A LEGAL MAP OF CYBERSPACE

(Reflections on some official positions of States and international organisations)

This publication is the result of the R+D+i Project within the framework of the state programmes for the generation of knowledge and scientific and technological strengthening of the R+D+i system and R+D+i DE oriented to the Challenges of Society, 2020 call. Project PID2020-112577RB-I00 (“La búsqueda de una regulación internacional para las actividades cibernéticas ¿una ineludible necesidad?”), funded by MCIN/ AEI/10.13039/501100011033

A LEGAL MAP OF CYBERSPACE

(Reflections on some official positions of States and international organisations)

Contents

Previous words

This work brings to a close the work carried out over three years as part of the project 'The search for international regulation for cyber activities: an unavoidable necessity?' (R+D+i project within the framework of the state programmes for the generation of knowledge and scientific and technological strengthening, 'Challenges of Society').

From the outset, our objective was to try to clarify existing doubts regarding the legal norms applicable to cyberspace, that complex environment in which states and actors increasingly interact. As we argued in the initial report we wrote for the award of the project, we wanted to 'shed some light' on both existing and emerging problems. During this time, the members of the research and work team have endeavoured to remain faithful to the commitment they made at the time, analysing the application of international law to cyberspace in different publications, reporting their results at conferences and seminars and trying to solve practical problems in various forums and institutions. As a final touch, we thought it necessary to produce a final publication, offering a general map of how different States approached the rules applicable to cyberspace in order, above all, to expose the different perspectives adopted with respect to the problems that have proven to be more complex in recent years.

Aware that it would be impossible to cover everything, in this book we have chosen to select those actors that we have considered most useful for the intended purpose: the European Union, whose exponential normative involvement we have witnessed as the project developed; Spain, an obligatory and necessary reference for specifying the problems that our country must face in this area; Africa and Latin America and the Caribbean, as a group of states that are perhaps somewhat neglected in cyberspace issues but which are also beginning to shed light on the necessary regulation; China and Russia, as powers whose involvement in cyberspace is vital, but which have also shown that they have a very different vision in some respects; and finally, the United States, whose technological and geostrategic weight has also proven to be essential in cyberspace and its legal configuration. Five researchers on the project, including its two PIs (María José Cervell Hortal, Juan Jorge Piernas López, Eugenia López-Jacoíste Díaz, Irene Vázquez Serrano and Mónica Chinchilla Adell), have been involved in these tasks and Professor Gutiérrez Espada has also drawn up final conclusions in light of the reflections

made in each chapter by its authors, which will undoubtedly allow the reader to gain first-hand knowledge of the legal map of cyberspace that we wanted to draw.

Thus ends our direct involvement with this project, but not our commitment to closely follow the evolution of cyberspace issues. Reality has confirmed what we sensed: there are still many doubts and, despite our efforts, the task cannot yet be considered finished.

María José Cervell Hortal

Principal Researcher 1

The European Union's position on the application of international law in cyberspace

Juan Jorge PIERNAS LÓPEZ
Professor of International Public Law and International Relations
University of Murcia

SUMMARY: I. INTRODUCTION. II. ON THE APPLICABILITY OF INTERNATIONAL LAW IN CYBERSPACE III. ON THE APPLICABILITY OF INTERNATIONAL LAW IN CYBERSPACE 1. The principle of due diligence. 2. Countermeasures. IV. THE COMMON POSITION OF THE EUROPEAN UNION: CONVERGENCE AND DIVERGENCE IN THE POSITIONS OF THE EU MEMBER STATES. V. POSSIBLE RESPONSES OF EUROPEAN UNION LAW TO CYBER-ATTACKS. 1. Primary law. 1.1. Activation of the solidarity clause. 1.2. Activation of the mutual defense clause. 2. Secondary law. 2.1. Adoption of sanctions against those responsible for cyber-attacks. 2.2. 2.2. Adoption of anti-coercion measures. VI. CONCLUSIONS

I. INTRODUCTION

In its second Cybersecurity Strategy, published on December 16, 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, stated that the Union "must develop an EU position on the application of international law in cyberspace."[1]

On November 18, 2024, the Council adopted a Declaration by the EU and its Member States on a common understanding of the application of international law in cyberspace (hereinafter also "the Declaration").[2] The Declaration builds on previous documents that provide insight into the position of the Union's institutions, particularly the Commission (and the High Representative), the Council, and the European Parliament, with respect to the applicability, in general, of international law to cyberspace, as well as the application, in particular, of some of its principles and rules. The Declaration notes that its terms complement and are to be interpreted without prejudice to the "current and future" national positions of the Member States of the EU,

1 Joint Communication to the European Parliament and the Council, The EU Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final, p. 23.

2 The statement can be consulted at the following link: https:

as well as to any future developments of this common understanding on the application of international law to cyberspace. [3]

Within this framework, the following lines analyze, firstly, the Union's position on the applicability of international law in cyberspace. Secondly, it examines the application of international law in cyberspace, and in particular some of its principles and institutions, such as the principle of due diligence and countermeasures, to which the European institutions have referred in greater detail. Third, the main convergences and divergences on the application of international law to cyberspace that emerge from the positions published up to April 2024 by the EU Member States are presented. It then examines the main responses that the European Union could adopt in the event of a cyber-attack, under the primary and secondary law of this organization, in particular the activation of the mutual solidarity and mutual defense clauses on the one hand, and the adoption of sanctions and anti-coercion measures on the other. Finally, a number of concluding remarks are included.

II. ON THE APPLICABILITY OF INTERNATIONAL LAW IN CYBERSPACE

In its first cybersecurity strategy, published in 2013, the Union committed to applying existing international law to cyberspace.[4] The strategy added that "In the event that armed conflicts spill over into cyberspace, international humanitarian law and, where applicable, international human rights law will apply."[5] In relation to the above, the strategy clearly stated that the Union did not consider new rules of international law to be necessary in this area, but rather to apply existing law and promote rules of conduct.[6] In the unequivocal terms of the strategy:

---

3 Id., Annex, p. 4: "We present below a non-exhaustive set of legal elements, which complements and is without prejudice to current and future national positions of EU Member States as well as any future evolution of this common understanding on the application of international law to cyberspace

4 JOIN(2013) 1 final, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "EU Cybersecurity Strategy: Open, Secure and Safe Cyberspace", p. 16: "In its international cyberspace policy, the EU will promote the openness and freedom of the Internet, encourage activities to develop norms of conduct and implement existing international law in this field."

5 Id., p. 17.

6 See in this regard also GUTIÉRREZ ESPADA, C., *La Responsabilidad Internacional por el uso de la fuerza en el ciberespacio*, Aranzadi, Cizur Menor, 2020, in particular Chapter 1, section III, paragraph 7: "Personally, I find no reason to think that the International Law in force cannot be applied to human activities in cyberspace, in particular those of its norms that refer to the use of armed force and to the international responsibility that would result from its illegal use (not in accordance, therefore, with International Law)" and, by the same author, *La legítima defensa y el ciberespacio*, Comares, 2020, paragraph 22.

"The EU does not advocate the creation of new international legal instruments to address cyberspace-related issues"[7] .

A similar line held by the EU's Global Strategy for Foreign and Security Policy ("Global Strategy"), presented in June 2016, and endorsed by the Council at its meeting in October 2016.[8] In particular, the Global Strategy stated that the Union would engage in cyber diplomacy and capacity building actions with its partners and would seek to conclude agreements on responsible behavior in cyberspace "based on existing international law."[9]

A few months later, specifically on September 13, 2017, a joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy was published under the title *Resilience, Deterrence and Defence: strengthening EU cybersecurity* and undertaking a review of the 2013 Cybersecurity Strategy, because, as the joint communication stated "faced with a continuously evolving and worsening threat landscape, new actions are needed to resist and deter attacks in the future"[10] .

The Commission and the High Representative referred to a detailed evaluation of the Cybersecurity Strategy, dated the same date as the joint communication (September 13, 2017). This evaluation underlined that, while the main objectives of the 2013 Strategy remained in place, its text did not address new challenges caused, *inter alia*, by technological developments such as the so-called "Internet of Things" [11] . The evaluation also recognized that, from the point of view of effectiveness, the Strategy had only partially achieved its main objectives .[12]

---

7 JOIN(2013) 1 final, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "EU Cybersecurity Strategy: Open, Secure and Safe Cyberspace", p. 17.

8 Council Conclusions on the Global Strategy on Foreign and Security Policy of the European Union, Luxembourg, October 17, 2016 (OR. en) 13202/16. See on this strategy DE CARLOS IZQUIERDO, J., "La nueva Estrategia de Seguridad Europea 2016", IEEE, Documento Marco 16/2016, 2016; or BORDONADO, J., "Nueva Estrategia Europea de Seguridad", *Análisis GESI*, 13/2016, 2016.

9 Global Strategy, pp. 35-36.

10 Joint Communication from the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament and the Council, Resilience, deterrence and defense: strengthening EU cybersecurity Brussels, 13.9.2017 JOIN(2017) 450 final, p. 3.

11 Commission staff working document, assessment of the EU 2013 Cybersecurity Strategy, Brussels, 13.9.2017 SWD(2017) 295 final.

12 Id., p. 57.

In this context, the joint communication proposed a package of cybersecurity measures, also referred to as the "EU Cyber Security Package", organized around three main objectives:

(i) strengthen the EU's resilience to cyber-attacks,

(ii) to create an effective cyber deterrent in the EU,

(iii) strengthen international cooperation in cybersecurity.

For our purposes, it should be noted that the Union was more forceful in its defense of the application of international law in cyberspace, also supporting the conclusions of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, created within the United Nations. Thus, the joint communication stated that

> "The EU firmly believes that international law, and in particular the UN Charter, applies in cyberspace. As a complement to binding international law, the EU supports the voluntary non-binding norms, rules and principles of responsible state behaviour formulated by the UN Group of Governmental Experts, and encourages the development and implementation of regional confidence-building measures, both in the Organization for Security and Cooperation in Europe and in other regions."[13] .

In relation to the above, the reports of the United Nations Group of Governmental Experts have concluded that international law, and the United Nations Charter in particular, are applicable to cyberspace. [14]

There is no doubt, therefore, about the European Union's position on the applicability of international law in general, and of some of its areas, such as international humanitarian law and the Charter of the United Nations, in cyberspace. In this respect, as the representative of the Union to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security has recently expressed, on behalf of the EU and its Member States, clearly that "The international community recognises that existing international law, including the UN

---

13 Id., p. 21.

14 See, for example, the 2013 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98). On the application of international law to cyberspace and the responses that the international legal system offers to States that are victims of cyber-attacks, see MOYNIHAN. H., "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", Research Paper, Chatham House, The Royal Institute of International Affairs, 2019; BANNELIER, K. AND CHRISTAKIS, T. "Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors", *Les Cahiers de la Revue Défense Nationale*, 2017, pp. 1-86, or GROSS, O., "Legal Obligations of States Directly Affected by Cyber-Incidents," *Cornell International Law Journal*, vol. 48, 2015, pp. 1-38.

Charter in its entirety is applicable in cyberspace and is essential for maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. States have also recognized the applicability of the law of state responsibility, international human rights law, and in situations of armed conflict, international humanitarian law".[15]

Likewise, and particularly relevant, the Declaration of November 18, 2024 reaffirms unequivocally that international law, in particular the United Nations Charter, international human rights law and international humanitarian law are fully applicable in cyberspace. [16]

III. ON THE APPLICATION OF INTERNATIONAL LAW TO CYBERSPACE

The aforementioned cyber diplomacy toolkit (or framework for a joint response to malicious cyber activities) concluded by stating that the Union would continue to work on the development of the framework for a joint EU diplomatic response to malicious cyber activities, namely by developing guidelines for the implementation of the toolkit[17] . These guidelines were adopted by the Political and Security Committee a few months later, namely in October 2017, in fulfillment of its functions to implement the policies agreed in this area under Article 38 TEU.[18]

The implementation guidelines further clarified the Union's position, not on the applicability but on the application of existing international law to cyberspace, adding in particular that the applicable international law includes:

> "the Charter of the United Nations, and specifically Articles 2(4) (prohibition of the use of force), 33 (peaceful settlement of disputes) and 51 (inherent right to act in individual or collective self-defense in response to armed attack), and international humanitarian law, [and] international legal instruments such as the Budapest Convention on Cybercrime."[19]

---

15 EU Statement - UN Open-Ended Working Group on ICT: International Law 19.12.2023, New York, available at the following link: https:

16 Declaration, *cit*., Annex, p. 4: "The European Union and its Member States reaffirm that international law, in particular the UN Charter, international human rights law and international humanitarian law, fully applies to cyberspace". In relation to the applicability of international humanitarian law, the Declaration devotes a section on the subject of international humanitarian law within the chapter on "Rights and Duties of States".

17 Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ("cyber diplomacy toolkit"), doc. 9916/17, p. 5.

18 Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, Brussels, 9 October 2017, CYBER 142CFSP/PESC 855COPS 302RELEX 836.

19 *Id*., p. 3 (author's translation).

In addition, the guidelines noted that the Tallinn Manual 2.0 provides an example of academic analysis of how existing international law could be applied to cyber operations.[20] The guidelines also proclaimed that the Union's response in this area should respect international law and fundamental rights and freedoms.[21]

Subsequent to the adoption of the guidelines, in April 2018, the Council again "strongly" advocated that existing international law applies to cyberspace, stressing that respect for international law, and in particular the UN Charter, is essential to maintain peace and stability.[22] This position was confirmed in the 2020 cybersecurity strategy, mentioned *above*, in which the Commission and the High Representative considered that the Union is best placed to promote, coordinate and consolidate the positions of the Member States in international fora in this field.[23]

It is also relevant to highlight the so-called "Cyber posture", adopted by the Council on May 23, 2022. The Council reaffirmed the Union's commitment to the settlement of international disputes in cyberspace by peaceful means and the application of international law, including international human rights law and international humanitarian law, to the actions of States in cyberspace.[24]

The cyber posture also showed the Union's commitment to collaborate with the United Nations in this area, and in particular with its first and third committees, adding that existing international law applies "without reservation" in and with respect to cyberspace.[25] Finally, the cyber position concluded by noting that it will constitute a step towards establishing "a doctrine for EU action in cyberspace, based on enhanced resilience, capabilities and response options, as well as a shared position on the application of international law in cyberspace."[26]

Recently, the Declaration on the common position of the Member States and the Union of November 2024 specifies, in a non-exhaustive manner, certain rights and obligations of States in cyberspace. In particular, the Declaration confirms the essential nature of the principle of sovereignty in international law, which can be violated through

---

20 *Id*., p. 3, footnote 5.
21 *Id*., p. 4.
22 Council conclusions on malicious cyber activities - approval, Brussels, 16 April 2018, 7925/18, p. 3.
23 Joint Communication to the European Parliament and the Council, The EU Cybersecurity Strategy for the Digital Decade, *cit.* p. 23.
24 Council conclusions on the development of the European Union's cyber posture, Brussels, 23 May 2022, 9364/22, paragraph 16, p. 12.
25 *Id*., paragraph 18, p. 12.
26 *Id*., paragraph 30, p. 19 (author's translation).

malicious cyber operations, attributed to a State, affecting, for example, its territorial integrity.[27] The declaration also stresses the importance of the principle of non-intervention in this area and points out that coercion can mean forcing another State to involuntarily follow a course of action or to renounce it, which can also be done through cyber means such as coercive interference in ICT systems, cloud services and networks on the territory of State, or even within its jurisdiction without its consent, within the framework of its "domaine réservé", provided that it is imputable to a State.[28]

The Declaration confirms that sovereignty is a basic principle of international law. A violation of the obligation to respect sovereignty may occur when a cyber operation, attributable to one State, violates the territorial integrity of another State or leads to interference with or usurpation of inherently governmental functions of that State. In addition, coercive interference with information and communication technology (ICT) systems, cloud services and networks on the territory of another State or within its jurisdiction may constitute prohibited intervention in violation of international law if such interference is attributable to a State

The Declaration also refers to other principles of international law as part of the "Rights and Obligations of States", in particular the principle of due diligence, the prohibition of the use of force, compliance with international humanitarian law and compliance with international human rights law. Finally, after a section devoted to the attribution of conduct triggering State responsibility in cyberspace (Section II), Section III of the Declaration lists the possible responses of States to the commission of malicious cyber activities, in particular the following (i) peaceful settlement of disputes, in accordance with Articles 2(3) and 33(1) of the UN Charter, (ii) retaliatory measures, (iii) and measures whose wrongfulness is excluded under certain conditions, in particular (a) self-defense, (b) countermeasures, (c) force majeure, (d) distress, and (e) state of necessity.

We analyze the position of the Union and the Member States in more detail with respect to some of these principles and possible responses, in particular the principle of due diligence and countermeasures below.

1.THE PRINCIPLE OF DUE DILIGENCE

[27] Declaration, *cit*., Annex, p. 4.
[28] *Id*., p. 5.

The 2017 Implementation Guidelines for the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activity noted that in the event that a State knowingly allows its territory to be used for malicious cyber activity, including internationally wrongful acts using ICT, 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. [29]

The 2017 guidelines added that, in accordance with voluntary standards, States should not knowingly allow their territory to be used for internationally wrongful acts, and should respond to appropriate requests for assistance from another State. The implementation guidelines did not explicitly mention the existence of an obligation or principle of "due diligence" under international law, and emphasized the non-binding nature of UN standards in this regard.

The text of the guidelines was consistent with the 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 not knowingly permit the use of their territory for malicious cyber activities, and "advocated" that States should assist each other . [30]

In a similar vein, the 2019 Council Decision establishing the EU sanctions regime in response to cyber-attacks noted that "States [...] should seek to ensure that their territory is not used by non-state actors to commit such acts" in reference to the aforementioned 2015 UN Group of Governmental Experts Report.[31]

In this context, on 12 April 2019, the then High Representative of the European Union for Foreign Affairs and Common Security issued, on behalf of the EU, a statement on the respect of a rules-based order in cyberspace which stressed, once again, the application of international law, including the principle of due diligence, to cyberspace,

---

29 *Ibid*.

30 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 work together to prevent harmful practices in the field of ICTs and not knowingly allow their territory to be used to commit internationally illegal acts using ICTs". It also called for greater information sharing and assistance in pursuing the use of ICTs for terrorist and criminal purposes, stressing that States must ensure full respect for human rights, including the right to privacy and freedom of expression.

31 Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber attacks posing a threat to the Union or its Member States, OJ L 129I, 17.5.2019, pp. 13-19, preamble.

with reference however to the 2015 consensus of the United Nations Group of Experts[32] , in which, as stated above, the enforceability of the principle appeared diluted.

Significant, however, is the change in this respect in the revised 2023 implementation guidelines, which are considerably stronger in characterizing the principle as an obligation under international law. In particular, the guidelines state that States have:

> "due diligence obligation under international law not to knowingly allow their territory to be used for acts contrary to the rights of other States and may also request other States to cooperate in the management of cyber incidents, in accordance with the United Nations framework for the responsible behavior of States in cyberspace." [33]

The revised guidelines clearly distinguish the above statement from the non-binding standards cited in the 2017 guidelines by holding that:

> "In addition, the agreed rules on responsible State conduct affirm, inter alia, that States should not knowingly allow their territory to be used to commit internationally wrongful acts using ICTs, and should respond to appropriate requests for assistance from another State"[34] .

On the other hand, the revised guidelines emphasize that requesting a State to prevent or deal with a cyber incident does not, by itself, constitute the imputation of international responsibility:

> "The EU and its Member States may request States to take appropriate measures to prevent or deal with cyber incidents originating in their territory, bearing in mind that an indication that a cyber attack emanates from the territory or infrastructure of a State does not, of itself, imply that State's responsibility for the incident, or that notification to a State that its territory is being used for an unlawful act does not, of itself, imply that it is responsible for the act itself."[35]

---

32 Statement by the High Representative, on behalf of the EU, on respecting a rules-based order in cyberspace, 12 April 2019. It states that "In order to maintain an open, stable and secure cyberspace, the international community needs to do more to address malicious cyber activities and must govern its use of ICTs by the application of existing international law in cyberspace, as well as through the observance of the norms, rules and principles of responsible behaviour by States, which are articulated in the cumulative reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE). In this regard, States must not knowingly allow their territory to be used for malicious activities using ICTs, as stated in the 2015 UNGGE report." The statement is available at the following link: https:

33 Revised Implementation Guidelines for the e-Diplomacy Toolkit, Brussels, June 8, 2023 (OR. en) 10289/23, point 12.

34 *Ibid*.

35 *Ibid*.

The United Kingdom's exit from the European Union may help explain the change in the Union's position, given this State's traditional defense of the non-mandatory nature of the due diligence principle. In this regard, as underlined by a study published by the Ministry of Defense of the Republic of Austria in 2018, funded by the EU and prefaced by the 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"[36] .

