed to 'report back' to another State's governmental cyber infrastructure, is usually insufficient evidence for attributing the operation to that State. That said, such usage can serve as an indication that the State in question may be associated with the operation".

"the Decision")[87] and Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (hereinafter "the Regulation")[88] . The Decision was extended for one year in May 2020, for another year in 2021,[89] and most recently for three years, until 18 May 2025,[90] showing the EU's commitment to the framework created in 2019.

The Decision and the Regulation aim to prevent and counter cyber-attacks that have a significant impact and constitute an external threat to the Union or its Member States, and are therefore consistent with the defense of the values, fundamental interests, security, independence, and integrity of the Union provided for in Article 21(2)(a) TEU. Furthermore, and only to the extent that they are deemed necessary for the fulfilment of the objectives of the CFSP provided for in Article 21 TEU, the Decision and the Regulation allow for restrictive measures in response to cyber-attacks - in this case attempted cyber-attacks are not envisaged - with a significant effect against third states or international organisations.

By decision and regulation adopted on 30 July 2020,[91] the Council imposed restrictive measures against six individuals and three entities from Russia, North Korea and China - thus avoiding singling out a state only - for their involvement in the attempted cyber-attack against the Organisation for the Prohibition of Chemical Weapons and in the

87 Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/7299/2019/INIT, OJ L 129I, 17.5.2019, p. 13/19.

88 Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks that threaten the Union or its Member States, ST/7302/2019/INIT, OJ L 129I, 17.5.2019, p. 1/12.

89 Council Decision (CFSP) 2020/651 of 14 May 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 153, 15.5.2020, p. 4-4; Council Decision (CFSP) 2021/796 of 17 May 2021 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 174I , 18.5.2021, p. 1-1.

90 Council Decision (CFSP) 2022/754 of 16 May 2022 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 138, 17.5.2022, p. 16-16.

91 Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 246, 30.7.2020, p. 12–17; Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 246, 30.7.2020, p. 4–9.

cyber-attacks publicly known as WannaCry, NotPetya and Operation Cloud Hopper. The Council imposed further restrictive measures on 22 October 2020 on two Russian nationals, including the current head of the Main Command of the Defence General Staff of the Armed Forces of the Russian Federation (GU/GRU), and a Russian official body, the 85th Main Centre for Special Services (GTsSS) of the Main Command of the Defence Staff of the Armed Forces of the Russian Federation (GU/GRU), for their involvement in the cyber-attack against the German Federal Parliament carried out in April and May 2015.[92] Subsequently, in November 2020 two listings of natural persons were amended following the receipt of updated information.[93]

In its first and second application of the framework of restrictive measures, however, this principle of due diligence was not mentioned. Nevertheless, in our view, the identification of certain entities and individuals as being responsible for cyber-attacks, or the attempted cyber-attack on the OPCW, may pave the way for the invocation of the due diligence principle in the future, and in particular to prove that Russia, North Korea and China must be, after these first applications, "aware" that these individuals and entities are launching cyber-attacks from their territory and/or infrastructures.

In this regard, the Government of Japan appears to have considering this possibility when holding that “when a State has received a credible notification from another State of the possibility that a person or group of persons located in its territory and receiving from it financial and other forms of support may be involved in a cyber operation that may cause serious adverse consequences, such as damage to a target State's critical infrastructure, the due diligence obligation owed by the informed State is presumed to include the obligation to exercise its capacity to influence the state-supported

92 Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 351I, 22.10.2020, p. 5/7; Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 351I, 22.10.2020, p. 1/4.