This evolution is also reflected in the November 2024 Declaration, which unambiguously states that due diligence is a principle of international law that has been interpreted by the Court of Justice as establishing an obligation for States not to knowingly permit the use of their territory for acts contrary to the rights of other States.[37]

The Declaration specifies that due diligence is an obligation of conduct, not of result, and stresses that States have jurisdiction over ICTs and are therefore obliged to ensure that this ICT infrastructure is not used by non-State or State actors for acts contrary to the rights of other States, once they know or even should have known of such activities. Furthermore, the Declaration states that States are obliged to take all appropriate and reasonably available and feasible measures, in the given context, to act against cyber operations that violate the rights of another State under international law. The same obligation applies to cyber activities within the territory or ICT infrastructure that they otherwise effectively control. As a corollary to these obligations, the Declaration concludes that if a State fails to exercise due diligence in relation to cyber activities taking place in its territory or using ICT infrastructure located in its territory, it may commit an internationally wrongful act, although it also clarifies that the obligation of due diligence does not require preventive monitoring of all cyber activities and ICT infrastructure in a State's territory or under its effective control.[38]

2. COUNTERMEASURES

---

36 REHRL, J., *Handbook on Cybersecurit.y 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.

37 Declaration, *cit*.

38 *Ibid*.

The 2017 Implementation Guidelines of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activity specifically referred to the possibility for a Member State to take *non-forceful countermeasures* against a State that has committed an internationally wrongful act through a cyberattack, in order to stop the malicious cyber activity,[39] confirming the "instrumental" and non-punitive nature of "countermeasures".[40]

In the terms used by the guidelines, in line with the substantive and procedural requirements for countermeasures under international law:

> "A Member State that is the victim of malicious cyber activity that constitutes an internationally wrongful act may, under certain conditions, lawfully resort to non-forcible and proportionate countermeasures. These countermeasures constitute actions directed at another State that is responsible for the internationally wrongful act, which would otherwise violate an obligation owed to that State. Such non-forcible countermeasures are conducted to compel or convince the latter to cease the malicious cyber activity, in compliance with its international obligations."[41]

The *Cyber Diplomacy Toolbox* guidelines did not provide for the possibility of other Member States to participate in countermeasures, nor for countermeasures to be taken collectively[42] , as was the case, according to the same document, with the right of self-defense guaranteed by Article 51 of the UN Charter in serious cases where malicious cyber activities could amount to the use of force or an armed attack within the meaning of the Charter. Confirming this position, in the context of the European Union, some

---

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

40 *El Derecho Internacional (Corazón y Funciones),* Civitas-Thomson Reuters, Editorial Aranzadi, Cizur Menor (Navarra), 2022, p. 351, paragraph 27 of chapter 7: Already in 1996, when approving on first reading its Draft on State responsibility, the ILC opted for an "instrumental" and not "punitive" conception of countermeasures (commentary 2 to art. 47, ILC Yearbook 1996, II, Part Two); and a year later (as. Gabcíkovo-Nagymaros), the ICJ reaffirmed this idea when it gave it a new meaning in its first reading. 47, ILC Yearbook 1996, II, Part Two); and a year later (as. Gabcíkovo-Nagymaros) the ICJ reaffirmed the idea by taking it for granted in the regulation of countermeasures in existing law (ICJ Reports 1997, pp. 56-57).

41 Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, Brussels, 9 October 2017, *cit*.

42 Guidelines for the Implementation of the EU Joint Diplomatic Response Framework for Malicious Cyber Activities, Brussels, 9 October 2017, p. 10: "A Member State that is the victim of a malicious cyber activity constituting an internationally wrongful act may, under certain conditions, have legal recourse to non-forceful and proportionate countermeasures. These countermeasures constitute actions directed at another State responsible for the internationally wrongful act, which would otherwise breach an obligation owed to that State. Such non-forceful countermeasures are taken in order to compel or convince the latter to cease the malicious cyberactivity, in compliance with its international obligations."

authors have considered the lack of collective countermeasures as a significant limitation to the Union's action.[43]

However, the European External Action Service has recently defended the lawfulness of collective countermeasures, not specifically referring to the cyber domain, with reference to international practice since the adoption of the International Law Commission ("ILC") Draft Articles in 2001, at least as a possible response to the violation of peremptory norms. [44]

Moreover, the International Law Commission already noted in 2001 that existing practice at the time included examples of a non-injured international organization taking countermeasures against an allegedly responsible State, citing in particular the measures taken by the Council of the European Union against Burma/Myanmar in view of the "gross and systematic violations of human rights in Burma". [45] Ten years later, the ILC again invoked this precedent in the same vein, adding:

> "A more recent example is the action taken by the Council of the European Union in view of the existing situation in Libya; the EU "strongly condemn[ed] the violence and use of force against civilians and deplore[d] the repression against peaceful demonstrators.""[46]

On the other hand, in the context of hybrid attacks, the European Parliament has been advocating since 2021 a reinterpretation of the mutual defense and solidarity clauses enshrined in Articles 42(7) TEU and 222 TFEU, and to which we will refer later,

---

43 See in this regard HÄRMÄ, K. and MINÁRIK, T., "European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox", The NATO Cooperative Cyber Defence Centre of Excellence: "there are two major obstacles to qualify a countermeasure response: firstly, the original malicious cyber activity has to be attributed to a state, not simply to a non-state actor operating from the state's territory; and secondly, only the state affected by the malicious cyber activity is entitled to resort to countermeasures, which limits the possibility for other EU member states to assist the affected state, as their response must not rise to the level of a countermeasure" (author's translation).

44 European External Action Service (Council of the European Union [General Secretariat]), Third-party Countermeasures under International Law, *cit.*

45 Draft articles on responsibility of international organizations 2011, adopted by the International Law Commission at its sixty-third session, held in 2011, and submitted to the General Assembly as part of the report of the Commission on the work of that session (A/66/10, para. 87), p. 96. See also for this reference GUTIÉRREZ ESPADA, C., "Las contramedidas de terceros (evolución del concepto a la luz de la práctica internacional)", *Anuario Español de Derecho Internacional*, vol. 40, 2024, pp. 581-603, p. 5.

46 Article 49 of the Draft Articles on Responsibility of International Organizations for Internationally Wrongful Acts, with commentaries [2011], commentary No. 9 to article 49, p. 100.

allowing, *among other things, the adoption of* collective countermeasures by EU Member States on a voluntary basis. [47]

In 2022, the European Parliament expressed a similar view in relation to China. The Parliament stressed

> "the need to foster closer cooperation with NATO and G7 countries to combat hybrid threats, such as cyber-attacks and disinformation campaigns emanating from China; allowing, for example, member states to impose collective countermeasures on a voluntary basis, even in cases where attacks are not so serious as to trigger Article 5 of the NATO Treaty or Article 42(7) TEU."[48]

In the same year, the European Parliament also considered "deterrence, attribution and collective countermeasures, including sanctions" as one of the areas of work of the recent special committee on foreign interference in all democratic processes in the European Union, including disinformation, and strengthening integrity, transparency and accountability in the European Parliament."[49]

The Parliament stated emphatically, in a resolution adopted in parallel to the above decision, that countermeasures in this context may include sanctions adopted under Articles 29 TEU and 215 TFEU,[50] and referred to those adopted in case of cyber-attacks under Council Decision (CFSP) 2019/797 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States[51] and Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against

---

47 European Parliament Resolution of 7 October 2021 on the state of EU cyber defence capabilities (2020/2256(INI)) OJ C 132, 24.3.2022, p. 102-112, paragraph 35. See, for a similar proposal, European Parliament Resolution of 17 February 2022 on the implementation of the Common Security and Defence Policy - Annual Report 2021 (2021/2183(INI)), OJ C 342, 6.9.2022, p. 167-190, paragraph 54.

48 European Parliament resolution of 16 September 2021 on a new EU-China strategy (2021/2037(INI)) OJ C 117, 11.3.2022, p. 40-52, paragraph 27.

49 Decision of the European Parliament of 10 March 2022 on setting up a special committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 2), and defining its responsibilities, numerical composition and mandate (2022/2585(RSO)), OJ C 347, 9.9.2022, p. 238-240, paragraph K(1)(a)(x). This decision has been amended in 2023 without affecting the cited part. Decision of the European Parliament of 14 February 2023 amending the Decision of 10 March 2022 on the establishment of a special committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 2), and adapting its name and powers (2023/2566(RSO)). OJ C 283, 11.8.2023, p. 60-63.

50 European Parliament Resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)), OJ C 347, 9.9.2022, p. 61-96, at 136-142.

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

cyber-attacks threatening the Union or its Member States, which will also be discussed in this paper.[52]

It is also relevant that the European Parliament requested "the Union to clearly define what constitutes an internationally wrongful act and to establish minimum thresholds for the implementation of countermeasures as a consequence of this new definition, which should be accompanied by an impact assessment in order to provide legal certainty [...]".[53]

On the other hand, some authors have recently argued that the General Court ("GC") should have explored the possible lawfulness of the restrictive measures adopted by the Council of the Union in light of Article 54 of the ILC Draft Articles as collective countermeasures taken in response to Venezuela's violation of peremptory norms, noting in this regard that this would have been consistent with the fact that the GC has held in the recent *RT France* case that the EU restrictive measures against Russia were adopted on the basis of a finding that Russia had violated *erga omnes* rules.[54]

In this regard, it is indeed relevant that in the *RT France* case, the General Court concluded that

> "the restrictive measures in question may be understood as the reaction, by the peaceful means at the Union's disposal and in order to achieve the objectives set out in Article 3(5) TEU, of a subject of international law to an aggression in breach of Article 2(4) of the Charter of the United Nations and, consequently, to a ***breach of the obligations erga omnes imposed by international law*** (emphasis added)."[55]

This conclusion, as pointed out by GESTRI, is very significant in that it seems to grant a direct right to the EU, as a subject of international law with a legal personality distinct from that of the Member States, to invoke liability in case of violation of its obligations towards the international community,[56] which it could do, *inter alia*, by means of collective cyber countermeasures.

---

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

53 European Parliament Resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation, cited in paragraph 137.

54 KASSOTI, E. 'Beyond Collective Countermeasures and Towards an Autonomous External Sanctioning Power? The General Court's Judgment in Case T-65/18 RENV, Venezuela v Council, *European Papers*, vol. 9, 2024, no. 1, pp. 247-259, (European Forum, 3 July 2024)', pp. 247-259, at p. 257.

55 T-125/22, *RT France*, EU:T:2022:483, par. 164. See also paragraph 86.

56 GESTRI, M., 'Sanctions, Collective Countermeasures and the EU', *Italian Yearbook of International Law*, vol. 32, 2022, pp. 67-92, p. 83.

Finally, in the November 2024 Declaration, the EU and its Member States recognize that countermeasures, cyber or otherwise, are one of the possible responses that States may legitimately adopt in response to malicious cyber activities. However, the Declaration restricts their invocation to the "injured State", and states that they must be consistent with the relevant rules of customary international law, which would also reinforce their individual character and the prohibition, in principle, of collective countermeasures. The Declaration has not, therefore, followed the lead suggested by Estonia and other States, as well as by the European Parliament, regarding the possibility of collective countermeasures, sticking to the classical position on this figure which seems to be the only one that allows consensus at the present time of all the Member States and of the Union itself.[57]

IV. THE COMMON POSITION OF THE EUROPEAN UNION: CONVERGENCE AND DIVERGENCE IN THE POSITIONS OF THE EU MEMBER STATES

A recent study analyzed all published positions of European Union Member States on the application of international law to cyberspace up to April 2024, a total of 13.[58] As mentioned in its introduction, the study was intended to inform the feasibility of developing a common EU position on how key rules of international law regulate the activities of states in cyberspace, and was intended to help identify those issues on which consensus could easily be reached among EU Member States and those where differences of legal opinion or silence on the matter could pose a challenge to moving forward in this regard.[59] Once the first common position of the EU and its Member States was adopted in November 2024, it is possible to see the remarkable reflection of the positions published by the States in the common position.

In particular, the authors of the study highlighted the convergence between the positions of the EU Member States on the following aspects, which have been reflected in the common position: [60]

(i) general applicability of international law in cyberspace,

---

57 Declaration, *cit*.

58 SCHMITT, M. N. & VIHUL, L., "European Approaches to the Application of International Law in Cyberspace: A Comparative Legal Analysis Policy brief", *EU Cyber Direct*, July 2024, pp. 1-91. For an earlier study on this issue based on the then 9 published positions see OSULA, A.M., et al., "EU Common Position on International Law and Cyberspace", *Masaryk University Journal of Law and Technology*, vol.16, 1, 2022, pp. 89-123.

59 *Id*., p. 10.

60 *Id*., pp. 85-86.

(ii) The "full consensus" as to the status of the due diligence principle as a rule of international law

(iii) The characterization of the prohibition of intervention in international law as consisting of coercion and *domaine réservé*.

(iv) The determination of whether a State's cyber operation has violated the prohibition on the use of force contained in Article 2(4) of the UN Charter and customary international law, and the determination of whether a cyber operation has risen to the level of an armed attack triggering a State's right of self-defense under Article 51 of the Charter and customary law. As the study points out, there is a clear tendency to apply a "scale and effects" approach. There is also agreement, as the authors note, that the threshold for the use of force is lower than that applied in determinations of armed attack or, as the Declaration notes, "the use of force does not always constitute an armed attack".[61]

(v) Broad consensus on the secondary rules of international law relating to the law of State responsibility, in particular States consider the International Law Commission's articles on State responsibility to be a "reliable restatement" of the customary rules of State responsibility.

contrast, the authors of the study note divergences between the positions of the EU Member States on the following aspects, which have not, in fact, been addressed in the common position reached in November 2024: [62]

(i) Questions not strictly linked to the cyber field, such as whether self-defense can be invoked in response to armed attacks by non-State actors, whether an armed response is possible in a State that is unwilling or unable to stop armed attacks from its territory, or whether collective cyber countermeasures are possible.[63]

(ii) Cyber-related issues, such as whether a state's sovereignty is violated by interfering with or usurping inherently governmental functions, such as the conduct of elections. As the authors point out, seven national positions

---

61 Declaration, *cit*. p. 6.

62 SCHMITT, M. N. & VIHUL, L., 'European Approaches to the Application of International Law in Cyberspace: A Comparative Legal Analysis Policy brief', *cit*.

63 See in this regard CERVELL HORTAL, Mª. J., 'Sobre la doctrina "unwilling or unable State" (¿podría el fin justificar los medios?)', *Revista española de derecho internacional*, Vol. 70, No. 1, 2018, pp. 77-100, at pp. 84-87.

expressly embrace the notion that sovereignty could be violated for this reason, while the remaining five do not address the issue. In this regard, while the Declaration does mention the possibility of a violation of sovereignty in the case of interference with or usurpation of inherently governmental functions of another State, it does not specify the holding of elections as an example of such a violation.[64]

(iii) Furthermore, as the study notes, five EU states believe that the due diligence obligation could be breached because a state failed to take adequate measures to prevent hostile cyber operations of the required nature being launched from or through its territory. For their part, seven States are silent on the matter and, as the authors point out, this silence raises the question of whether they would limit the obligation to situations where hostile cyber operations are ongoing. In this regard, as discussed above, the Declaration appears to refer to ongoing malicious activities and specifically rejects that the due diligence obligation requires preventive vigilance actions.

(iv) Thresholds for determining whether serious non-physical harm violates rules of international law such as territorial integrity and inviolability, use of force and armed attack. The authors note that States vary significantly in their interpretation of these thresholds or, given the difficulty of articulating a clear threshold, the positions do not develop this issue in depth.

In the light of these conclusions, the authors rightly emphasized that the European Union could move towards a common position in those areas where there is a broad consensus, as has finally been done, as well as in those areas that have not been addressed in depth by the States but on which no significant divergences are expected, such as international human rights law and peaceful settlement of disputes. [65]

Finally, the authors also consider that International Humanitarian Law constitutes an area in which it would be desirable for States to make a significant effort to develop

64 Declaration, *cit*. p. 4. On the issue, CERVELL HORTAL, Mª. J., "Ciberinjerencias en procesos electorales y principio de no intervención (una perspectiva internacional y europea)", *Revista Electrónica de Estudios Internacionales*, vol. 45, June 2023, pp. 1-33.

65 *Ibid*.

common positions to regulate the use of cyber operations during armed conflicts, which the Declaration also does, as mentioned above.[66]

V. POSSIBLE RESPONSES OF THE EUROPEAN UNION LAW TO CYBER-ATTACKS

PRIMARY LAW

1.1. Activation of the solidarity clause

The EU Cybersecurity Strategy foreseen as early as 2013 that EU Member States can invoke the solidarity clause provided for in Article 222 TFEU in the face of a cyber attack of particular gravity[67] , which was confirmed in the 2017 review of the strategy[68] . Similarly, the European Parliament in 2012 called "cyber attacks" one of the main security threats and, while accepting that Member States retain primary responsibility for crisis management within their territory, considered it essential to establish "binding solidarity between Member States and a coordinated response to such threats" . [69]

To that end, the Parliament called for "an appropriate balance between flexibility and consistency as regards the types of attacks and disasters for which the [solidarity] clause can be activated, so as to ensure that significant threats, such as attacks in cyberspace, pandemics or energy shortages, are not overlooked; notes that the solidarity clause could also cover serious incidents occurring outside the Union that have a direct and significant impact on a Member State"[70] .

---

66 *Id*., pp. 86-87.

67 The Strategy noted, in particular, that if a cyber incident "appears to be related to cyber espionage or a state-sponsored attack, or affects national security, national law enforcement and defense authorities should alert their counterparts that they are under attack and are in a position to defend themselves. Early warning mechanisms and, if necessary, crisis management or other procedures will then be activated. A particularly serious cyber incident or attack could be sufficient grounds for a Member State to invoke the EU solidarity clause (Article 222 of the Treaty on the Functioning of the European Union)." Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Union Cybersecurity Strategy: Open, Secure and Safe Cyberspace, JOIN/2013/01 final, p. 21.

68 Joint Communication to the European Parliament and the Council, Resilience, deterrence and defence: strengthening EU cybersecurity, JOIN/2017/0450 final, p. 9. See also in this respect 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. 239: "The need to respond to a particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause".

69 European Parliament Resolution of 22 November 2012 on the EU mutual defence and solidarity clauses: political and operational dimensions (2012/2223(INI)), (2015/C 419/21), recital H. See on this issue PIERNAS LÓPEZ, J.J., *Ciberdiplomacy and cyberdefence in the European Union*, Thomson Reuters Aranzadi, 2020, e.g. at p. 150 *et seq.*

70 *Id*., paragraph 20.

Therefore, both the Member States, through the cyber defense policy framework, and the Commission, the European Parliament and the High Representative consider that the solidarity clause can be invoked in the event of a cyber attack.

The Member States of the Union do indeed have at their disposal the clause provided for in Article 222 TFEU[71] , and developed by the Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause[72] , although this is a mechanism originally designed to deal with acts of terrorism or natural disasters. However, the recent Declaration of November 2024 does not mention this possible response, which in our opinion would have been desirable, although its absence could be justified by the fact that the solidarity clause is not based on international law but strictly on Union law.

1.2. Activation of the mutual defense clause

The cyber defense policy framework foresees, in case of cyber attack, the possible application of the mutual assistance or mutual defense clause included in Article 42(7) TEU[73] . In the same vein, the 2017 cyber diplomacy toolkit implementation guidelines also mentioned the possibility for Member States to invoke Article 42(7) TEU in case of armed aggression on the territory of a Member State .[74]

In accordance with this article

> "If a Member State is the object of armed aggression on its territory, the other Member States shall render it aid and assistance by all the means in their power, in accordance with Article 51 of the Charter of the United Nations. This is without prejudice to the specific character of the security and defense policy of certain Member States.
>
> Commitments and cooperation in this area will continue to be consistent with the commitments undertaken within the framework of the North Atlantic Treaty Organization, which

71 See on this clause, GONZÁLEZ ALONSO, L. N. "¿Daños jurídicos colaterales?: La invocación del artículo 42.7 del Tratado de la Unión Europea y la lucha contra el terrorismo internacional", *Revista electrónica de estudios internacionales*, 2016, n.º. 32, pp. 1-23; or URREA CORRES, M., "Las cláusulas de asistencia mutua y solidaridad tras los atentados de París: la respuesta europea frente al terrorismo internacional", *Revista Española de Derecho Europeo,* 2016, n.º 57, pp. 13-34.

72 Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause, OJ L 192, 1.7.2014, p. 53/58. See also doc. 12607/15 "IPCR Standard Operating Procedures", agreed by the "Friends of the Chair" Group and annotated by COREPER in October 2015.

73 EU cyber defense policy framework (2018 update), Brussels, November 19, 2018, 14413/18, p. 9. See on this issue PIERNAS LÓPEZ, J.J., *Ciberdiplomacy and cyberdefense ..., op. cit.* e.g. at p. 159 *et seq*.

74 Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, Brussels, 9 October 2017, *cit.* p. 10.

will remain, for its member states, the foundation of their collective defense and its implementing body."

In connection with the foregoing, we consider it necessary to use the term "armed aggression" *ex* Article 42.7 TEU as a synonym for "armed attack" within the meaning of Article 51 of the Charter, although we are aware that the wording of Article 42.7 allows us to state, as has been done[75] , that the concept of armed aggression in Article 42.7 TEU is broader than that of armed attack *under* Article 51 of the Charter, and would therefore cover the assistance and aid of the Member States of the Union to the State affected by an attack that does not reach the threshold required to invoke the right of self-defense provided for in the United Nations Charter (minor uses of force, for example).

We believe, however, that equating armed attack with armed aggression is preferable for at least three reasons. First, the term armed aggression (*agression armée*) appears in the French version of Article 51 of the UN Charter, and has been translated into other versions, in particular the English version, as *armed attack*. Secondly, the preparatory work of the predecessor of Article 42.7 TEU in the Constitutional Treaty would also support this equation[76] , given that the mutual assistance clause was included with the express intention of replicating Article V of the Treaty of Brussels of 17 March 1948, as amended by the Protocol signed in Paris on 23 October 1954[77] . Well, this article uses the term "armed aggression" in its French version[78] , as well as in the Spanish version[79] , and *armed attack* in the English version[80] , as does Article 42.7 TEU.

---

75 See in this regard SARI, A., "The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats," *Harvard National Security Journal*, vol. 10, 2019, pp. 417 and 419.

76 *Id*., p. 418.

77 Instrument of Ratification of the Protocol of Accession of the Kingdom of Spain and the Portuguese Republic to the Treaty on collaboration in economic, social and cultural matters and on collective self-defense, signed in Brussels on March 17, 1948, as amended by the Protocol amending and supplementing the Treaty of Brussels, signed in Paris on October 23, 1954, and the Exchange of Letters of the Ministers of Foreign Affairs of the respective countries, regarding the Spanish reservation to Article 10 of the aforementioned Treaty. BOE No. 110, of May 8, 1990, pp. 12141 to 12156.

78 "In the event that one of the High Contracting Parties should be the object of armed aggression in Europe, the others shall, in accordance with the provisions of Article 51 of the Charter of the United Nations, give it aid and assistance by all means in their power, military and otherwise."

79 *Id*., Article V: "In the event that one of the High Contracting Parties should be the object of armed aggression in Europe, the other High Contracting Parties shall, in accordance with Article 51 of the Charter of the United Nations, give them aid and assistance by all the means in their power, military or otherwise.

80 "If any of the High Contracting Parties should be the object of an armed attack in Europe, the other High Contracting Parties will, in accordance with the provisions of Article 51 of the Charter of the United Nations, afford the Party so attacked all the military and other aid and assistance in their power."

Thirdly, the equating of the two terms is useful to provide the Member States of the Union with interpretative guidelines on the cases in which it is acceptable to invoke the mutual assistance clause. This is visible in the case of the possible invocation of the cyber-attack clause, for which the case law and doctrine relating to Article 51 of the Charter, including the Tallinn Manual 2.0, provide solid criteria, which would not be applicable if the concept of armed aggression were different from that of armed attack *under* Article 51 of the Charter.

This last ground, or criterion of utility, is particularly relevant in the context of Article 42(7) TEU, given that, as part of the Common Foreign and Security Policy , this provision cannot be interpreted by the Court of Justice of the Union, as provided for in Article 24(1) TEU. It is therefore up to each Member State, starting with the Member State concerned, to verify whether the criteria required for invoking this article, and in particular the existence of an "armed aggression", are met. In the event of disagreement between a Member State, recourse could be had to Article 32 TEU, which provides that the Member States shall consult each other within the European Council and the Council on any foreign and security policy issue of general interest, as could certainly be the invocation of Article 42(7) TEU, in order to define a common approach.

Finally, the November 2024 Declaration includes, unlike the solidarity clause, the possibility for Member States to invoke Article 42(7) TEU, and does so in the section on self-defense against malicious cyber activities.[81]

In short, it is clear from the documents published by the EU institutions that Member States could activate both the solidarity clause and the mutual defense clause provided for in primary law to respond to hostile cyber activities such as cyber-attacks, provided they are of the scale and effects required under international law.

2. DERIVATIVE LAW

2.1. Adoption of sanctions against cyberattackers

The growing threat posed by cyber-attacks prompted an increasingly determined reaction from the European Union, which led to the adoption of a legal framework of restrictive measures to deal with them, and the implementation of the same. 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

[81] Declaration, *cit*.

Member States (hereinafter "the Decision")[82] , extended in May 2020[83] , and by again in 2022 until 18 May 2025,[84] and by Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber attacks that threaten the Union or its Member States (hereinafter "the Regulation")[85]

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 insofar as they are deemed necessary for the fulfillment of the objectives of the CFSP provided for in Article 21 TEU, the Decision and the Regulation allow the application of 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 organizations.

Article 1(3) of the aforementioned Decision states that cyber-attacks are actions involving any of the following elements:

> "(a) access to information systems; (b) intrusion into information systems; (c) intrusion into data; or (d) interception of data, where such actions are not duly authorized by the owner or other rightholder of the system or data or part thereof, or are not permitted by Union or Member State law".

The restrictive measures that Member States may agree to under the 2019 Decision are set out in Articles 4 and 5 of the 2019 Decision. These measures consist of restrictions on entry or transit and/or the freezing of funds and economic resources, the former applicable only to natural persons and the latter to natural persons, legal persons, entities or bodies. It is also prohibited to make funds available, directly or indirectly, to the sanctioned persons and entities or organizations.

The natural persons against whom these restrictive measures are directed must be listed in the Annex to the Decision. Thus, by Decision and Regulation adopted on July

---

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

83 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.

84 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.

85 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.

30, 2020[86] , the Council imposed restrictive measures against six individuals and three entities from Russia, North Korea and China - thus avoiding singling out a single State - for their involvement in the attempted cyberattack against the Organization for the Prohibition of Chemical Weapons and in the cyberattacks publicly known as *WannaCry*, *NotPetya* and *Operation Cloud Hopper*. The Council imposed new restrictive measures on October 22, 2020 on two Russian nationals, including the head of the Main Command of the Defense General Staff of the Armed Forces of the Russian Federation (GU/GRU), and a Russian official body, the 85th Main Special Services Center (GTsSS) of the Main Command of the Defense General Staff of the Armed Forces of the Russian Federation (GU/GRU), for their involvement in the cyberattack against the German Federal Parliament carried out in April and May 2015.[87] Subsequently, in May 2024, the grounds were updated to include six individuals and two entities on the list of natural or legal persons, entities and bodies subject to restrictive measures contained in the Annex to Decision (CFSP) 2019/797,[88] and finally in June 2024 the aforementioned list was again amended to include six natural persons.[89]

Sanctions adopted on the basis of the thematic regime described above are, in our view, compatible with public international law. In particular, due to their targeted nature, and the fact that they do not necessarily constitute an internationally wrongful act, EU sanctions in response to cyber-attacks could be qualified as retaliatory measures under public international law, even if they are not directly aimed at inducing a change of behavior in a subject of international law, which leads to a certain distortion of the figure

---

86 Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber attacks that threaten 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 that threaten the Union or its Member States, OJ L 246, 30.7.2020, p. 4/9.

87 Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber attacks that threaten 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 that threaten the Union or its Member States, OJ L 351I, 22.10.2020, p. 1/4.

88 Council Decision (CFSP) 2024/1391 of 17 May 2024 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber attacks that threaten the Union or its Member States, OJ L, 2024/1391, 17.5.2024; and Council Implementing Regulation (EU) 2024/1390 of 17 May 2024 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber attacks that threaten the Union or its Member States, OJ L, 2024/1390, 17.5.2024.

89 Council Decision (CFSP) 2024/1779 of 24 June 2024 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber attacks that threaten the Union or its Member States, OJ L, 2024/1779, 24.6.2024; and Council Implementing Regulation (EU) 2024/1778 of 24 June 2024 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber attacks that threaten the Union or its Member States OJ L, 2024/1778, 24.6.2024.

of retaliation traditionally considered as instrumental and non-punitive.[90] This conclusion has also been reached recently by some Member States of the European Union in their public positions on the application of international law to cyberspace.[91]

Sanctions adopted under the regime of restrictive measures can contribute to the development of international law in this area, not only by reflecting the views of a large group of States, but also because they can contribute to the invocation of the principle of due diligence vis-à-vis the States from whose jurisdiction the cyber-attacks targeted by the sanctions were launched. The Union would thus help to reinforce the normative nature of this principle and to promote compliance with existing international law, one of the objectives laid down in the Treaties.

2.2. Adoption of anti-coercion measures

On November 22, 2023 the European Union adopted Regulation (EU) 2023/2675 of the European Parliament and of the Council on the protection of the Union and its Member States against economic coercion by third countries (hereinafter referred to as "the Regulation" or "the Anti-Coercion Regulation"). [92]

The Regulation allows the European Union to adopt response measures to counter economic coercion by third countries against the Union or its member states. Under the Regulation, the Union's response measures may take the form of countermeasures, i.e. measures involving non-compliance with international obligations vis-à-vis the third country. In this way, the Regulation gives the Union the ability and creates a framework for the identification and adoption of countermeasures under international law to deal with economic coercion by third countries. In this regard, although the Regulation does not specifically refer to the cyber field, we consider that nothing prevents, at principle, both that coercion is carried out by cyber means and that the Union's response could be carried out in the future by cyber means.

---

90 See on this issue PIERNAS LÓPEZ, J.J., *Ciberdiplomacia y ciberdefensa ..., op. cit.* p. 192.

91 Estonia Position Paper, 2021, available at https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf, p. 29 "[Retorsion] measures could, for example include the expulsion of diplomats or applying restrictive measures to officials of a third country such as asset freezes or travel bans. One example of such a mechanism would be the European Union's cyber sanctions regime and cyber diplomacy toolbox, which offer an array of measures that could be taken as a response to malicious cyber operations."

92 Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the protection of the Union and its Member States against economic coercion by third countries, OJ L, 2023/2675, 7.12.2023.

Specifically, as provided for in Article 8(4) of the Regulation, insofar as the third country's measure constitutes an internationally wrongful act, the Union's response measures may consist of measures in breach of international obligations vis-à-vis the third country. In this way, the Regulation recognizes the Union's capacity to adopt countermeasures under international law to deal with economic coercion exercised by third countries, not only against the Union but also against its Member States.

Thus, as stated in paragraph 13 of the preamble to the Regulation, in a passage that is fully applicable to the cyber field:

> "Customary international law, as noted in Articles 22 and 49 to 53 of [the United Nations International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts] (ARSIWA), permits, subject to certain restrictions, such as proportionality and prior notice, the imposition of countermeasures, namely measures which would otherwise be contrary to the international obligations of an injured party towards the country responsible for a breach of international law, and which are intended to obtain cessation of or reparation for the breach. Consequently, the Union's response measures could, where appropriate, consist not only of measures consistent with the Union's international obligations, but also of non-compliance with international obligations towards the third country concerned, insofar as the economic coercion by the third country constitutes an internationally wrongful act. Under international law, in accordance with the principle of proportionality, countermeasures must be proportionate to the injury suffered, taking into account the gravity of the internationally wrongful acts and the rights in question. In that regard, under international law, the injury caused to the Union or to a Member State is understood to include injury caused to economic operators of the Union."[93]

With regard to this recent regulation, as explained *above*, in the current state of development of international law, in principle only the State victim of a breach of international law is entitled to resort to countermeasures, as stated by the International Law Commission in 2001 [94] . However, the Regulation allows the Union to act not only when it is the injured party but also when one or more of its Member States are injured.

---

93 See also paragraph 11: "In accordance with the principle of proportionality, it is necessary and appropriate, in order to create an effective and comprehensive framework for Union action against economic coercion, to lay down rules concerning the examination, determination and adoption of countermeasures to deal with economic coercion exercised by third countries".

94 Paragraphs 1 and 8 of the Introductory Commentary to chapter II of part three of the Draft on Responsibility of States for internationally wrongful acts, Responsibility of States for internationally wrongful acts, Official Records of the General Assembly, Fifty-sixth Session, Report of the International Law Commission, Fifty-third Session (23 April-1 June and 2 July-10 August 2001), Supplement No. 1 (A/53/40), Official Records of the General Assembly, Fifty-sixth Session (23 April-1 June and 2 July-10 August 2001), Supplement No. 1 (A/53/40), Official Records of the General Assembly, Fifty-sixth Session (23 April-1 June and 2 July-10 August 2001), Supplement No. 10 (A/56/10), United Nations, New York, 2001, pp. 1-591, at pp. 309-316 (hereinafter also ILC 2021). See also J.A. FROWEIN "Reactions by not directly affected States to breaches of public international law", *RCADI* 1994-IV, vol. 248, 1995, Martinus Nijhoff, Dordrecht, p. 345.

In this sense, the Regulation seems to go beyond previous declarations and positions, given that it is a legislative and therefore binding act of the European Union.

However, it could also be argued, based on the Regulation itself, that the Union is also an injured party when a single Member State is subject to economic coercion, and therefore that it is not strictly speaking a matter of collective countermeasures. Indeed, according to the preamble of the Regulation "Economic coercion by a third country against a Member State affects the internal market of the Union and the Union as a whole."[95] Furthermore, the same paragraph of the preamble adds that "Member States, as individual subjects under international law, may not be empowered to counter economic coercion exercised on the Union by third countries",[96] which seems to support the thesis that the Union is not advocating collective countermeasures and even that it recognizes that these could ("may") be contrary to international law. This interpretation would also be consistent with the fact that the November 2024 Declaration has limited the invocation of countermeasures to the injured State.

The adoption of this regulation could pave the way for the adoption of other similar regulations concerning the violation of international law, and in particular of the principle of non-intervention, through cyber-attacks. Indeed, as discussed above, it is not inconceivable that economic coercion could be exercised through cyber-attacks carried out by third countries, and that the current anti-coercion regulation would be applicable to such cases.

VI. CONCLUSIONS

In light of the above considerations, the following conclusions can be reached:

First, the European Union has been very clear on the applicability of existing international law, and in particular the United Nations Charter and areas such as international humanitarian law, to cyberspace. Both the November 2024 Declaration and numerous declarations and documents of the institutions confirm the position of the Union and its Member States in this respect.

Secondly, the EU institutions have confirmed the application of international law to cyberspace in specific areas, such as the principle of sovereignty, the principle of non-intervention, the use of force, the principle of due diligence and countermeasures. In this respect, it is important to underline the evolution within the Union of the position on the

95 Regulation, preamble, paragraph 10.
96 *Ibid*.

principle of due diligence, which has become considerably more forceful in terms of its mandatory nature in recent years. It is also worth underlining the recognition, by various bodies and institutions of the Union, of the possibility of adopting collective countermeasures, in particular in response to breaches of *erga omnes* obligations, although the common position included in the November 2024 Declaration does not mention this possibility.

Thirdly, it has been noted that there is a remarkable convergence in the positions of the Member States on the application of international law to cyberspace, which has paved the way for the development of a common position of the Union in this field, adopted as described in November 2024.

Fourthly, the Union's primary law, and in particular the mutual solidarity and mutual defense clauses, can be interpreted, as the Union's institutions have done, as being applicable in response to cyber-attacks that are sufficiently serious. Furthermore, secondary legislation has in recent years been equipped with instruments specifically designed to respond to cyber-attacks, namely a system of restrictive measures against those responsible for them, and the possibility of adopting collective anti-coercion measures which could, in our opinion, be applied in the future also in the cyber field.

Finally, both the positions expressed by the EU institutions and the content of the legal acts adopted by them, for example as regards the definition of cyber-attack or the mandatory nature of the principle of due diligence, can contribute to the progressive development of international law, in line with the provisions of Article 3 TEU, paragraph 5 - an article whose mention is notably missing in the Declaration of November 2024 - and the case law of the European Courts,[97] and to the establishment of global rules, the conduct of States and other actors in this field for the benefit of global peace and security, as well as the fundamental rights and freedoms of citizens around the world.

Bibliography

BANNELIER, K., and CHRISTAKIS, T., "Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors", *Les Cahiers de la Revue Défense Nationale*, 2017, pp. 1-86.

97 T-65/18 RENV - *Venezuela v. Council*, EU:T:2023:529, nr. 87.

BORDONADO, J., "New European Security Strategy," *GESI Analysis*, 13/2016, 2016.

CERVELL HORTAL, Mª. J., 'Sobre la doctrina "unwilling or unable State" (¿podría el fin justificar los medios?)', *Revista española de derecho internacional*, vol. 70, No. 1, 2018, pp. 77-100.

ID., "Cyberinjerencias en procesos electorales y principio de no intervención (una perspectiva internacional y europea)", *Revista Electrónica de Estudios Internacionales*, vol. 45, June 2023, pp. 1-33.

DE CARLOS IZQUIERDO, J. "The new European Security Strategy 2016", IEEE, Framework Document 16/2016, 2016

FROWEIN, J.A. "Reactions by not directly affected States to breaches of public international law", *RCADI* 1994-IV, 1995, Martinus Nijhoff, Dordrecht, vol. 248.

GESTRI, M., "Sanctions, Collective Countermeasures and the EU", *Italian Yearbook of International Law*, vol. 32, 2022, pp. 67-92.

GONZÁLEZ ALONSO, L. N. "Collateral legal damage: The invocation of Article 42.7 of the Treaty on European Union and the fight against international terrorism", *Electronic Journal of International Studies*, 2016, n.º. 32, pp. 1-23.

GROSS, O. "Legal Obligations of States Directly Affected by Cyber-Incidents," *Cornell International Law Journal,* vol. 48, 2015, pp. 1-38.

GUTIÉRREZ ESPADA, C., 'Las "contramedidas de terceros" (evolución del concepto a la luz de la práctica internacional)', *Anuario español de derecho internacional*, nº 40, 2024, pp. 581-603.

ID. "The growing need for legislation against cyber threats, sources of serious transnational harm," Transnational Law Notebooks (October 2022), Vol. 14, No. 2, pp. 10-46.

ID. *La legítima defensa y el ciberespacio*, Comares, 2020.

ID. *La Responsabilidad Internacional por el uso de la fuerza en el ciberespacio*, Aranzadi, Cizur Menor, 2020.

GUTIÉRREZ ESPADA, C and CERVELL HORTAL, M.J., *El Derecho Internacional (Corazón y Funciones)*, Civitas-Thomson Reuters, Editorial Aranzadi, Cizur Menor (Navarra), 2022.

K. HÄRMÄ and T. MINÁRIK, "European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox," The NATO Cooperative Cyber Defence Centre of Excellence.

KASSOTI, E. 'Beyond Collective Countermeasures and Towards an Autonomous External Sanctioning Power? The General Court's Judgment in Case T-65/18 RENV, Venezuela v Council, *European Papers*, vol. 9, 2024, no. 1, (European Forum, 3 July 2024), pp. 247-259.

MOYNIHAN., H., "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", *Research Paper, Chatham House*, The Royal Institute of International Affairs, (2019).

OSULA, A.M., et al., 'EU Common Position on International Law and Cyberspace', *Masaryk University Journal of Law and Technology*, vol 16, 1, 2022, pp. 89-123.

PIERNAS LÓPEZ, J.J., *Ciberdiplomacia y ciberdefensa en la Unión Europea*, Thomson Reuters Aranzadi, 2020.

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.

SARI, A., "The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats," *Harvard National Security Journal*, vol. 19, 2019.

SCHMITT, M. N. & VIHUL, L., "European Approaches to the Application of International Law in Cyberspace: A Comparative Legal Analysis Policy brief", *EU Cyber Direct*, July 2024, pp. 1-91.

URREA CORRES, M., "Las cláusulas de asistencia mutua y solidaridad tras los atentados de París: la respuesta europea frente al terrorismo internacional", *Revista Española de Derecho Europeo*, n.º 57, 2016, pp. 13-34.

Spain and the international legal regulation of

(proposals for a possible official position)

María José CERVELL HORTAL

Professor of Public International Law and International Relations

University of Murcia

SUMMARY: I. INTRODUCTION: ON THE CONVENIENCE OF HAVING AN OFFICIAL POSITION ON CYBERSPACE. II. DOES SPAIN ALREADY HAVE A DEFINED OPINION ON THE INTERNATIONAL LEGAL REGULATION OF SPACE? III. WHAT IS ESSENTIAL IN ANY POSITION ON CYBERSPACE: BASIC OBLIGATIONS AND RIGHTS OF STATES. 1. Sovereignty as a starting point: yes, it is a norm. 2. 2. A more flexible principle of non-intervention. 3. Due diligence. IV. HOW TO CONFIGURE THE RESPONSIBILITY OF THE STATE. 1. Attribution. Towards a broad concept of countermeasures. 3. 3. State of necessity as an alternative. V. THE GREAT CONTROVERSIES. Use of force, armed attack and self-defense. 2. 2. How to apply international humanitarian law. 3. Human rights and their delicate situation in cyberspace. VI. CONCLUSIONS.