93 Council Decision (CFSP) 2020/1748 of 20 November 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 393, 23.11.2020, p. 19-20.

person or group of persons so as to prevent them from implementing such cyber operations."[94]

The principle of due diligence is particularly appropriate for the type of response to cyber-attacks that the Union has decided to adopt, which avoids the formal imputation of responsibility for cyber-attacks. Indeed, as it has been argued, the principle of due diligence is a palliative to the problem of international responsibility for the commission of a cyber-attack[95]. In the same vein, as it has been held in the UN context, the due diligence obligation is particularly important in cases where a malicious cyber operation may not be attributed to an actor, the territorial state from which the cyber operation was launched would be responsible from breach of the due diligence principle.[96]

However, the compatibility of the current EU cyber-sanctions regime with international law has also been questioned for a number of reasons, and particularly in light of the lack of internationally agreed obligations regulating behavior in cyberspace and the lack of attribution of cyberattacks to a State under the rules of state responsibility.[97]In this regard, the lack of attribution to specific international actors on which the framework is based may also significantly limit its purported deterrence effect.

VI. CONCLUSIONS

In light of the foregoing, a number of conclusions can be highlighted.

Firstly, the principle of due diligence is an international obligation based on customary international law that applies to activities in and from cyberspace.

[94] Ministry of Foreign Affairs of Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (28 May 2021), available at https://www.mofa.go.jp/files/100200935.pdf, at pp. 5-6.

[95] DELERUE, F., *Cyber operations and international law*, Cambridge University Press, 2020, p. 356.

[96] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States' UNODA, A/76/136 (August 2021), available at https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdfat p. 72: "Norway considers the due diligence obligation to be of particular importance in a cyber context. In situations where a targeted State cannot directly attribute (technically and legally) a wrongful cyber operation – for instance election interference – to the State from whose territory it is being carried out, the territorial State may nevertheless still be held accountable on the basis of a breach of the due diligence obligation."

[97] BOGDANOVA, I., & VÁSQUEZ CALLO-MÜLLER, M., "Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value", Vanderbilt Journal of Transnational Law, Vol. 54, No. 4, 2021, available at SSRN: https://ssrn.com/abstract=3976261, at page 943.

Consequently, a State may incur in international responsibility under international law if it knows, and arguably also if it should have known, that malicious cyber activities targeting third States are carried out from its territory, or through its territory, and fails to take adequate measures.

Secondly, despite the opposition of some States, including relevant States in the cyber context such as the United States or the United Kingdom, the due diligence principle has, in my view, a clear mandatory character. Two main arguments support this view: (i) the ICJ has referred to it as an international obligation, and (ii) the majority of States support also this view.

Thirdly, while the precise content of the principle depends on the circumstances and on the capabilities of the State that bears this international obligation, it is apparent that the duty of due diligence entails an obligation of means and not of result.

Fourthly, the European Union has seemingly evolved towards a more assertive position on the mandatory character of the principle. This is a positive development in line with the EU's self-proclaimed role as a responsible cyber actor protecting values in the digital world, in particular by promoting a free and secure global internet.[98]

Finally, the invocation of the principle of due diligence in future restrictive measures adopted by national and international actors such as the EU might be appropriate to signal cyber conduct that the these players consider unacceptable under international law. This could contribute to the development of international law, for instance by providing content to the discussions of the proposed UN convention on cybercrime, and by reinforcing the content and contours of the due diligence principle,

[98] See the document "A Common Vision, Acting Together: A Stronger Europe, Global Strategy for the Foreign and Security Policy of the European Union", presented by the High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the Commission (HR/VP) on 28 June 2016, in particular on pages 17-18, in relation to public diplomacy, and on pages 33-34, in relation to cyber diplomacy. On public diplomacy in the European Union, see also, among others, ORRICO SANDRIN, P., and RIBEIRO HOFFMANN, A., 'Silences and hierarchies in European Union Public Diplomacy', Revista Brasileira de Política Internacional, Vol 61, 1 (2018), pp. 1-18.

for instance by pointing to some States that their territory is being used for malicious cyber conduct that they should aim to halt and prevent.

BIBLIOGRAPHY

BOGDANOVA, I., & VÁSQUEZ CALLO-MÜLLER, M., "Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value", Vanderbilt Journal of Transnational Law, Vol. 54, No. 4, 2021, at page 943.

BOOTHBY, WH, "Cyber Capabilities", in BOOTHBY, WH (ed.), *New Technologies and the Law in War and Peace*, Cambridge University Press, Cambridge, 2018, p. 89.