I. INTRODUCTION: ON THE DESIRABILITY OF HAVING AN OFFICIAL POSITION ON CYBERSPACE

The number of states deciding to officially make public their position on international law and cyberspace has been growing in recent years. The first to do so was the United States, when the legal advisor of the State Department, at the UScybercom Conference (September 18, 2012) expressly declared the application of that legal order to cyberspace[1] . In 2016, the same statement was repeated, but this time adding one more element to be taken into account: support for the development of an international consensus on additional non-binding norms of responsible behavior[2] which, as time

[1] Https://2009-2017.state.gov/s/l/releases/remarks/197924.htm . See DELERUE, F., "Toward and EU position on the application of International Law in cyberspace", *Briefing Paper, EU Cyber Direct*, available at https://eucyberdirect.eu/research/toward-an-eu-position-on-the-application-of-international-law-in-cyberspace.

[2] The document stated "the applicability of existing international law to State activity in cyberspace in both peacetime and during armed conflict," Statement by Brian J. Egan, legal advisor to the State Department, during a speech at Berkeley Law School: International Law and Stability in

would show, today are also a mandatory reference in most official positions on cyberspace.

The United Nations, particularly active in discussing issues related to technology and communications, became the natural forum in which States, regardless of whether or not they had an official position, could express their views. In 2014, the Group of Governmental Experts on Advances in Information and Telecommunications in the Context of International Security was created[3] , whose work would be taken over in 2018 by two other groups with, it could be said, different sensitivities. The Group of Governmental Experts on Promoting Responsible State Behavior in Cyberspace in the Context of International Security, promoted by the United States, would end its work in 2021[4] . For its part, the Russian-sponsored Open-Ended Working Group on ICT Developments in the Context of International Security[5] (OEWG) will continue to work until 2025, when it is due to be disbanded[6] . The statements that States have been making within these groups are also a direct way of finding out how they are addressing the issue . [7]

In 2019, several States made public for the first time documents specifically designed to declare their vision on international law and cyberspace (Estonia, the Netherlands, France)[8] . Since that date, quite a few more have been encouraged to do so and the example has also spread in some international organizations. In NATO, the

Cyberspace Berkeley Law - November 10, 2016, available at https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf

3 United Nations General Assembly Resolution 68/243.

4 With the drafting of a final report, doc. A/76/135, 14 July 2021. On the two groups and their work, see PONTA, A., "Responsible State behaviour in cyberspace: two new reports from parallel UN processes", *ASIL Insights*, vol 25, 14, 20 July 2021 and MOYNIHAN, H., "The application of international law to state cyberattacks. Sovereignty and non-intervention", *Research Paper, Chatham House*, December 2019, pp. 52 and 53.

5 Doc. A/C.1/73/L.27/Rev.1, 29 October 2018. The Group works on virtually identical issues to its predecessor, with perhaps its main difference being its open-ended nature, which also implies the participation of non-state actors.

6 A/RES/75/240, December 31, 2020. Its final report was to be adopted in 2021 (A/AC.290/2021/CRP.2, March 10, 2021).

7 The document "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", 13 July 2021, UN doc A/76/136.

8 A list of all the positions can be found on the website of the Cyber Law Toolkit project, sponsored by several institutions, in particular the CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence), https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions.

reference document is the 2020 *Joint Allied Doctrine for Cyberspace Operations*[9] ; the Organization of American States confirmed the application of international law to cyberspace at its 2020 plenary session[10] ; the African Union adopted in January 2024 a *Common Position on the application of international law to the use of information and communication technologies in cyberspace*[11] and the European Union did the same on 18 November 2024, in a *Declaration on a Common Position on International Law and Cyberspace*[12]

Within the European Union, thirteen Member States have an official position on international law and cyberspace. Spain is not among them and, although work is being done on the issue, until there is a specific document on the matter, the most recent official reference framework on the position of our country is the one expressed by the European Union in the Common Position of November 2024, in which it basically embraces what it has been stating for years before the United Nations: the application of international law to cyberspace and the commitment to the respect and implementation of the Eleven Non-Binding Rules of Responsible Behavior, proposed in 2015 by the United Nations Group of Governmental Experts on Developments in Information and Telecommunications .[13]

The official positions on cyberspace are convenient and even necessary because they are an excellent starting point to know what States think about the legal regime applicable to cyberspace: they all assume the general application of international law, but

---

9 *Allied Joint Doctrine for Cyberspace Operations* (AJP)-3.20 (available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf)

10 AG/RES. 2959 L-O/20, October 21, 2020.

11 Available at https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf?sequence=11&isAllowed=y

12 Declaration on a Common Position on International Law in Cyberspace, doc. 15833/24. On the EU's positions, see the chapter of this work devoted specifically to the issue, by Professor Juan Jorge Piernas López. Similar positions can be found in the Association of Southeast Asian Nations, *ASEAN Leaders' Statement on Cybersecurity Cooperation*, 16 November 2018, https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf) and the Organization for Security and Cooperation in Europe (Decision No. 1106, Initial OSCE Confidence-Building Package of Measures to Reduce the Risks of Conflict Arising from the Use of Information and Communication Technologies, doc. PC.DEC/1106, 3 December 2013).

13 They are eleven "norms, rules and principles of responsible behaviour by States" which, in the words of the Group itself, "can reduce risks to international peace, security and stability", doc. A/70/174, 22 July 2015, para. 10 . On these norms, see CERVELL HORTAL, Mª. J., "Un soft law para el ciberespacio? (De las normas no vinculantes y otras iniciativas)", Marcial Pons, 2025, in press .

some modulate it when it comes to specific sectors or introduce specific nuances that allow us, in addition, to know especially the parameters to be adjusted in case of cyberincidents and how to assume responsibilities for conduct carried out in the digital environment. In fact, the OEWG has on several occasions encouraged States to adopt this type of document,[14] especially useful on issues where talks at the United Nations have reached an impasse[15] . The European Union itself, when presenting its position to this group, was strongly in favor of them:

> "We see that, with every published national, regional or international position and common understanding on the application of international law to cyberspace, we make progress towards a truly common and global baseline of understanding."[16]

From the conviction of the convenience that more and more States should publish this type of positions on cyberspace, this chapter will analyze, in the first place, what is the current position of Spain on the international legal regime applicable to cyberspace, analyzing for this purpose the existing official documents. The remaining sections have been devoted to the aspects that, in the opinion of this writer, any official position on cyberspace should include. Not all the details will be analyzed in depth, as the limits of this contribution would be clearly exceeded, but we have included the issues that have given rise to most debate or those on which the States are still divided, trying to make concrete proposals of what Spain should expressly include.

---

14 And also several States support the idea; *ad. ex*., Statements of Czechia, 4th substantive session of the Open-ended Working Group on security of and in the use of information and telecommunications technologies 2021-2025, March 8, 2023, available at https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Czechia_Statement_-_OEWG_ICTs_-_Application_of_International_Law_-_8_March_2023.pdf.

15 Kajander, for example, shows how having them on board speeds up the discussion and presentation of certain issues in international forums. In particular, he expressly mentions how at the 2023 OEWG sessions Switzerland expressly stated that, in order to know more closely certain details about its views, its official position should be consulted (KAJANDER, A., "A tale of two draft resolutions: a report on the polarising International Law discussions at the 2023 OEWG substantive sessions", 2023, p. 10, available at https://ccdcoe.org/uploads/2023/12/Kajander-OEWGSummaryExportFinalL.pdf). Also on the desirability of these positions, see UNIDIR, *A Compendium of Good Practices Developing a National Position on the Interpretation of International Law and State Use of ICT,* 2024, available at https://unidir.org/wp-content/uploads/2024/05/UNIDIR_A_Compendium_of_Good_Practices_Developing_a_National_Position_on_the_Interpretation_of_International_Law_and_State_Use_of_ICT.pdf, pp. 1-12.

16 Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025 Ninth Substantive Session 2 - 6 December 2024 Key EU messages for Agenda item: International Law, para. 7, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/24_12_03_OEWG_ICT_Cyber_(December_2024)_-_Int_Law_-_FINAL_0.pdf

II. DOES SPAIN ALREADY HAVE A DEFINED OPINION ON THE INTERNATIONAL LEGAL REGULATION OF SPACE?

Spain, as already mentioned, does not yet have an official position on cyberspace[17] and no document allows to form an exact, detailed and complete idea of how our country understands that the Law should be applied to cyberspace. In fact, until the approval of the Declaration on a Common Position of the EU in November 2024, date from which it can be affirmed that Spain formally shares the opinion of the European Union on cyberspace, there were few documents that allowed us to get a precise idea of how our State conceived it legally. Only a few scattered brushstrokes in different publications allowed us to intuit the Spanish position on specific issues.

In 2013 the first National Cybersecurity Strategy was approved, establishing basic guidelines for action to address the vulnerability of cyberspace. Since then, Spain has been more active in cybersecurity issues[18] , although official documents did not always give many clues as to how it legally conceived cyberspace. The National Security Law (2015)[19] , besides a line dedicated to it in the Preamble, where it appears as a "concern" for society (along with others such as environment, energy or economic stability), merely states, in Article 10, the following:

> "Areas of special interest of National Security shall be considered those that require specific attention because they are basic to preserve the rights and freedoms, as well as the welfare of citizens, and to ensure the provision of essential services and resources. For the purposes of this law, they shall be, among others, *cybersecurity*, economic and financial security, maritime security, airspace and outer space security, energy security, health security and the preservation of the environment" (emphasis added).

The 2017 National Security Strategy[20] already contemplates cybersecurity in a concrete way, and giving it its own weight. Two years later, the National Cybersecurity

---

17 Although it is true that there have been attempts to write it and even some drafts. At the date of this writing, the author is not yet aware that it has materialized.

18 Thus, for example, Royal Decree-Law 12/2018 transposed into Spanish law the so-called NIS 1 Directive (EU Directive 2016/1148), which directly sought to improve cybersecurity in strategic sectors, which would later be developed by Royal Decree 43/20 (BOE January 28, 2021). There is, for the time being, no transposition of the NIS 2 Directive, although the deadline has already been met at the time of writing.

19 Law 36/2015, of September 28, BOE of September 29, 2015.

20 Available at https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/documents/2017-1824_estrategia_de_seguridad_nacional_esn_doble_pag.pdf

Strategy[21] would establish, as stated in its Introduction, "Spain's position before a new conception of cybersecurity within the framework of the National Security Policy". The Strategy itself is defined as a turning point, as it no longer seeks only "the protection of the technological heritage", but also enters the political, economic and social spheres. In other words, cybersecurity is no longer a mere technological issue, but has a role of its own, directly linked to security and defense. In fact, cyberspace is defined as a common global space, in which "the absence of sovereignty and its weak jurisdiction, the ease of access and the difficulty of attribution of the actions that take place in it", make it one of the great challenges of security .[22]

This is the document that gives us more information about Spain's views on cyberspace issues. In chapter 3, under the section "Purposes", the applicability of international law is expressly mentioned:

> "The transversality and global nature of cyberspace requires, in addition to cooperation and compliance with international law, the utmost respect for the principles contained in the Constitution and the United Nations Charter; in coherence with the National Security Strategy and with the initiatives developed in the European, regional and international framework, with national interests prevailing at all times".

In Objective V (Security of cyberspace in the international arena), it reiterates its commitment to the United Nations and to international law, while introducing non-binding standards of responsible behavior and support for confidence-building measures:

> "Spain] will advocate the creation of an international framework for conflict prevention, cooperation and stability in cyberspace, in which the principles of the United Nations Charter in its entirety, International Law, Human Rights and War Humanitarian Law are applied, as well as the non-binding norms on the responsible behavior of States.
>
> Aware of the importance of multilateralism, he considers relevant the role of the United Nations to advance in consensus building which, together with the adoption and implementation of confidence-building measures, collaboration and participation of all the actors involved (States, private sector, civil society, users and academia), constitute the basis for achieving security and stability in cyberspace and advancing towards its regulation".

Action Line 6 re-emphasizes the idea:

---

21 BOE April 30, 2019. It would then be completed with the 2022 National Cybersecurity Plan.

22 Chapter 1, p. 7 of the Strategy.

"Promote within the United Nations the search for consensus for the full respect of the Charter of the United Nations and the application and implementation of international law and norms for the responsible behavior of States. And likewise to advance in the adoption and implementation of Confidence Building Measures in cyberspace."

The 2021 National Security Strategy once again includes cyber-attacks as one of the major challenges, but this time expressly alluding to disinformation campaigns (most of which are generated and developed in a digital environment). This Strategy is clearer than its predecessor, since it expressly states that cyberspace makes it necessary to "incorporate new forms of action". In this case, it also describes the types of threats, classifying them into two:

- Cyber-attacks, understood as disruptive actions against systems and technological elements (*ransomware*, denial of services...).
- Cyberspace as an area in which illicit activities (cybercrime) are carried out.

Some more note on cyberspace can be found in the Doctrine for the employment of the FAS, published by the Ministry of Defense in 2018, which, in addition to including it as one of the new possible scenarios of conflict and as a field of interest for national security[23] , defines it as follows:

"The cyberspace domain is the artificial domain composed of infrastructures, networks, information and telecommunication systems and other electronic systems, by their interaction through the communication lines over which they propagate and the electromagnetic spectrum (EEM), as well as by the information that is stored or transmitted through them. It is transversal to other fields and is not subject to a specific geographical area. It is characterized by its extension, anonymity, immediacy and easy access. Finally, its artificial character and its rapid evolution generate continuous vulnerabilities and opportunities."[24]

In September of that same year (2018) the JEMAD approved the Cyber Defense Concept[25] , defining the capabilities and cooperation mechanisms between the actors involved in this field.

From all the documents reviewed so far, the first conclusion that can be drawn is that Spain is aware of the new threats generated by this environment, that it considers

[23] PDC-01(A) Doctrine for the employment of the SAF, Ministry of Defense, 2018, p. 20, para. 25 and p. 33, para. 79.

[24] *Id*., p. 81, para. 309.

[25] Https://emad.defensa.gob.es/prensa/noticias/2018/10/list/181023_Concepto_de_Ciberdefensa.html.

international law to be the applicable regulatory framework and that it also supports the non-binding norms of responsible behavior that are being forged at the international level. But, as we said, there is as yet no declaration or document that specifies in more detail how it actually conceives the application of international law to cyberspace. It is true that, as also noted, the publication of the Common Position of the European Union would allow a direct reference to this document, but it would not be superfluous for Spain, like other Member States, to have its own position on international law and cyberspace, mainly because it could be the opportunity to express its views on some still rather controversial issues.

III. THE ESSENTIALS OF ANY POSITION ON CYBERSPACE: BASIC STATE OBLIGATIONS AND RIGHTS

International law applies to cyberspace, as most states recognize. This is the position of NATO[26] and the European Union: "The EU and its Member States underline that international law, in particular the United Nations Charter, international human rights law and international humanitarian law fully apply to cyberspace"[27] . Similar positions can be found in the Organization of American States (OAS)[28] , the Association of Southeast Asian Nations (ASEAN)[29] and the Organization for Security and Cooperation in Europe (OSCE)[30]

Although this generalized recognition of the application of international law to cyberspace may lead us to think that the debate has been overcome, and that this statement is a truism, any document that implies a formal position on cyberspace should expressly

---

26 *Allied Joint Doctrine for Cyberspace Operations ...*, *op. cit.)* The document states on p. 19: "NATO Allies recognize that international law applies in cyberspace". In fact, such a statement had already been made at the Wales Summit of 5 September 2014 (https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease): "Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace" (para. 72). It would be reaffirmed at the 2016 Warsaw and 2018 Brussels summits. The *NATO Strategic Concept 2022* also stated: "We recognise the applicability of international law and will promote responsible behaviour in cyberspace and space" (p. 7, para. 25).

27 Statement on the Common Position of the European Union on Cyberspace, *op. cit.,* p. 4. It had earlier also stated this in the Council Conclusions on EU Policy on Cyber Defence, 22 May 2023, doc. 618/23, para. 32 and in the 2017 EU *Cybersecurity Strategy* ("The EU strongly promotes the position that international law, and in particular the UN Charter, applies in cyberspace").

28 AG/RES. 2959 (L-O/20), October 21, 2020, p. 1.

29 *ASEAN Leaders' Statement on Cybersecurity Cooperation*, *op. cit.*

30 Decision No. 1106, OSCE Initial Set of Confidence-Building Measures to Reduce the Risks of Conflict Arising from the Use of Information and Communication Technologies, doc. PC.DEC/1106, 3 December 2013.

state it. The Spanish Position should not, therefore, be an exception. It is common, in fact, to find this basic formula (*international law applies to cyberspace*), normally accompanied by references to the need to respect the framework of the United Nations Charter. It is a different matter what content is given to the different areas (non-intervention, sovereignty, due diligence, human rights, international humanitarian law, etc.).

A possible Spanish Position should also include a specific reference to the Eleven Norms, Rules and Principles for Responsible State Behavior, proposed by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in its 2015 Report[31] . Some States, and also the Common Position of the European Union, already do so, all of them nuancing that, despite not being binding rules[32] , they express commitments of a political nature. Moreover, let us remember that the Spanish Cybersecurity Strategy of 2019 mentioned them, so it would be congruent to confirm Spain's commitment to them. Also, the most recent Declaration published by Spain and the United States on the occasion of the second Dialogue on Cybersecurity and Digital Issues (June 6, 2024[33]) made express reference to these standards. Moreover, an eventual Spanish position could even include our country's commitment to the United Nations Cyberspace Action Agenda, designed to serve as a permanent forum to channel debates and progress on these issues, which will be the reference framework[34] , once the OEWG finishes its work. It does, in fact, the U.S.-Spanish Declaration just mentioned and also the EU Common Position.

---

31 *op. cit.*, para. 13.

32 Germany, e.g., *On the Application of International Law ..., op. cit,* pp. 12 and 16; Australia, *Australia's International Cyber Engagement Strategy*, Department of Foreign Affairs and Trade October 201, pp. 47-48. Also the EU Cyber Posture recalled the commitment of States "to act in accordance with voluntary and non-binding norms on responsible conduct in cyberspace", *Council Conclusions on the development of a European Union Cyber Posture*. The European Union, in fact, has expressly alluded to some of these Principles of Responsible Behaviour in its statements to the UN Open-Ended *Working Group on ICT: rules, norms and principles of responsible behaviour of States* (*EU Statement-UN Open-Ended Working Group on ICT: rules, norms and principles of responsible behaviour of States*, 30 March 2022). In the case of the EU, this is recognized in the Declaration on a Common Position on International Law in Cyberspace (doc. 15833/24), pp. 2-3.

33 Https://www.exteriores.gob.es/es/PoliticaExterior/Documents/240610%20EEU%20ES%20Declaraci%C3%B3n%20Conjunta%20Di%C3%A1logo%20Ciber-Digital%20versi%C3%B3n%20ES%20FINAL.pdf

34 This program was born to try to put an end to the existing division in the two groups of the United Nations in cyberspace. It was promoted by France (and supported by forty States and the European Union). On December 7, 2022, it was adopted by the General Assembly (A/RES/77/37, Action program to promote responsible behavior by States in the use of information and communication

1. SOVEREIGNTY AS A STARTING POINT: YES, IT IS A RULE.

Clarifying how sovereignty is conceived in cyberspace is an essential issue present in any position on cyberspace. The principle of non-intervention is the ultimate expression of state sovereignty, which also conditions the application of many other norms. The vast majority of states recognize this principle also in cyberspace, although it is true that some have preferred to qualify its legal nature and

The first issue in a possible Spanish position would be to make it clear that our country, in line with what the European Union advocates, conceives sovereignty as the primary rule of international law[35] . This is, in fact, what most States do, with the exception of the United Kingdom, which prefers to redirect the problems that may arise in this area exclusively to the principle of non-intervention .[36]

Perhaps the most complex issue to outline would be the link between the principle of sovereignty and actions against territorial integrity, whereby a Spanish cyber posture should expressly mention that the principle implies the jurisdiction of the State over persons, goods and activities that take place within its territorial limits. A specific reference to critical infrastructures would also be welcome, because although it is true that it could be included in the concept of "goods", the debates that have arisen in this regard would justify such express inclusion. It should also be recalled that in the Eleven Norms, Rules and Principles of Responsible State Conduct adopted within the United Nations[37] , it is expressly stated that "States should not knowingly engage in or support ICT activities contrary to their obligations under international law that intentionally

technologies in the context of international security. For the States that supported it, see doc. A/C.1/77/L.73, 13 October 2022).

35 Austria, Czech Republic, Costa Rica, Denmark, France...

36 For a broader study of the issue and what is defended by the United Kingdom, CERVELL HORTAL, Mª. J, "Ciberinjerencias en procesos electorales y principio de no intervención (una perspectiva internacional y europea)", *Revista Electrónica de Estudios Internacionales*, vol. 45, June 2023, pp. 1-33, pp. 26-27. In general, on the issue of sovereignty in cyberspace, by the same author, "Soberanía y ciberespacio: deben cambiar las reglas del juego?", *Seguridad y responsabilidad penal internacional en el uso de lsa TIC y la inteligencia artificial*, Iustel, 2024, pp. 65-80, pp. 73-79.

37 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 Report (doc. A/70/174, 22 July 2015, para. 13, endorsed by the General Assembly in 2018 (resolution A/RES/73/27, 5 December 2018).

damage critical infrastructure or otherwise impair the use and operation of critical infrastructure to provide services to the public".

On the other hand, given that physical territoriality and tangibility are concepts that sometimes do not find a perfect fit in cyberspace, an open wording, allowing broad interpretations, would be the best option, so as not to close the door to any kind of violation of sovereignty. Discussions have been frequent in this regard: is it necessary for the cyberoperation to take place or manifest itself in the infrastructure of the territory of the State affected by a possible violation of the principle, or would an encroachment on the functions of the Government be sufficient?[38] Let us think of cases in which a State decides to host sensitive data for its security in a cloud *hosted* in another State (remember that this is what Ukraine did when it was invaded by Russia[39]); or situations in which Internet traffic is diverted, changing the servers that provide the service. An express mention of this intangibility, or a reference to the fact that the territorial link could disappear in some cases, would undoubtedly be appropriate to cover these cases.

2. A MORE FLEXIBLE NON-INTERVENTION PRINCIPLE

The application of the principle of non-intervention in cyberspace is widely accepted[40] , with some nuances or exceptions by certain states. A position on cyberspace should note the customary nature of the principle and clarify, in a way, the necessary concurrence of two elements[41] : firstly, that such intervention falls within the State's own affairs (*domaine reservé*) and, secondly, that there is, in addition, a coercive element.

---

38 These were discussions that, in fact, already arose in the Tallinn *Manual* 2.0 (*Tallinn Manual 2.0 on the International Law applicable to cyber operations*, ed. by SCHMITT, M., Cambridge University Press, Cambridge, 2017, p. 23, para. 19).

39 From the first days of the conflict, the government made use of the so-called *Snowball Edge*, Amazon devices in which the data was taken to Poland and other states and from there stored on its cloud servers (the information can be found on the company's own website: https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future).

40 Not only the Tallinn Manual 2.0 is clear about this (*Tallinn Manual 2.0 ..., op. cit.*, rule 66, p. 31), but also the various groups in the United Nations that have worked on the issue. Both the Group of Governmental Experts on Advances in Information and Telecommunications in the Context of International Security, in its 2015 Report (doc. A/70/174, *Report of the Group of Governmental Experts on Advances in Information and Telecommunications in the Context of International Security*, 22 July 2015, p. 10, para. 13) as the Group of Governmental Experts on Promoting Responsible State Behavior in Cyberspace in the Context of International Security (Final Report of 28 May 2021, doc. A/76/135 of 14 July 2021, para. 71) recognize this.

41 Case concerning military and paramilitary activities in and against Nicaragua, *ICJ Reports 1986*, p. 108, para. 205.

The limits of these elements, which are already quite complex, are diluted even more in cyberspace, so it would be necessary, in addition, and especially given the concern that the issue is raising, to include in some way, as a violation of the principle, immaterial interferences; that is, those behaviors that, using cyberspace, intend not only a *physical* manipulation, but also to influence or manipulate aspects that are state prerogative, such as, for example, electoral processes. In fact, there are States (United States, Australia, Iran, United Kingdom) that expressly reflect this [42] . Also of concern are interventions that seek to alter networks or programs related to health or the financial system .[43]

Beyond what some states may have expressly stated with respect to the principle of non-intervention, what seems clear is that the traditional limits to it may be altered by certain operations in cyberspace. Given the difficulty of discerning in certain cases whether there is indeed coercion and whether there has been such interference, it would not be superfluous to add the nuance that the final decision will be taken on a "case-by-case" analysis. This is, in fact, the practice of several States (Canada, Estonia, Germany, Norway, Romania, Switzerland, Sweden or the Netherlands). The EU Common Position does not use the expression, but it can be seen, in its wording, that it leaves the question equally open to the final qualification that each State considers appropriate ("coercive interference with ICT systems, cloud-services and networks on another State's territory or within its jurisdiction without its consent, within its domaine réservé, *can* constitute a prohibited intervention under international law if it is attributable to a State"; emphasis added). The assessment of each situation on an individual basis would also make it possible to determine whether or not the threshold separating non-intervention and the use of force has been crossed (see section V.1 *below*).

3. DUE DILIGENCE

42 United States (*Official compendium ..., op. cit.,* p. 140) or Australia (*Australia's position on how international law applies to State conduct in cyberspace*), Iran (*Statement of the General Staff of the Armed Forces of the Islamic Republic of Iran on international law applicable to cyberspace*, August 2020, https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat), United Kingdom (*UK's position on applying international law to cyberspace, Attorney's General Speech Suella Braverman*, Chatham House, May 19, 2022, https://www.gov.uk/government/speeches/international-law-in-future-frontiers),...

43 See, for example, Costa Rica, Ireland and Italy (with respect to interventions in public health systems) or Australia (interference in the financial system).

The obligation of States to take the necessary measures to ensure that no acts are committed in their territory (or areas under their jurisdiction) that harm other States, presents several problems, even beyond the scope of cyberspace, and which mainly affect its legal nature (principle? rule? parameter of conduct?). Although some States are reluctant to accept due diligence as an obligation [44] (United States[45] , United Kingdom[46] , Australia, Canada, Israel or New Zealand)[47] , the European Union confirmed in its Position of 2024 its defense as such, so including an explicit reference in this sense in a possible Spanish position would be quite congruent. Let us not forget, on the other hand, that the obligation to respect the principle of due diligence has been pointed out by the International Court of Justice[48] , which has also emphasized, due to technological progress, the importance of principles such as this, not regulated by law[49]

In an official Spanish position, it would therefore be advisable to recognize due diligence as a legal obligation, while stating, however, that it is an obligation of behavior and not of result. This is what is done, for example, in France, Estonia, the Czech Republic, Australia, Finland, Germany, Italy, Japan, the Netherlands, Norway, Switzerland and Sweden. On the other hand, the due diligence obligation would, in principle, cover three parties: the State targeted by the cyber operation, the State in which the illicit activity takes place or of which the perpetrators are nationals, and the State to

---

44 SCHMITT, for example, considers that the rule exists (since the Corfu Channel case), but whether it is applicable (he believes it is) to cyberspace is another matter ("the pertinent question is whether it is reasonable to *interpret* that pre-existing rule as applicable to cyber operations", SCHMITT, M., "The United Kingdom on International Law in cyberspace", *EJIL Talk*, 24 May 2022). By the same author and in that vein, "In Defense of Due Diligence in Cyberspace", *The Yale Law Journal Forum*, vol. 125, 2015, pp. 68-81. On the debates about the norm in cyberspace, see also PIERNAS LÓPEZ, J. J., "The international law principle of due diligence and its application to the cyber context", *Anales de Derecho*, vol 41, 2024, pp. 52-59 and, by the same author, El *Derecho internacional y las contramedidas cibernéticas*, Aranzadi, 2024, pp. 47-58 .

45 "The United States has not identified the State practice and opinio juris that would support a claim that due diligence currently constitutes a general obligation under international law", *Official compendium*..., July 13, 2021, p. 141.

46 "...there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace", *Official compendium*..., *op. cit*., 13 July 2021, p. 117.

47 "Whether this norm also reflects a binding legal obligation is not settled...", *The Application of International Law to State Activity in Cyberspace*, New Zealand, December 1, 2020, p. 3, https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

48 Corfu Channel Case, *ICJ Reports 1949*, p. 4. In fact, the question had already been raised in the Isle of Palms arbitration, which held that States should protect the rights of other States in their territory (Isle of Palms Case, Netherlands-United States, 4 April 1928, *Report of International Arbitral Awards,* vol. II, pp. 829-871, p. 839).

49 Case concerning the Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, *ICJ Reports 1986*, para. 39.

which, if any, the activity is directly attributed. A complex question[50] is to clarify whether the obligation would also be applicable to the State that may have a mere transit status of the cyber-operation. It seems clear that if that State is aware of the situation and does not take measures, the principle would also be applicable to it, but an express reference to this problem would not go amiss, to avoid interpretative doubts.

IV. HOW TO CONFIGURE THE RESPONSIBILITY OF THE STATE

1. ATTRIBUTION

The applicability of the rules on international responsibility of States was accepted in 2015 by the Group of Governmental Experts on Developments in Information and Telecommunications and also by the Tallinn Manual[51] . An official position on cyberspace should take special care of this issue, expressly noting that the applicable rules would be those adopted in 2001 by the International Law Commission in its customary Draft Articles on Responsibility of States for Wrongful Acts (2001) . [52]

Actions carried out in cyberspace have the added difficulty of attribution. Some states specifically distinguish between technical, political and legal attribution, which is particularly convenient in cyberspace[53] . In fact, a political attribution does not necessarily have to entail legal consequences, as that would be a decision to be taken ultimately by the State concerned. Let us not forget that countermeasures taken against a State to which the action (or omission) has been wrongly attributed may cause States to commit a wrongful act and that is why they are particularly careful with the issue, so that

---

50 And that already highlighted in the Tallinn Manual 2.0, *op. cit.,* pp. 33-34 (comments 13-14 to rule 6), p. 42 (comment 42 to rule 6), p. 43 (comments 1 and 2 to rule 7).

51 Doc. A/70/74, 22 July 2015 (para. 28, f: "States must comply with their international obligations in relation to internationally wrongful acts") and *Tallinn Manual 2.0, op. cit.* standards 14 and 17, respectively

52 Resolution 56/83 of 12 December 2001 and doc. A/66/10 (Report of the International Law Commission 63rd session,26 April to 3 June and 4 July to 12 August 2011), respectively.

53 Canada: "Attribution in its legal sense is of course distinct from the technical identification (or technical attribution) of the actor responsible for malicious cyber activity, whether State or non-State, as well as from the public denunciation of the responsible actor (political attribution)" (International Law applicable in cyberspace. Government of Canada, April 2022, para. 10 https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng). In the same vein, the Netherlands (*Government of the Kingdom of the Netherlands, Appendix: International Law in cyberspace*, 26 September 2019, pp. 6-7), Sweden (Position Paper on the Application of International Law in Cyberspace, p. 5) and the United States (*Official compendium..., op. cit.,* pp. 141-142).

sometimes a mere political attribution would be sufficient for what the State is looking for (warnings for possible future actions).

Acts carried out by its organs are attributed to the State[54] and also acts of "private persons or entities empowered by the State itself to exercise functions proper to public authority" (art. 5), but cyberspace would force to reinterpret certain premises, because the division between private and governmental sphere may not be so clear in that environment. To the State are also attributed acts "organs of another State but which act, because they have been officially placed at its disposal, on the instructions of another" (art. 6) . [55]

It is particularly necessary in the field of cyberspace to state that certain individual actions may also be attributed to a State. For this, it is necessary that these individuals act on behalf of a State or under its direction and control (Article 8), or that they are compelled, in the absence of the competent authorities, to take charge of powers proper to the public authority (Article 9) and when they are acts, under certain conditions, of an insurrectional movement (Article 10)[56] . The possibility that the cyber-operations of non-State actors could be imputable to the State was expressly admitted by the Tallinn Group, which preferred (as the International Court of Justice and the International Law Commission itself have also done) the theory of *effective control*[57] to that of general control. Although the former (effective control) seems to continue to be the favorite[58] ,

---

54 According to article 4 of the ILC Draft *Articles on Responsibility of States for Internationally Wrongful Acts*, Report of the International Law Commission on the work of its fifty-third session (23 April-1 June and 2 July-10 August 2001, A/56/10, *Yearbook of the International Law Commission*, 2001, Vol. II, Part 2, pp. 20-153.

55 On the difficulties, no longer legal but technical of attribution (explained, moreover, with clarity), see TSAGOURIAS, N. and FARRELL, M., "Cyber attribution: technical and legal approaches and challenges", *European Journal of International Law*, vol 31, 3, 2020, pp. 941-967 (pp. 947-948). Also, on the types of attribution, SEGURA SERRANO, A., *El desafío de la ciberseguridad global,* Aranzadi, 2023, p. 32.

56 In this regard, GUTIÉRREZ ESPADA, C., *La responsabilidad internacional por el uso de la fuerza ..., op. cit.*, pp. 82-86, paras. 38-39 and, by the same author, *El hecho ilícito internacional*, Dykinson, Madrid, 2005 , pp. 79-105.

57 *The Tallinn Manual 2.0 ..., op. cit.,* pp. 96-97, comments 6 and 8. In particular, the Tallinn Group states (p. 96, rule 17, para. 6): "A State is in 'effective control' of a particular cyber operation by a non-State actor whenever it is the State that determines the execution and course of the specific operation and the cyber activity engaged in by the non-State actor is an integral part of that operation". The theory of general control, it should be recalled, was coined by the Criminal Tribunal for the former Yugoslavia and is applicable when a State equips, finances, coordinates or assists in the general plan of activities of an organized group, without giving specific instructions (*Appeal Judgment, Prosecutor v. Tadic*, case ICTY-94-I-A, Appeal Chamber, Judgment of 15 July 1999, para. 131).

58 GUTIÉRREZ ESPADA, C., *La responsabilidad internacional por el uso de la fuerza..., op. cit.,* pp. 85-86, paras. 38-39.

perhaps Spain could consider whether it would be advisable to adhere to it or, on the contrary, to adopt some formula (always depending on the specific case) closer to that of general control, mainly because of the technical difficulty that the process of attribution sometimes involves. .[59]

The decision to allocate is, however, an internal political decision. The European Parliament, in a resolution of 2022[60] , raised the possibility of adopting general rules for attribution (or a minimum frame of reference), but this was not the option finally chosen in the November 2024 document. Although minimum guidelines would be desirable, at least within some international organizations, States do not seem to be very willing to compromise on this point[61] , which is consistent with their traditional reticence when it comes to issues as closely linked to sovereignty as security. Another matter is, of course, the cooperation mechanisms that could be put in place between Member States to try to determine who has indeed been the perpetrator of a cyber-incident. The positions of the Member States also clearly state that attribution is a national decision (France[62] , Finland[63] , Germany[64] , Italy[65] and Estonia[66] , which does not preclude cases of attribution from two or more States (there is already, in fact, some precedent). [67]This sentiment is,

59 There are already some who defend it (TSAGOURIAS, N. and FARRELL, M., *op. cit*, p. 962).

60 Doc. P0_TA(2022)0064, March 9, 2022.

61 Indeed, in 2022 the Council stated, in the Conclusions on a Framework for a coordinated EU response *to* hybrid campaigns, that "attribution to a state or a non-state actor remains a sovereign political decision based on all-source intelligence and taken on a case-by-case basis, *Council Conclusions on a Framework for a coordinated EU response to hybrid campaigns*, *Press Release 603/22*, June 21, 2022, para. 17 (also para. 14).

62 *Droit international appliqué aux opérations dans le cyberspace*, 2019.

63 *International law and cyberspace.* https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727

64 Whose opinion on the attribution of a cyberoperation coincides almost entirely with that of the Tallinn Group (*On the application of...*, *op. cit.*).

65 Italian Position Paper on International Law and Cyberspace, 2021, available at https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

66 *Official compendium... op. cit.,* p. 28.

67 The first was that carried out jointly by the United Kingdom and the Netherlands after the attack on the Organization for the Prohibition of Chemical Weapons (see DELERUE, F., *Cyberoperations and International Law*, Cambridge University Press, Cambridge, 2020, pp. 178-181).

in fact, shared by States outside the European Union: Australia[68] , Israel[69] , Switzerland[70] and the United Kingdom .[71]

2. TOWARDS A BROAD CONCEPT OF

Among the circumstances precluding wrongfulness for which States have opted in their cyberspace positions are, above all, countermeasures and state of necessity. A Spanish position should expressly mention that the legal framework of reference for the application of countermeasures is that set by the International Law Commission's Draft Articles on International Responsibility of States, later confirmed by the International Court of Justice[72] : they must be responses to prior wrongful acts, have a non-punitive purpose (reversible, therefore), be notified in advance, proportional, their adoption is only possible by the State directly injured (except, it could be argued, in the case of the violation of collective norms or those affecting the international community as a whole[73]) and must be directed against the State that caused the act that triggered them.

The acceptance of countermeasures in cyberspace, with the requirements attached to them, has not given rise to major problems and several States have already confirmed their readiness to resort to them[74] . More controversial has been the possibility of allowing a third party, other than the State directly injured, to also apply them. In principle, the figure was not specifically designed for such cases, except in the circumstance provided for in Article 48 of the ILC Draft, which allows responsibility to be invoked also in the case of a breach of an obligation that "exists in relation to the international community as

---

68 "Australia will, in its sole discretion, and based on its own judgement, attribute unlawful cyber activities to another State", Annex B, *Australia's position on how international law applies to State conduct in cyberspace,* https://www.internationalcybertech.gov.au/our-work).

69 Https://digital-commons.usnwc.edu/ils/vol97/iss1/21/

70 Federal Department of Foreign Affairs, *Switzerland's position paper on the application of International Law in cyberspace*, May 2021, pp. 5-6.

71 That it further reserves the right to decide whether or not to make public such attribution, United Kingdom Foreign, Commonwealth, Development Office, *Application on International Law to States' conduct in cyberspace, UK Statement*, 3 June 2021.

72 Gabcikovo Nagymaros case, Judgment of 2 September 1997, *ICJ Reports 1997*, pp. 55-57. On countermeasures in cyberspace GUTIÉRREZ ESPADA, C., *La responsabilidad internacional por el uso de la fuerza ...*, *op. cit.,* pp. 131-137; by the same author, "La creciente necesidad de legislación contra las amenazas cibernéticas, fuentes de graves daños transnacionales", *Cuadernos de Derecho Transnacional*, vol. 14, 2, October 2022, pp. 10-46, pp. 30-37.

73 *See* Article 48 of the ILC Draft on International Responsibility of States

74 For example, Australia, Estonia, France, Germany, the Netherlands, the United Kingdom, New Zealand, Japan and the United States.

a whole" (*erga omnes*), an option, by the way, to which States are showing less and less resistance[75] . In the case of cyberspace, some States seem to go even further and give an even broader interpretation of the possibility for third States to take countermeasures when, for example, it is impossible to identify the perpetrator of the unlawful cyberoperation or in favor of third parties who so request (collective countermeasures)[76] . Would it be possible to force the letter in this direction and go beyond *erga omnes* obligations? The gamble is risky, no doubt, and the European Union itself, in its Common Position of November 2024, prefers to be cautious and not to affirm anything much beyond established customary law. However, in the section on attribution, it does expressly accept that, in the case of collective obligations, liability may be invoked by a State other than the injured State, so that it would be feasible to transfer this possibility to countermeasures[77]

At the moment, the number of States that openly accept the possibility is too limited to speak of a change of trend, but this could, why not, change, especially in a volatile environment such as cyberspace. Spain, in any case, should at least expressly admit, in line with what the EU already seems to be very clear, that countermeasures by States not directly injured are perfectly possible in case of violation of *erga omnes* obligations. The nature of cyberspace, where actions may end up having consequences for other States that may not be the direct target of the cyberattack, seems to make it

75 See PIERNAS LÓPEZ. J. J., *El Derecho internacional ...., op. cit*., pp. 103-107 and, by the same author, "Las medidas de autotutela frente a amenazas cibernéticas en derecho internacional. Especial referencia a la posible adopción de contramedidas colectivas", *Cuadernos de Derecho Transnacional,* vol 16, 1, 2024, pp. 10-35.

76 *Ad. ex*., Estonia: "Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation" (*Opening address (President of Estonia) at the 11th International Conference on Cyber Conflict (CyCon) in Tallinn*, 29 May 2019, https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon). Also New Zealand: "New Zealand is open to the proposition that victim states, in limited circumstances, may request assistance from other states in applying proportionate countermeasures to induce compliance ..." (*The application to International Law to State activity in Cyberspace..., op. cit.*). On the rigidity of countermeasures in cyberspace, SCHMITT, M., "Below the threshold ..., *op. cit.*, p. 73 and, also on collective countermeasures, JACKSON, M. and PADDEU, F. I., "The countermeasures of others: when can States collaborate in the taking of countermeasures?", *AJIL*, vol. 118, 2, April 2024, pp. 231-274 .

77 P. 11. The EU External Action Service (European External Action Service (Council of the European Union [General Secretariat]),*Third-party Countermeasures under International Law (Revised paper),* Brussels, 17 November 2022, WK 15858/2022 INIT, LIMITE, COJUR, pp. 1-33, pp. 19-33, letters C-E), which did address countermeasures directly, openly admitting them in the case of *erga omnes* obligations and even not closing itself completely to cases beyond these.

advisable to do so. Admitting them, moreover, in other cases, when requested by the injured State would be a risk, but why not? Some have already done so....