CERVELL HORTAL, M.J., *La legítima defensa en el derecho internacional contemporáneo: (nuevos tiempos, nuevos actores, nuevos retos)*, *Tirant lo Blanch*, Valencia, 2017, p. 128.

COCO, A. & DIAS, T. "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law, European Journal of International Law, Volume 32, Issue 3, August 2021, Pages 771–806, at p. 806.

DELERUE, F., *Cyber operations and international law*, Cambridge University Press, 2020, p. 356.

GAUTIER, L. (Preface), *Stratégie nationale de la cyberdéfense*, Economica, Paris, 2018, p. 102.

GROTIUS, H., *De Jure Belli Ac Pacis* 1646, translated by KELSEY F. W., William Hein & Co, New York, 1995.

GUTIÉRREZ ESPADA, C., "La creciente necesidad de legislación contra las amenazas cibernéticas, fuentes de graves daños transnacionales", Cuadernos de Derecho Transnacional (Octubre 2022), Vol. 14, No. 2, pp. 10-46, at pp. 11 and 15.

GUTIERREZ ESPADA, C., *La Responsabilidad Internacional por el uso de la fuerza en el ciberespacio*, Aranzadi, Cizur menor, 2020.

MIADZVETSKAYA, Y. and WESSEL, R.A., "The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox", European Papers, Vol. 7, 2021, No 1, pp. 413-438, p. 413.

MONNHEIMER, M., *Due Diligence Obligations in International Human Rights Law*, Cambridge University Press, Cambridge, 2021, p. 80.

national Law.")", available at https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/

OKWORI, E.O., "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States", in DESTA, Y., HAILU, M. (eds) *Ethiopian Yearbook of International Law*, vol 2018, Springer, at pp. 205–242, p. 209.

ORRICO SANDRIN, P., and RIBEIRO HOFFMANN, A., 'Silences and hierarchies in European Union Public Diplomacy', Revista Brasileira de Política Internacional, Vol 61, 1 (2018), pp. 1-18.

PANTIN URDANETA, S., "EU Cyber sanctions and Cyber norms", in directionsblog.eu, available at https://directionsblog.eu/eu-cyber-sanctions-and-cyber-norms/

PAWLAK, P. and BIERSTEKER, T. (eds.), *Guardian of the Galaxy, EU cyber sanctions and norms in cyberspace*, Chaillot Paper 155, European Union Institute for Security Studies, 2019, p. 66.

REHRL, J., *Handbook on Cybersecurity The Common Security and Defence Policy of the European Union*, Federal Ministry of Defence of the Republic of Austria, Viena, 2018, p. 31.

SEGURA SERRANO, A. *El desafío de la ciberseguridad global*, Aranzadi, Cizur menor, 2023

SCHMITT, M.N. (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, p. 30.

SCHONDORF, R., "Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations (Transcript of the keynote speech delivered at the Stockton Center for International Law, U.S. Naval War College.

OTHER SOURCES

Alabama claims of the United States of America against Great Britain (1872) 24 RIAA 125, 129-131, at p. 129

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BOSNIA AND HERZEGOVINA v. SERBIA AND MONTENEGRO), Judgment of 26 February 2007, page 221, para. 430.

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, ICJ Reports 2005, p. 168, [179].

Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) (Judgment on the merits) [1949] ICJ Reports 4, 22.

G7 Declaration on responsible states behavior in cyberspace Lucca, 11 April 2017

International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2001. Text adopted by the International Law Commission at its fifty-third session, in 2001, and submitted to the General Assembly as a part of the Commission's report

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996 (I), pp. 241-242, para. 29.

Trail smelter case (United States, Canada), 16 April 1938 and 11 March 1941, Reports of International Arbitral awards, pp. 1905-1982, at p. 1963

UNGA (1972) Declaration of the United Nations Conference on the Human Environment (16 June 1972). UN Doc A/RES/2994 (Stockholm Declaration), principle 21.

UNGA (1992) Declaration on Environment and Development (12 Aug 1992). UN Doc A/CONF.151/26 (Rio Declaration), principle 2