In any case, adopting countermeasures seems to be the natural way out in many situations and the options are varied: although in principle it might be more logical for such a response to be also in the cyberspace domain (e.g. a cyber response operation to disable a program that is manipulating election results or directed against cyberinfrastructures other than those directly involved in the hostile operation)[78] , nothing would prevent it from also being an *analog* response. The Common Position of the European Union accepts this.

3. THE STATE OF NECESSITY AS AN ALTERNATIVE

The state of necessity, another circumstance of exclusion of wrongfulness according to article 25 of the Draft Articles of the International Law Commission, would make the wrongfulness disappear when it is a question of reacting to a grave and imminent peril essential to the interests of a State. Moreover, the act the wrongfulness of which is sought to be precluded must not seriously affect an essential interest of the State or States towards which the obligation exists, or of the international community as a whole. Nor could necessity be invoked if the international obligation in question excludes such a possibility or if the State has in any way contributed to the creation of such a state of necessity.

Such requirements would force a careful examination of each case, but even so, this ground of exclusion of wrongfulness has gained ground in many positions on cyberspace for two reasons. First, because it could be invoked in cases where countermeasures - for example, because a state is not directly injured (or there is no obligation *erga omnes* to invoke them) - would not be feasible. Secondly, and above all (in fact, this is the key to the fact that more and more States are including it) because it

[78] SCHMITT, M. N., "Foreign cyber interference in elections: an international law Primer, Part III", *EJIL Talk*, 19 October 2020.

will be possible to invoke it in any other case in which the action not could be attributed to a specific State[79] , which is more likely in cyberspace than in the analog world.

The State affected by the cyber-operation would have, with the state of necessity, another option to react, yes, but we must not forget that the requirements that this figure demands are not few. For the time being, only a limited number of States have expressly included it (far fewer than those that do mention countermeasures), but most of them are European: Czech Republic, France, Germany, Japan, Netherlands, Norway, Sweden and Switzerland[80] . The EU has also chosen to mention it expressly in a paragraph (the last one, by the way, of its Declaration on a Common Position on Cyberspace), so perhaps it would not be superfluous for Spain to do so as well. The most problematic question would be to elucidate when there is an *essential danger* to the State that justifies recourse to the State of necessity. The EU's position is that an attack on an infrastructure relevant to the State would be a clear case . [81]

V. THE GREAT CONTROVERSIES

1. USE OF FORCE, ARMED ATTACK AND SELF-DEFENSE

One of the essential aspects of a position on cyberspace must be how the prohibition of the use of force in this environment is to be conceived. The obligatory reference would be, of course, Article 2.4 of the Charter, but if the use of force in the traditional (analogical) sense is already a debated issue, new elements arise when it is taken to the cyberspace environment. It would be useful to include them in order to have an exact idea of how the State is going to deal with them.

79 SPÁČIL, J., "Legal key to protection against unattributable cyber operations", *Masaryk University Journal of Law and Technology*, vol.16, 2, 2022, pp. 215-239, p. 234. See also LAHMANN, H. "The plea of necessity in cyber emergencies: unresolved doctrinal questions", *Nordic Journal of International Law, vol.* 92, 3, 2023, pp. 422-445.

80 Czech Republic: "Position paper on the application of international law in cyberspace", p. 16; France: Droit international..., *op. cit*, p. 8; Germany: " On the Application of International Law in Cyberspace , Position Paper", pp. 14-15; Japan: "Basic Position of the Government of Japan on International Law Applicable to Cyber Operations", p. 5; Netherlands: "International law in cyberspace", pp. 7-8; Sweden: *op. cit.*, p. 6 and Switzerland: " Switzerland's position paper on the application of international law in cyberspace ", p. 7.

81 P. 12 of the Declaration on a Common Position on Cyberspace.

Assuming that, as the International Court of Justice has stated, the definition of attack does not depend on the weapon used[82] , using the digital route to carry it out would be possible, but some things would have to be nuanced. Probably the greatest difficulty would be to determine the dividing line between what constitutes what would be a minor use of force and one that, by its very nature, could be qualified as an "armed (cyber)attack". The logical solution would be to bring to this new environment the reference to the definition of aggression included in resolution 3314 (1974) and, more particularly, the "scale and effects" parameter[83] traditionally used to mark that line[84] . Thus, a reference should be included to the effect that a cyber operation should be considered a use of force when its scale and effects are comparable to operations outside cyberspace that can be considered uses of force per se. And, if such a use of force could be equated to an armed attack, the right of self-defense could then be triggered in cyberspace as well. It seems clear that any cyber-operation that seriously injures or kills people or causes significant damage or destruction of property would meet the requirements of scale and effects in terms of armed attack, but other actions such as brief or periodic interruptions of non-essential services are more contentious. *A priori*, they would not be considered as an armed attack (and therefore legitimate self-defense),[85] but... what about cyber operations that do cause significant effects on, for example, critical infrastructures, that generate serious socioeconomic consequences and end up leading to situations of particular gravity and even causing indirect or deferred damage to people and property? Some States (few as yet) are beginning to open up to this possibility[86] . France, for example, considers that self-defense could also be activated in

---

82 Advisory Opinion on the Legality of the Threat or Use of Force*, ICJ Reports 1996,* para. 39.

83 Case concerning Military and Paramilitary Activities in and against Nicaragua, Judgment of 27 June 1986*, ICJ Reports 1986*, para. 195.

84 Which, in fact, is expressly accepted, for example, by the Tallinn Manual (*Tallinn Manual 2.0 ..., op. cit.,* p. 339, rule 71*).*

85 See, among others, ROSCINI, M. *Cyber operations and the use of force in International Law*, Oxford University Press, Oxford, 2014, pp. 73-77. See also BERMEJO GARCÍA, R. and LÓPEZ-JACOÍSTE DÍAZ, E., *La ciberseguridad a la luz del Jus ad Bellum y del Jus in Bello*, Eunsa, Pamplona, 2020, pp. 65-77 and GUTIÉRREZ ESPADA, C., *La responsabilidad internacional..., op. cit.*, pp. 51-63.

86 The United States, for its part, reserves the right to respond in self-defense against *any* use of force, whatever the entity (as it does, it must be said, in the analogical setting): "...the United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response" (https://2009-2017.state.gov/s/l/releases/remarks/197924.htm). Also NATO, in the 2022 Strategic Concept, stated that "a single or cumulative set of malicious cyber activities or hostile operations to, from or within space could rise to the level of an armed attack" (*NATO Strategic Concept*, 2022, para. 25).

cases of considerable economic damage[87] and similar positions are defended by Finland[88] or Norway[89] . The Declaration on an EU Common Position of November 2024, however, does not expressly do so, although it does state that the combined effects of several cyber operations, taken as a whole, could be considered a use of force if they were comparable to a kinetic use of force.

The truth is that this is still somewhat unexplored terrain, because to date most major cyber operations have been accompanied by conventional-type actions, but a position should at least leave the door open to the possibility of leaving some room for interpretation of the concept of use of force and armed attack. The formula "case-by-case analysis" would again be useful in this area. Obviously, in the case of self-defense, the traditional requirements of necessity, proportionality and referral to the Security Council would be equally applicable and as such should be expressly included. It would not even be superfluous to include a reference to the fact that in the case of an armed attack carried out via cyberspace, the response could also be analogous (again, respecting proportionality).

It would also be appropriate to take this opportunity to clarify Spain's views on some general issues of self-defense and some of the most debated in recent times. In the first place, the possibility of invoking self-defense against an attack in cyberspace when it comes from non-state actors could be expressly recognized (something particularly convenient and frequent, I would say, in this environment) and, of course, to clarify that self-defense would also operate on imminent armed attacks, something that in cyberspace seems totally logical.

2. HOW TO APPLY INTERNATIONAL HUMANITARIAN LAW

The rules of international humanitarian law also apply in cyberspace. The Tallinn Manual accepts this, but how to interpret some of them has given rise to more than one discussion. For example, in 2017, the Group then working on the issue at the United Nations did not adopt the final report because of the opposition of China, Russia and Cuba to, among other issues, admitting the application of International Humanitarian Law,

87 *Droit international apliqué ..., op. cit.*, p. 9, 2019.
88 *International law and cyberspace. Finland's national positions*, *op. cit.*
89 *Official compendium ..., op. cit.*, p. 70.

which according to them "would legitimize a scenario of war and military actions in space"[90] . Be that as it may, in general, the States have accepted in their positions its application to cyberspace, but the dissensions have come at the time of determining how it was done.

The definition of "attack" in the sense of Article 49.1 of Additional Protocol I to the Geneva Conventions ("acts of violence against the adversary, whether offensive or defensive") would probably be the first question to be determined, to see whether it is feasible to apply the rules governing hostilities. The doubts would be raised, above all, by how to qualify operations that do not involve a direct and/or physical attack against an infrastructure, but that do involve damage to essential services and that could, therefore, give rise to acts of violence or have a serious impact on the loss of functionality of some infrastructure or facility that could have a particular impact on the civilian population. The logical rule would be to require that the consequences be comparable to those that occur in the analogical sphere and, in addition, in doubtful cases, to resort once again to the inclusion of the "case-by-case" formula.

The basic principles of International Humanitarian Law, such as humanity, military necessity, distinction, precaution and proportionality would, of course, be applicable in cyberspace.

Another particularly problematic issue has been the distinction between civilians and combatants, which is essential to protect the former (civilians cannot be the object of attack) and, in the case of the latter, to apply the status of war . [91]

Dual-use goods, military and civilian, are particularly difficult to distinguish in cyberspace, so perhaps some clarification should also be made in this regard in the sense

---

90 Russia, for example, has continued to insist on the idea. In March 2023 it stated the following: "(...) there are no grounds for assessing the legality of the use of ICTs from the IHL perspective. Under these circumstances, it is inadmissible to speak about automatic applicability of the existing norms of IHL to the field of information security without taking into account its specifics and adapting these norms accordingly" (Statement by the representative of the Russian Federation at the fourth session of the UN Open-Ended Working Group on security of and in the use of icts 2021-2025, New York, 7 March 2023).

91 On the question, VÁZQUEZ SERRANO, I., "Rusia-Ucrania: ¿la primera ciberguerra global?", in BOLLO AROCENA, M. D. and JIMÉNEZ PINEDA, E., *El Derecho internacional y europeo contemporáneos ante la agresión rusa a Ucrania*, Tirant lo Blanch, 2024, pp. 213-241. Also, GILL, T. D. "International humanitarian law applied to cyber-warfare: precaution, proportionality and the notion of attack under the humanitarian law of armed conflict" in TSAGOURIAS, N. and BUCHARN, R., *Research Handbook on International Law and Cyberspace*, Elgar, 2021, pp. 457-470 .

that the criteria valid for the analog environment would also be valid in cyberspace. What about data? If they are of a civilian nature, they are protected because they cannot be subject to attacks, but in the case of cyberspace the problem that arises is that the *physical* destruction of these data does not always exist (data hosted in the cloud), so there are already voices, especially the ICRC, which argues that the protection of these civilian assets should be extreme, whether they have physical or electronic support. The conclusion seems absolutely necessary in a world so dependent on this type of non-physical data.

As for the States, with a few exceptions (Ireland or the Czech Republic[92]), few of them qualify or specify how to apply the rules of International Humanitarian Law. At most, the more daring ones openly declare that cyber operations must be in accordance with its principles and rules. The EU's position, although it devotes three paragraphs of some length to the issue, is basically limited to treading on familiar ground, surely knowing and aware that this is still one of the issues on which States continue to argue. However, it has not hesitated to strongly support the fact that international humanitarian law does indeed apply to cyberspace (probably to counter the opinion of those who are not very much in favor of it). This is what its representative to the UN OEWG did at the December 2024 session, in which, in addition to insisting that the group's final report (which, let's remember, will finish its work in 2025) should include the application of international humanitarian law to cyberspace, he stated:

> "Here, I would like to reiterate, and underscore, that recognising the applicability of international humanitarian law to cyberspace does not lead to or encourage the militarization of cyberspace, nor does it legitimmise cyber warfare."[93]

3. HUMAN RIGHTS AND THEIR DELICATE SITUATION IN CYBERSPACE

The Human Rights Council affirmed, quite some time ago, that human rights apply both *online* and *offline*[94] . Also the 2015 Report of the Group of Governmental Experts on Developments on Information and Telecommunications in the Context of

92 Czech Republic: "Position paper..", *op. cit*., p. 10.

93 Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025, Ninth Substantive Session, 2 - 6 December 2024, Key EU messages for Agenda item: International Law, para. 6. In fact, it insisted and developed this idea in paragraphs 11-13.

94 Resolution A/HRC/RES/20/8 of 16 July 2012.

International Security, within its Eleven Non-Binding Principles and Norms (section e) reaffirmed the need to protect human rights on the Internet, making express mention of freedom of expression[95] . But, as was the case with international humanitarian law issues, it has been their application to specific problems that has become the great workhorse within the United Nations OEWG.

A Spanish position on cyberspace should make it clear that rights such as freedom of expression, the right to privacy, the right to information, free association or the prohibition of discrimination must be guaranteed in a special way in that environment, precisely because they are much more vulnerable there. It should also state which basic human rights treaties bind Spain, mentioning, in addition to applicable customary law, the basic United Nations human rights treaties to which it is a party (International Covenant on Civil and Political Rights, International Covenant on Economic, Social and Cultural Rights, etc.), including those of a regional nature (European Convention on Human Rights or the European Social Charter, for example).

Similarly, perhaps it would be advisable to imitate other positions that have expressly stated that they support the promotion of a *free, open and secure* cyberspace[96] , since it is not in vain that this is already recognized in the National Cybersecurity Strategy (*see* section II *above*). China, for example, arrogates to itself considerable prerogatives in the control of cyberspace, which leave little room for the exercise of certain human rights[97] and Russia is also quite restrictive in this regard[98] . In fact, in August 2024, a controversial draft Convention against cybercrime[99] , which originated

---

95 "States, in ensuring the safe use of ICTs, should respect Human Rights Council Resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly Resolutions 68/167 and 69/166 on the right to privacy in the digital age, to ensure full respect for human rights, including the right to freedom of expression," 2015 Report of the Group of Governmental Experts on Developments in Information and Telecommunications in the Context of International Security, *op. cit.*

96 See, among the most recent, the position of Austria, for example (p. 12), the Czech Republic, *op. cit.*, pp. 12-13 or the African Union, *op. cit.*, pp. 9-10. Other states advocating this are Sweden, *op. cit*., pp. 5-6) or the United Kingdom (Application of international law to states' conduct in cyberspace: UK statement, 3 June 2021).

97 China's Views on the "Application of the Principle of Sovereignty in Cyberspace, Ministry of Foreign Affairs of the People's Republic of China, p 3. In this regard, KULAGA, L., "Mapping the position of States on the application of sovereignty in cyberspace", *Polish Review of International and European Law*, 2024, vol 13, 1, pp. 65-87 , pp. 70-71.

98 Federal Law No. 90-FZ, dated May 01, 2019.

99 The text, in doc. A/AC.291/L.15 of 7 August 2024 of the Ad Hoc Committee on the Elaboration of a Comprehensive International Convention on Combating the Use of Information and Communication Technologies for Criminal Purposes (Draft United Nations Convention against Cybercrime Strengthening international cooperation in combating certain crimes committed

from a Russian initiative started in 2019, was approved at the United Nations. The whole process was closely watched by several States and human rights associations, which feared the inclusion of significant restrictions on the exercise of human rights. The EU, in fact, after refusing the proposal, claiming that there was already a convention (the Budapest Convention) regulating the issue, chose to get involved to at least try to control and modulate the content[100] . The final draft of the Convention was adopted in August 2024.[101]

Nor would it be out of place, precisely because it is also a controversial issue in certain States (in a minority, of course, the most representative being the United States and Israel), to affirm the extraterritorial application of human rights[102] , stating in some way that the protection of human rights is effective in the territory of a State and in the areas under its jurisdiction, but also in those situations in which it exercises effective control or in which it otherwise has some power over the individuals of a territory. It is true, however, that this is not a common assertion in states' positions on cyberspace[103] and, in fact, that of the European Union is rather sparing in this regard, limiting itself to stating that states have an obligation to protect the rights "of individuals within their jurisdiction".

VI. CONCLUSIONS

through information and communication technology systems and in the transmission of evidence in electronic form of serious crime)

100 Without going any further, the European Data Protection Agency was already warning about the content of the convention in 2022 (https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/new-united-nations-convention-cybercrime_en). However, it continues to state publicly that, although it agrees with the final version, it will closely monitor its implementation and application (EU Explanation of Position - UN General Assembly 3rd Committee: Adoption of the United Nations Convention against Cybercrime, 11 November 2024, https://www.eeas.europa.eu/delegations/un-new-york/eu-explanation-position-un-general-assembly-3rd-committee-adoption-united-nations-convention-against_en).

101 Doc. A/AC.291/L.15, 7 August 2024

102 This obligation is expressly stated in Article 2.1 of the International Covenant on Civil and Political Rights. It is true, however, that it is a subject whose profiles have not yet been fully delimited. On the issue in cyberspace, McDERMOTT, H., "Application of the International Human Rights Law Framework in Cyber Space", in AKANDE, D.; KUOSMANEN, J.; MCDERMOTT, H and ROSER, D., *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment*, Oxford University Press, 2020, pp. 190-210. Also, FIDLER, D. P. "Cyberspace and human rights", in TSAGOURIAS, N. and BUCHARN, R., *Research Handbook on International Law and Cyberspace*, Elgar, 2021, pp. 130-151 .

103 Switzerland is the only exception, since it does expressly so (Switzerland's position paper on the application of international law ..., *op. cit.,* p. 8).

States' positions on cyberspace have become an ideal way of finding out in detail and precisely which rules of international law apply and, more importantly, how they will be applied. It is true that some of them are formulated in too general a manner, especially in areas where discussions are still ongoing, but for the time being they seem to be the best way to take the pulse of States. Let us not forget, moreover, that knowing how they think and, in particular, what they consider to be a genuine legal obligation in cyberspace is important for determining the *opinio iuris* on a subject that still remains partly in the shadows.

Spain, as a middle power among the fifteen most developed economies, should have its own position on international law and cyberspace. It could be thought that the urgency does not exist, once the EU approves its own Common Position on cyberspace (November 2024), but beyond the fact that it agrees with everything that is contained in it, a position of its own would be a unique opportunity for our Government to clarify issues still in doubt or, even better and since we are speaking from the realm of the purely hypothetical, to take a step forward in others regarding which some States still do not dare to do so.

According to what has been gathered in this chapter, some elements that would not be superfluous to include would be an express mention of sovereignty as a norm, opting for flexible interpretations of the principle of non-intervention that would allow for those operations of interference or manipulation that are of such concern to today's society (in the European Union, precisely as this is being written, the scandal over the suspension by the Constitutional Court of the elections in Romania, after it was proven that voters were influenced by means of social networks, is still resounding) or due diligence, the scandal over the suspension by the Constitutional Court of the elections in Romania, after it was proven that voters were influenced by social networks, is still resounding) or due diligence as an obligation, to demand responsible behavior from other States but also to be coherent with what is happening in one's own.

Another necessary mention would be to make it clear that conduct in cyberspace generates the responsibility of States and that countermeasures or the state of necessity can be perfectly legitimate responses. And, why not, Spain could expressly pronounce itself on the so-called collective countermeasures that some States (few for the time being, of course) are already expressly accepting.

Resorting to the formula that each problem will ultimately be determined on *a case-by-case basis* is always a good option for our State to have a certain freedom of action. In an environment such as cyberspace, moreover, where changes are rapid, it seems the most convenient option if we want to avoid official positions that are soon outdated.

And while we are at it, allow me to suggest that Spain should not be shy about committing itself to the protection of human beings in cyberspace. Defending the basic rules and principles of international humanitarian law is not, as some states claim, to militarize it, but to recognize a reality that recent armed conflicts have already shown. And the same could be said of human rights: the temptations to curtail certain fundamental freedoms are many, but precisely for this reason the guarantees offered must be particularly careful or cyberspace will irretrievably lose the essence of what it once was: that free environment that allowed human beings to escape the constraints of the analog world. Controls will be necessary, of course, and this is already being done (the European Union's extensive regulations in this regard, or even the United Nations Convention on Cybercrime, are two good examples), but always seeking the necessary balance between freedom and abuse. Is that too much to ask? Perhaps, but that is our job as jurists and as such we should not miss any opportunity to defend it.

Bibliography

BERMEJO GARCÍA, R. and LÓPEZ-JACOÍSTE DÍAZ, E., *La ciberseguridad a la luz del jus ad bellum y del jus in bello*, Eunsa, Pamplona, 2020.

CERVELL HORTAL, Mª. J, "Ciberinjerencias en procesos electorales y principio de no intervención (una perspectiva internacional y europea)", *Revista Electrónica de Estudios Internacionales*, vol. 45, June 2023, pp. 1-3 3.

ID., "Sovereignty and cyberspace: should the rules of the game change?", *Seguridad y responsabilidad penal internacional en el uso de las TIC y la inteligencia artificial*, Iustel, 2024, pp. 65-80.

ID., "Un soft law para el ciberespacio? (De las normas no vinculantes y otras iniciativas", Marcial Pons, 2025, in press.

DELERUE, F., "Toward and EU position on the application of International Law in cyberspace", Briefing Paper, EU Cyber Direct, available at https://eucyberdirect.eu/research/toward-an-eu-position-on-the-application-of-international-law-in-cyberspace.

ID, *Cyberoperations and International Law*, Cambridge University Press, Cambridge, 2020, pp. 178-181.

FIDLER, D. P. "Cyberspace and human rights", in Tsagourias, N. and Bucharn, R., *Research Handbook on International Law and Cyberspace*, Elgar, 2021, pp. 130-151.

GAVRILLA, A., "Ukraine's Great Cyberwar That Didn't Happen," *Opinion Paper 99/2022*, IEES, November 10, 2022.

GILL, T. D. "International humanitarian law applied to cyber-warfare: precaution, proportionality and the notion of attack under the humanitarian law of armed conflict" in Tsagourias, N. and Bucharn, R., *Research Handbook on International Law and Cyberspace*, Elgar, 2021, pp. 457-470.

GUTIÉRREZ ESPADA, C *El hecho ilícito internacional*, Dykinson, Madrid, 2005.

ID., *La responsabilidad internacional por el uso de la fuerza en el ciberespacio*, Aranzadi, Cizur Menor, 2020.

JACKSON, M. and PADDEU, F. I., "The countermeasures of others: when can States collaborate in the taking of countermeasures?", *AJIL*, vol. 118, 2, April 2024, pp. 231-274.

KAJANDER, A., A tale of two draft resolutions: a report on the polarising International Law discussions at the 2023 OEWG substantive sessions", 2023, p. 10, available at https://ccdcoe.org/uploads/2023/12/Kajander-OEWGSummaryExportFinalL.pdf.

KULAGA, L., "Mapping the position of States on the application of soveregnty in cyberspace", *Polish Review of International and European Law*, 2024, vol 13, 1, pp. 65-87.

LAHMANN, H. "The plea of necessity in cyber emergencies: unresolved doctrinal questions", *Nordic Journal of International Law, vol.* 92, 3, 2023, pp. 422-445.

McDERMOTT, H., "Application of the International Human Rights Law Framework in Cyber Space", in Akande, D.; Kuosmanen, J.; McDerm,ott, H and Roser, D., *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment*, Oxford University Press, 2020, pp. 190-210.

MOYNIHAN, H., "The application of international law to state cyberattacks. Sovereignty and non-intervention", *Research Paper, Chatham House*, December 2019.

OSULA, A. M.; KASPER, A., KAJANDER, A., *EU Common Position on International Law and Cyberspace", Masaryk University Journal of Law and Technology,* vol 16, 1, 2022, pp. 89-121.

PAVLOVA, P., "A calm before the storm?", *Cyber Digital Europe blog*, 2 August 2024, https://directionsblog.eu/a-calm-before-the-storm.

PÉREZ-PRAT DURBÁN, L., "Los ciberataques y el uso de la fuerza en las relaciones internacionales", in Millán Moro, L. (dir.) and Fernández Arribas, G. (coord.), *Ciberataques y ciberseguridad en la escena internacional*, Aranzadi, Cizur Menor, 2019, pp. 17-50.

PIERNAS LÓPEZ, J. J., "Las medidas de autotutela frente a amenazas cibernéticas en derecho internacional. Especial referencia a la posible adopción de contramedidas colectivas", *Cuadernos de Derecho Transnacional,* vol 16, 1, 2024, pp. 10-35.

ID, "The international law principle of due diligence and its application to the cyber context," *Annals of Law*, vol. 41, 2024, pp. 52-59.

ID, El *Derecho internacional y las contramedidas cibernéticas*, Aranzadi, 2024.

PONTA, A., "Responsible State behaviour in cyberspace: two new reports from parallel UN processes", *ASIL Insights*, vol 25, 14, 20 July 2021.

ROSCINI, M. *Cyber operations and the use of force in International Law*, Oxford University Press, Oxford, 2014.

SCHMITT, M. N. & VIHUL, L., 'European Approaches to the Application of International Law in Cyberspace: A Comparative Legal Analysis Policy brief', EU Cyber Direct, July 2024, pp. 1-91.

SCHMITT, M. (ed.), *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, Cambridge University Press, Cambridge, 2017.

ID, "Foreign cyber interference in elections: an international law Primer, Part III", *EJIL Talk*, 19 October 2020.

ID, "Below the threshold cyberoperations: the countermeasures response option and International Law", *Virginia Journal of International Law*, vol 54, 3, 2014.

ID, "In Defense of Due Diligence in Cyberspace," *The Yale Law Journal Forum*, vol. 125, 2015, pp. 68-81.

ID, "The United Kingdom on International Law in cyberspace", *EJIL Talk*, 24 May 2022.

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

SPÁČIL, J., "Legal key to protection against unattributable cyber operations", *Masaryk University Journal of Law and Technology*, vol.16, 2, 2022, pp. 215-239.

TSAGOURIAS, N. and FARRELL, M., "Cyber attribution: technical and legal approaches and challenges", *European Journal of International Law*, vol 31, 3, 2020, pp. 941-967.

VÁZQUEZ SERRANO, I.: "Rusia-Ucrania: ¿la primera ciberguerra global?", in Bollo Arocena, Mª. D. and Jiménez Pineda, E., *El Derecho internacional y europeo contemporáneos ante la agresión rusa a Ucrania*, Tirant lo Blanch, 2024, pp. 213-241.

Regional Approaches to Cybersecurity: Africa and Latin America and the Caribbean

Eugenia LÓPEZ-JACOISTE DÍAZ
Professor of International Law and International Relations.
University of Navarra

I. INTRODUCTION N

Cybersecurity can be defined as the set of tools, policies, guidelines, and best practices in the context of information and communication technologies (ICTs) aimed at protecting a state's cyberspace and all its users. Improving cybersecurity should be a priority for States and the international community as a whole, despite the lack of specific international legal regulation in this area.

The only two existing international treaties related to cyberspace are the Council of Europe's 2001 Budapest Convention on Cybercrime[1] , and the 2014 African Union Convention on Cyber Security and Personal Data Protection[2] . These regional instruments specifically address the issue on cyber operations conducted by, or against States. However, the draft UN cybercrime treaty has not yet reached the necessary consensus to become a universally binding standard, as its scope, key definitions and specific

1 Council of Europe, Budapest Convention on Cybercrime, ETS No. 185, in force since January 7, 2004.

2 African Union Convention on Cyber Security and Personal Data Protection, adopted on June 27, 2014.

safeguards necessary to protect the human rights of victims of cybercrime are still in question .[3]

On the other hand, there are specialized studies such as the *Tallinn Manual* on *International Law Applicable to Cyberwarfare*[4] , now in its third revision and update[5] , which reaffirms that the general principles of international law apply to cyberspace and identified 95 rules applicable to this "fifth space". The *Tallinn Manual* provides relevant commentary on cyberspace and sovereignty, state responsibility, *jus ad bellum,* international humanitarian law and the laws of neutrality as they relate to cyberwarfare. This *Handbook* is therefore the international framework of reference for cybersecurity, without prejudice to the intergovernmental processes sponsored by the United Nations, such as the reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[6] ; the resolutions of the General Assembly[7] or the reports of the UN Open-ended Working Group . [8]

The international approach to cybersecurity has attracted a great deal of academic interest[9] , while regional approaches - particularly African and Latin American - seem to

---

3 The Ad Hoc Committee on the Elaboration of a Comprehensive International Convention on Combating the Use of Information and Communication Technologies for Criminal Purposes has resumed its 2024 session, although it has only reached some compromises on certain aspects**.** *Cf.* A/78/986-A/AC.291/28 of 19 August 2024, Report of the Ad Hoc Committee on the Elaboration of a Comprehensive International Convention on Combating the Use of Information and Communication Technologies for Criminal Purposes on the resumption of its closing session.

4 SCHMITT, M. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.

5 Indeed, in 2021, the North Atlantic Treaty Organization Cooperative Cyber Defense Center of Excellence (CCDCOE), which is an international military organization based in Tallinn, launched a five-year project for the realization of the future Tallinn Manual 3.0 that will revise some of the existing chapters and explore new topics of importance to states.

6 U.N. Secretary-General, *Report of the Group of Governmental Experts on Promoting Responsible State Behavior in Cyberspace in the Context of International Security,* U.N. Doc. A/76/135 (July 14, 2021); Report *of the Group of Governmental Experts on Developments in Information and Telecommunications in the Context of International Security*, 19, U.N. Doc. A/68/98 (June 24, 2013); *Report of the Group of Governmental Experts on Advances in Information and Telecommunications in the Context of International Security*, 10, U.N. Doc. A/70/174 (July 22, 2015).

7 United Nations General Assembly, Resolution A/ RES/ 75/240 "Advances in the field of information and telecommunications in the context of international security," adopted December 31, 2020; Resolution A/RES/73/27, "Advances in the field of information and telecommunications in the context of international security," December 5, 2018; Resolution A/RES/73/266, "Promoting responsible behaviour of States in cyberspace in the context of international security," December 22, 2018.

8 United Nations General Assembly, *Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security,* A/AC.290/202/CRP.2, 10 March 2021.

9 *Cfr.,* among many others, CERVELL HORTAL, M.J. and PIERNAS LÓPEZ, J. J. (dirs), *Hacia una regulación internacional de para el ciberespacio*, Thomson-Aranzadi, Pamplona, 2023; VAN DER

have been relegated to the background, despite the fact that the particular needs and conditions of each region are not necessarily identical to international cybersecurity concerns. While it is true that cybersecurity is just another facet of international security, some governments sometimes see the development of cybersecurity policies and standards as an opportunity to extend or consolidate their power, to punish new forms of criminality, but without tackling the vulnerability of networks at the root, or even to extend their political influence in third countries.

In recent years, Africa and Latin America and the Caribbean have pushed forward with determination to build their own cybersecurity through international cooperation by means of strategies, policies and national legislation both to detect and mitigate cyber intrusions and the effects of cyber operations (passive cyber defense), and also to act proactively against malicious cyber operations in order to mitigate or stop their harmful effects (active cybersecurity)

In this context, this chapter aims to analyze regional approaches to cybersecurity in Africa and Latin America and the Caribbean. The African Union (AU) and the Organization of American States (OAS) are promoting studies and concrete actions on cybersecurity in their respective regions, reflecting the challenges and particularities of their peoples. However, given the political, social, economic and legal divergences between these two regions, it is necessary to analyze them individually, although under the same questions. First, we must analyze to what extent the member states of the AU and the OAS understand the norms and principles of international law to be applicable to cyberspace in their international relations. Second, what is the degree of cybersecurity maturity achieved by the states of both regions with their respective national cybersecurity strategies. And third, what are the particularities and strengths of both regional systems.

II. APPROACHES TO CYBERSECURITY IN AFRICA

BERG, B., *Governing cyberspace: behavior, power and diplomacy*, Lanham; Boulder; New York; London: Rowman & Littlefield, 2020; ENEKEN, T; MIKA, K., *Routledge Handbook of International Cybersecurity*, Routledge, 2020; GIACOMELLO, G, (ed.) *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals*. New York: Bloomsbury Academic, 2014; TSAGOURIAS, N. and BUCHAN, R. (eds.), *Research Handbook on International Law and Cyberspace,* Edward Elgar Publishing, UK 2021; HELLER, K.J., "In Defense of Pure Sovereignty in Cyberspace," *International Law Studies,* vol. 97, 2021, pp. 1432-1499.

The Internet penetration rate in Africa is relatively high compared to global rates[10] . Many governments in Africa are adopting digitization measures thanks to international cooperation - from the European Union and China in particular - so that citizens have access to digital tools and their economies can benefit from a continuously evolving, yet secure and open digital environment. Accordingly, the African Union adopted the *National Digital Transformation Strategy for Africa* (2020-2030)[11] , which aims to provide internet connectivity to all African citizens by 2030 and foster inclusive digital and personal skills in various fields such as, for example, encryption, programming, security, *blockchain* and machine learning tools or artificial intelligence. It includes the "Policy and Regulatory Initiative for Digital Africa (PRIDA)", which is carried out in collaboration with the European Union and the International Telecommunication Union and aims, among others, to harmonize ICT regulatory frameworks and enhance the capacity of African stakeholders to participate in global Internet governance forums.

It should be noted, however, that until relatively recently, African states were not major targets of hostile cyber operations, nor were they at the forefront of operators engaging in such behavior. However, in the last two years, *ransomware* attacks against critical infrastructure have increased significantly in the region, although online scams remain the most common form of digital crime against individuals and businesses, which have already reached large volumes and financial implications. To cite a few examples, Ghana's largest electricity trader, the Electricity Company of Ghana (ECG), suffered several *ransomware* attacks in 2023*;* but also national banks in Zambia and South Sudan; government institutions in Ethiopia, Senegal and Zimbabwe and the South African Internet service provider RSAWEB. Even the African Union faced a crippling attack by the BlackCat group (also known as ALPHV) against its intranet in 2023, which Interpol and its partners were able to mitigate[12] . According to Interpol this reality manifests the rapid evolution and expansion of cyber threat actors and their *modus operandi*, which

---

10 According to INTERPOL, the average social media penetration in the African region is approximately 27%, with a higher proportion of active social media users in the North and Southern African regions (56% and 45% respectively). In *Report on Assessing Cyber Threats in Africa. Overview of cyber threat trends, by the office of cybercrime operations in the African region,* March 2023, p. 10.

11 *Cf. The Digital Transformation Strategy for Africa* (2020-2030) at https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf.

12 *Cf.*, *Le Monde, "Vent de panique à l'Union africaine après une nouvelle cyberattaque"* (2023): https:.

with a high degree of sophistication exploit social networks, the use of artificial intelligence and advanced techniques in social engineering .[13]

Given this reality, it is understandable that, from a political perspective, African states advocate an open, peaceful and secure cyberspace for their young population and growing economies. And that - from a legal perspective - African institutions aspire to adopt rules and mechanisms for protection against foreign cyber operations, which infringe on their national interests, but also how to deal with cyber operations that are channeled through networks on their territory and all while preserving the inviolability of the fundamental principles of international law to safeguard their sovereignty and inviolability.

1. THE APPLICABILITY OF INTERNATIONAL LAW TO CYBERSPACE, ACCORDING TO THE AFRICAN UNION

The African Union's determined commitment to establishing binding cybersecurity standards that harmonize the rules applicable to cyberspace in the region is manifested in a number of concrete acts. In 2014, African Convention on Cybersecurity and Personal Data Protection[14] was adopted, which provides a legal framework for national legislations to be able to adequately combat cybercrimes of a cross-border nature. Subsequently, at the 2022 Lomé Summit on Cybersecurity, African Heads of State and Government confirmed their commitment to ensure that cybersecurity remains a top priority at the highest level of governance, suggesting that "the existence of binding standards [...] was a *sine qua non* condition for strengthening the confidence of citizens, businesses and administrations in the digital economy"[15] . And in 2024, the AU *adopted the Common African Position on the application of international law to the use of information and communication technologies in cyberspace*, (hereinafter *Common African Position*). This Position is not a legally binding instrument, but it proves the *opinio iuris* of the region

Indeed, in February 2024, the AU Assembly unanimously endorsed the *Common African Position* presented by the AU Peace and Security Council[16] . This *Position* makes

---

13 *Cf.,* INTERPOL, *Interpol Africa Cyber Threat Assessment Report - 2024 prepared by the African* Cybercrime *Operations Office*, p. 11.

14 *Cf. infra,* section 3.

15 *Cf.* The Lomé Declaration on Cybersecurity and the Fight Against Cybercrime, 23 March 2022, at .

16 For a better understanding of the scope and content of this *Common African Position*, *see* HELAL, M., "Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, and all associated Communiqués adopted by the Peace and Security Council of the African Union (February 2024)", *Ohio State Legal Studies Research Paper* No. 823, at https://ssrn.com/abstract=4714756 or

a significant contribution to the development of international cyber law, until then the involvement of African states in cybersecurity issues was somewhat marginal[17] . Moreover, the *Common African Position* reflects the views of all 55 AU member states, which is clear evidence of *opinio iuris* on the norms and concepts of international law applicable to cyberspace. State support for this *Position* manifests the firm resolve of African leaders to fight malicious and criminal cyber operations executed by both States and non-State actors, as all of them must refrain from malicious or criminal use of ICTs in cyberspace.

It is worth highlighting the successful process for its elaboration. The *Common Position* involved not only the active participation of the 55 AU Member States, its main organs and departments, but also the specialized sector of African civil society. In addition to the Secretariat for Political Affairs and Peace and Security, the Office of the Legal Counsel and the Department of Infrastructure and Energy, experts from the Committee on Intelligence and Security Services in Africa were also involved in the drafting of the Common Position. During the first negotiation phase, a cyber capacity building program, funded and co-organized by Canada, was developed for the politicians and lawyers who - in the second phase - would be responsible for drafting the legal issues of *the Position*. The second phase also involved leading scholars in the field, such as, for example, Dapo Akande who co-founded the Oxford Process on the Protection of International Law in Cyberspace and Michael Schmitt, Liis Vihul, and Marko Milanovic, who were the principal drafters of the Tallinn Manual, among others[18] . In addition, in to gain greater legitimacy, the AU invited several prominent African jurists to join the process, including Dire Tladi, Makane Mbengue, Erika de Wet, Mamadou Hébié, and Martha Bradley. Hence - for Helail[19] - the success of the *Common African Position* was precisely the spirit of collaboration and collegiality present throughout the negotiation and drafting process.

As a starting point, the *Common African Position* recalls that all states have an equal right to participate in the articulation of the rules of international law that apply in cyberspace and that the views of all states have equal weight and value in this process

---

17 VERNIER, S., "The Common African Position on the Application of International Law to the use of information and Communication technologies in cyberspace", *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, *Rivista Trimestrale della Società Italiana per l'Organizzazione Internazionale*, 2024, pp. 291-308.

18 SCHMITT M. N. and VIHUL, L., "Respect *for Sovereignty in Cyberspace," Texas Law Review*, vol. 95, 2017, p. 1639.

19 *Cf.* HELAL, M., "The Common African Position ...", *op. cit.*

(paragraph 6 of the *Common African Position*). Accordingly, the AU Peace and Security Council proposed to draw on Africa's collective expertise and resources, but also on the state strengths of its members. Thus, for example, it is worth noting the intervention of cybersecurity experts from Morocco, when the section on sovereignty was discussed when explaining to diplomats and lawyers the various types of intrusive cyber operations that could be carried out against African states. Computer forensics and cybersecurity experts from Cameroon and Tanzania provided their nuances and differences between legal and technical attribution, and highlighted the challenges that African States could face in meeting their due diligence obligation in preventing and mitigating malicious cyber attacks. Hence, the *Common African Position* places particular emphasis on the importance of international cooperation to enable States to exercise due diligence and combat malicious and hostile cyber operations. Egypt also participated as an expert, having previously served as a member of the First Committee of the UN General Assembly on cybersecurity, so its active presence ensured that the resulting *Common African Position* would be consistent with international political interests and those of African states

The *Common African Position* has a basic structure consisting of a preamble and ten substantive parts on the fundamental principles and norms of the international order. Taking into account the type of experts involved in the process of elaboration of this *Position*, it is understood that its material contents are in tune with the principles and norms of international law and their specific developments relating to cyberspace, albeit sometimes with African overtones. The *Common African Position* examines the application of a number of international legal norms and regimes to cyberspace, especially the respect for territorial sovereignty, the principle of non-intervention, the prohibition of the use of force, the peaceful settlement of disputes and the upholding of the rules of international humanitarian law and human rights

Some of these issues are discussed below, not for the sake of completeness, but with the intention of reflecting the particular African position on the scope and application of the international order to cyberspace.

1.1. Sovereignty and cyberspace

The principle of territorial sovereignty gives states exclusive control and jurisdiction over their territory and population, a principle that applies equally in the realm of cyberspace, which includes "the components of cyberspace located on their territory"

(para. 14 of the *African Common Position*). The African Union affirms that international law, as it applies to the use of ICTs in cyberspace, does not permit a State to exercise authority in the territory of a foreign State in response to unlawful cyber activities emanating from the territory of that foreign State. This criterion applies even when the exercise of such coercive authority by a State has no harmful effects, whether virtual or physical, on the territory of a foreign State. In other words, if a cyber operation - for example, cyber espionage in a foreign State - does not produce direct material damage in that State, the *Common Position* distances itself on this point from the Tallinn Manual, which holds that certain cyber activities, if carried out without causing harmful effects on the territory of the target State, do not constitute violations of sovereignty and are therefore not unlawful[20]

On this issue, the *Common African Position* takes a "more African" or protective stance on the scope of application of the international norm and arguably takes a "pure" approach to cyber sovereignty[21] . For the AU, the obligation to respect the territorial sovereignty of States, as understood for cyberspace, should not require a *de minimis* threshold of harmful effects below which an unauthorized access by a State to ICT infrastructure located on the territory of a foreign State would not be unlawful (paragraph 16 of the *Common African Position*). The AU further states that cyber operations attributable to a State against ICT infrastructure located on the territory of a foreign State that cause effects, such as loss or impairment of functionality, on the territory of a third State, may constitute a violation of the territorial sovereignty of the latter State. In other words, for the AU, the absence of physical damage or harm does not exclude the unlawfulness of cyber interference[22] . The AU justifies its position exhaustively, recalling that this same interpretation inspires other areas of the international order, such as, for example, the unauthorized overflight of a foreign aircraft over the territory of a State. It is considered an unlawful violation of territorial sovereignty, although the mere overflight will not cause any damage or harm to the State in question[23] . Applying, therefore, this

---

20 TERRY, P. C., "Cyber Espionage and Public International Law: The African Union Rejects the Tallinn Manual's Relativist Approach to Cyber Sovereignty," Online Scholarship, Perspectives, dated May 4, 2024, at

21 TSAGOURIAS, N. and BUCHAN, R. (eds.), *Research Handbook on... op. cit.,* pp. 1194-1197.

22 HELLER, K.J., "In *Defense of Pure Sovereignty in Cyber Space"*, *International Law Studies*, vol. 97, 2021, pp. 1464-68; VON HEINEGG, W., *Territorial Sovereignty and Neutrality in Cyberspace*", *International Law Studies*, vol. 89, 2013, p. 123; SCHMITT, M.N., *"*Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*"*, *Chinese Journal of International Law*, vol. 19, 2018, pp. 30, 40, 42-43.

23 *ICJ Reports* 1986, *Military and Paramilitary Activities in and against Nicaragua*, pp. 87-91.

interpretation to cyber espionage, for the AU no specific harm or damage should be required to qualify the remote intrusion into the territory of the other State as unlawful[24]

Moreover - from a political perspective - the African Union considers that it would be highly dangerous to attempt to codify or interpret norms of international law applicable in cyberspace that would allow States to exercise coercive authority on the territory of a foreign State or that would establish a threshold of harm that would reduce the protective scope of the norm of the inviolability of the territorial sovereignty of States. Given the enormous divergences in technical capabilities among States, such new rules or interpretations would be *de facto* reserved to the most powerful States, which could lead to serious abuses that would undermine *de jure* the principles of the independence and sovereignty of States (paragraph 17 of the *African Common Position).* According to the AU, the sovereign cyber infrastructure of a State *must have* and *receive* the same protection as its physical territory. This is the only way to ensure that cyberspace is a safe, secure and peaceful domain. The *African Common Position* also explains that cyber operations conducted by States against persons on foreign territory may violate international human rights law (such as the right to privacy) in addition to potentially violating the territorial sovereignty of States in the territory where the operations occur (para. 55 of the *African Common Position*). This interpretation is in line with international jurisprudence in the Nicaragua case[25] and aligns with the approaches of a growing number of States such as France, Switzerland, Brazil and China, as well as with the position of the Organization of American States .[26]

As can be seen, the *Common African Position* makes a strict interpretation of the principle of territorial sovereignty, in line with the strong political and legal attachment of African states to sovereignty, as a consequence of their particular historical trajectory. This interpretation confirms that for the AU, cyberspace does not constitute an area different from other spaces under the jurisdictional control of the State, and in which international law is fully applicable.

1.2. Prohibition of intervention in a State's domestic affairs

For the AU, the prohibition of intervention in the internal affairs of a State is particularly relevant in the context of cyberspace, given the increasing connectivity

---

24 HELLER, K.J., "In *Defense of Pure ..., op. cit,* pp 1464-74.

25 *ICJ Reports* 1986, *Military and Paramilitary Activities in and against Nicaragua,* para. 251.

26 *See* section III.1.1 *below.*

between States and societies, which offers greater opportunities for States and malicious actors to misuse ICTs to intervene in the internal affairs of third States . According to international law, both direct intervention by *de jure* and *de facto* organs of a state and indirect intervention by persons or groups acting under the direction, instruction or control of a state are prohibited. From this perspective, for the AU, the prohibition of intervention in cyberspace is violated when ICTs are used in such a way as to amount to coercion, understood (coercion) as a policy aimed at imposing restrictions on the will of a foreign state (paragraph 31 of the *African Common Position*). However, the determination of cyber-coercion emanating from a third State is a matter to be assessed on a case-by-case basis. Moreover, for "coercion" to exist, it is not necessary for a State's conduct to rise to the level of completely depriving a foreign State of its freedom of choice or to compel that State to act or refrain from acting involuntarily (para. 32 of the *Common African Position*). Whether cyber coercion is clearly established below the threshold of deprivation of choice must be assessed on a case-by-case basis, although the *Common African Position* also argues for a broader definition of "coercion" when it states that it is policies, rather than actions, that are coercive (paragraph 31 of the *Common African Position*) and that it is the objective of the policies, rather than their success, that counts (paragraph 32 of the *Common African Position*).

Finally, the *Common African Position* recalls that, by virtue of their territorial sovereignty, all States have an obligation to exercise due diligence to prevent other States or non-State actors from using their territory to conduct cyber operations that constitute a violation of the prohibition of intervention in the internal affairs of States. It is not surprising that the *African Common Position* gives a broad interpretation of the principle of non-intervention, given that African States are strong advocates of the principles of sovereign equality of States and the prohibition of interference in the internal affairs of a State[27] , of any kind of interference, including cyber interference.

1.3. Prohibition of the use of force and cyberspace

Regarding the applicability of the prohibition of the use of armed force to cyberspace, the *African Common Position* starts from the premise that the prohibition of the use of armed force applies to *armed* force, regardless of the means used, as already explained

[27] BUCHAN, R., and TSAGOURIAS, N., "The African Union's Statement on the Application of International Law to Cyberspace: An Assessment of the Principles of Territorial Sovereignty, Non-Intervention, and Non-Use of Force," February 20, 2024, at

by the International Court of Justice on the occasion of its advisory opinion on *nuclear weapons*[28] . Thus, for the AU, cyber operations would fall within the scope of application of the prohibition on the use of force, when the scale and effects of the cyber operation are comparable to those of a conventional act of violence covered by the prohibition. In particular, a cyber operation would amount to a use of force, if it is expected to cause physical damage, injury or death comparable to the traditional use of armed force prohibited in the international order (para. 39 of the *African Common Position*). On this issue it does not depart from the Tallinn Manual; rather - on the contrary - it corroborates the Tallinn interpretation.

Doubts may arise, however, when the cyber operation does not result in death or injury, but disables computer networks and systems that support the critical infrastructure of the attacked state. In such a case, the AU aligns itself with the international trend of embracing a more developed or updated interpretation on this issue and extends the prohibition on the use of force to cover cyber operations that disable critical computer networks and systems, especially if the cyber operation *permanently disables critical infrastructure or civilian objects* within a state, just as the prohibition on the use of force is violated, when a cyber operation destroys a military target or disables a missile defense system (paragraph 40 of the *Common African Position*). On the other hand, it takes a strict position on self-defense against cyber operations and rejects the use of force in self-defense against non-State actors, except when their acts can be attributed to a State, in accordance with the law of State responsibility (paragraph 43 of the *Common African Position*). The refusal to admit the right of self-defense against non-state cyber-actors can be understood from the African social and political perspective, whose main concern is to avoid "a normalization" of further unilateral uses of force . [29]

1.4. International humanitarian law and cyberspace

For the AU, International Humanitarian Law (IHL) applies equally to cyberspace, despite the fact that most IHL rules predate the emergence of ICTs. IHL will apply to cyber operations carried out in the context of an international (between states) or non-international (between non-state belligerents and state belligerents) armed conflict, provided that the intensity of the conflict reaches the level of protracted armed violence

---

28 *ICJ Reports 1996, Advisory Opinion on the Legality of the Use or Threat of Use of Nuclear Weapons*, para. 39.

29 BUCHAN, R., and TSAGOURIAS, N., "The African Union's Statement ...," *op. cit*.

required for conventional "wars". The AU justifies its position by expressly bringing to the coalition the advisory opinion of the ICJ on the *legality of the threat or use of nuclear weapons*, where it argues that "by virtue of its "intrinsically humanitarian character", IHL applies to "all forms of warfare and all types of weapons, past, present and future"[30] . For the AU, it is equally required that "the right of belligerents to adopt means to harm the enemy is not unlimited" and that belligerents have an obligation to limit the suffering, damage and destruction caused by an armed conflict (para. 51 of the *African Common Position).*

In paragraph 52 of the *African Common Position*, the AU stresses the due protection of civilian objects and the distinction between civilian objects and military objectives, and includes as civilian objects the ICT infrastructure and scientific infrastructure of a State. It holds that civilian objects must be respected and protected at all times and understands as civilian objects all those goods and objects that are indispensable for the survival of the civilian population, which embraces hospitals, medical personnel and facilities, as well as humanitarian relief operations. And for the same reason - their civilian nature - such assets may not be subject to any kind of cyber-operations, whether intrusions or other attacks, resulting in their destruction or rendering them useless

The *Common African Position* constitutes a relevant guide to the AU's essential views on the applicability of existing international law to cyberspace. Some of its interpretative issues are resolved from a very regional approach, which is a legacy of its own history and the structure of African society today. In short, the *African Common Position* has a strong sovereigntist approach that reflects the legal and political culture of African states.

2.2. NATIONAL CYBERSECURITY STRATEGIES IN AFRICA

Any national strategy in a given area involves the State's roadmap for establishing the means and ways it deems necessary to achieve substantive objectives in that area. Thus, to make progress in cybersecurity, the AU and its Member States are promoting the development of national cybersecurity strategies, through the guidelines of the AU Specialized Technical Committee (STC) on Communication and ICT (CICT) and the Expert Group on Cybersecurity (AUCSEG). This approach would not have been possible

[30] *ICJ Reports* 1996, Advisory Opinion on *the Legality of the Use or Threat of Use of Nuclear Weapons*, para. 86.

without the international cooperation of various institutions, such as the World Bank, the European Union, the Norwegian Institute of International Affairs and cyber research centers such as the Global Cybersecurity Capacity Center (GCSCC), the Oceania Cyber Security Centre (OCSC) and the Cybersecurity Capacity Center for Southern Africa (C3SA). Thus, through workshops, seminars and studies, the AU helps its member states to acquire cyber expertise and to progressively build their cybersecurity. National strategies must be used to manage cyber risks, identify challenges, adopt cyber laws and adapt the existing legal and institutional frameworks of the digital environment

In order to be able to assess the degree of cybersecurity achieved or planned in national cybersecurity strategies, the aforementioned centers - Global Cybersecurity Capability Center (GCSCC), the Oceania Cyber Security Centre (OCSC) or the Cybersecurity Capability Centre for Southern Africa (C3SA) - often assist states in applying the Cyber Maturity Model created by the Oxford University's Global Cyber Security Centre (CMM)[31] . This Model assesses each country's cybersecurity commitment in terms of five pillars that involve the adoption of various types of measures: (i) Legal measures: Whether there is a sufficient legislative framework to harmonize practices at the regional/international level, strengthen cybersecurity systems and simplify international frameworks to combat cybercrime; (ii) Technical measures by national institutions with standards and technical frameworks related to cybersecurity and cybercrime; (iii) Organizational measures to promote information exchange and to assess and implement good cybersecurity practices and systems standards for secure ICTs; (iv) Capacity building measures, including education programs, training of professionals and public awareness campaigns; and (v) Cooperation measures, promoting partnerships, cooperation frameworks and information exchange networks at the national, regional and global levels. As these indicators are met, the degree of cyber maturity is classified into five levels, ranging from the lowest (T5), when the cybersecurity strategy is still under construction, to the highest possible (T1), which is considered achieved, when the State in question meets all or almost all indicators and has a national cybersecurity strategy adopted to the changing circumstances of the moment.

[31] *Cf.,* https://gcscc.ox.ac.uk/the-cmm . The CMM was designed in 2013 by the Global Cyber Security Capability Center (GCSCC) at the University of Oxford. To ensure that the CMM remains current and a powerful tool that captures important developments, the model undergoes periodic reviews. As capability requirements evolve, it becomes necessary to reflect this progress in the model to adequately capture developments and provide information on possible next steps for further improvement. In this regard, the model itself was updated in February 2017, in line with evolving security challenges and based on the experience of implementing the model in the field.

The Global Cybersecurity Index (GCI)[32] developed by the International Telecommunication Union measures countries' commitment to cybersecurity in relation to the five pillars described above and publishes its reports in order to generate public awareness of the achievement of the different dimensions of cybersecurity. Its assessment helps to graphically understand what the level of cybersecurity in Africa is in terms of its national cybersecurity strategies. As derived from the Global Cybersecurity Index (2024), the levels of cyber maturity achieved to date in the region are as follows :[33]

National cybersecurity strategies in Africa Performance levels in 2024				
T5: under construction	**T4: evolved**	**T3: establishing**	**T2: moving forward**	**T1: updated**
Burundi	Angola	Botswana	Benin	Ghana
Central African Republic	Cape Verde	Burkina Faso	South Africa	Kenya
Eritrea	Chad	Ivory Coast	Togo	Mauritius
	Republic of the Congo	Cameroon	Zambia	Rwanda
Guinea-Bissau	Equatorial Guinea	Republic Democratic Congo		Tanzania
	Gabon	Ethiopia		
	Lesotho	Gambia		
	Liberia	Guinea		
	Madagascar	Malawi		
	Mali	Mozambique		
	Namibia	Nigeria		
	Niger	Senegal		
	Seychelles	Sierra Leone		
	South Sudan	Uganda		
	Zimbabwe			

32 *Cf.*, *Global Cybersecurity Index 2024,* available at https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

33 *Cf.*, *Global Cybersecurity Index 2024*, p. 26.

As can be seen, most of the national cybersecurity strategies of African states are still at the stage of construction and identification of their priority objectives (levels T5, T4 and T3 in the table). In contrast, Benin, South Africa, Togo and Zambia have already reached the advanced level in cybersecurity (T2), as they have demonstrated a strong commitment to coordinated and effective cybersecurity, and their respective national strategies envisage concrete actions for the establishment and implementation of certain cybersecurity measures in relation to the five areas described above. To date, only Ghana, Kenya, Mauritius, Rwanda and Tanzania have achieved T1 level, as they have developed national legislative measures in relation to the main pillars of cybersecurity.

Given the impossibility of delving into each and every one of these strategies, we highlight just a few data that illustrate well how the development of African strategies does not follow a single pattern; they cover very diverse issues and logically each State prioritizes its lines of action in the face of its particular challenges and according to the resources available.

A) Kenya is at the forefront of digitization and cybersecurity planning. It has been actively developing cyber defense standards for over two decades. From its first cybersecurity law, the Kenya Information and Communication Act of 1998, to the present day, following the passage of the *National Cybersecurity Strategy (2022-2027)*, the Kenyan government has been deepening its cyberspace security[34] . The promulgation of its Constitution in 2010 paved the way for the revision of that information and communication law, amended in 2013, but also for the adoption of other more far-reaching regulations, for example, the Data Protection Act of 2019 or the Kenya Cybercrime and Computer Misuse Act (No.No. 5 of 2018) , and other strategic plans such as the *National Cybersecurity Strategy* of 2014, the Cybersecurity Guidance Note for Payment Service Providers (PSP) of 2017, the Digital Economy Plan (2019**)** or the National ICT Policy Guidelines of 2020**.**

Kenya's Strategy has three clear objectives: 1). Empower individuals and businesses by equipping them with the knowledge and tools to navigate the digital world securely; 2) Boost the national economy and building a secure cyberspace fosters trust and attracts investment, driving economic growth; and 3) Protect national security by safeguarding critical infrastructure and information is essential for national stability and development.

---

[34] *Cf.* ATANDI, F., *Crossing the Digital Divide: Kenya's Cyber Security Journey*, February 24, 2024, at .

To achieve these it has a proactive plan to cultivate a trusted information environment for all. It establishes clear governance structures and sound legal frameworks. It strengthens critical infrastructure protection, and creates a plan to "invest" in expertise that fosters a skilled workforce equipped with advanced cyber capabilities. In addition, *the Strategy* contemplates that in order to achieve the three objectives it is necessary to activate mechanisms to reduce cybercrime incidents and mitigate their damage. And it also establishes the urgency of "joining forces" and cooperation and collaboration, both nationally and internationally to strengthen cyber resilience. Kenya's proposed cybersecurity plan is comprehensive, advanced and adapted to evolving technology and challenges, justifying its top rating (T1) for cyber maturity in the Global Cybersecurity Index.

B) Among the T3 level states is the Federal Republic of Nigeria, as it is still building its cybersecurity system. In August 2024, Nigeria announced a new technology target for 2050. Its Nigerian Minister of Communications, Innovations and Digital Economy announced its cybersecurity plan to transition from Internet Protocol version 4 (IPv4) to the more advanced Internet Protocol version 6 (IPv6). The implementation of this latest version of the fundamental technology (Internet Protocol) that powers the Internet will substantially improve Nigeria's cybersecurity posture, as IPv6 technology can support an Internet of billions of devices and can provide sufficient address space to meet the needs of the growing Internet.

C) Since 2019, the Republic of Chad has also been seeking to develop a national cybersecurity strategy, but its development has slowed down considerably, given the urgency of other priorities, such as food security, as stated in the strategic plan for Chad (2024-2028)[35] . In terms of cybersecurity, the Global Cybersecurity Index gives it a T4 rating, as there has been some progress in the fight against cybercrime. Thus, for example, in 2022, it was finally possible to define some objectives to improve the fight against cyber threats, thanks to the joint action of various government agencies and departments[36] , which resulted in two national laws on the subject: Ordinance No. 007/PCMT/2022 of

35 *Cfr.*

36 Specifically, the Ministry of Telecommunications and Digital Economy, the National Agency for Information Security and Electronic Certification (ANSICE) and the International Telecommunication Union (ITU).

August 31, 2022, on cybercrime and cyber defense and Ordinance No. 008/PCMT/2022 of August 31, 2022, on cybersecurity.

3. THE FIGHT AGAINST CYBERCRIME AS A CYBERSECURITY PRIORITY IN AFRICA

The AU and its member states are committed to the rule of law at the national and international level with regard to the protection of cyberspace and its citizens against cybersecurity threats. Thus it is clear from the diversity of African strategies that - despite their great substantive differences and their level of performance - one common element can be drawn from them all: the fight against cybercrime as the central core of cybersecurity.

The fight against cybercrime must be an integral part of a good national cybersecurity strategy. But a poor distinction between cybersecurity and the fight against cybercrime is insufficient and highly dangerous, in my view, as it leaves real cybersecurity, which goes beyond cybercrime and requires a technical and legal approach to protect systems, critical infrastructure, services and the consumer from attacks and failures, without resources and measures.

Early regional approaches in Africa focused on the adoption of model laws against cybercrime that could serve as a regulatory guide for States in their national laws. In 2008, the Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA) project was launched with the assistance of the International Telecommunication Union and the European Union, which resulted in the development of the Southern African Development Community (SADC) Model Law on Cybercrime and Cybercrime. This Model Law has been progressively incorporated into many African laws, such as, for example, in the cybercrime law of Egypt (2023)[37] , Ethiopia (2016)[38] , Kenya (2018)[39] , Malawi (2016)[40]

---

37 https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites-and-full-surveillance-of-egyptians/

38 *Cf.,* YILMA, K.M., "Ethiopia`s new cybercrime legislations: some reflections", *Computer Law & Security Review*, vol. 33, 2, April 2017, pp. 250-255.

39 https://thecommonwealth.org/publications/commonwealth-cybercrime-journal-volume-1/comparative-review-cybercrime-law-kenya-juxtaposing-national-legislation-international-treaty

40 Although, it only regulates some aspects, *cfr,* Electronic Transactions and Cyber Security Act 2016 (No. 33, 2016) and Communications Act 2016 (No. 34, 2016). The Electronic Transactions and Cyber Security Act 2016 (No. 33, 2016) criminalizes as cyber crime: Sec. 84 Unauthorized access, interception or interference with data; Sec. 85 Child pornography; Sec. 86 Prohibition of cyber harassment; 87 Prohibition of offensive communication; 88 Prohibition of cyber stalking; 89. Prohibition of hacking, decryption and introduction of virus; 90. Illegal deactivation of a computer system; 91. Prohibition of sending spam; 92. Prohibition of illegal trade and commerce; 93.

, Mauritius (2003) ,[41] Morocco (2003)[42] , Nigeria (2015)[43] , Senegal (2008)[44] , South Africa (2020)[45] , Tanzania (2015)[46] , Tunisia (2022)[47] , Uganda (2011)[48] and Zimbabwe

41 Mauritius passed its first Computer Misuse and Cybercrime Act in 2003. Its adaptation against cybercrime responds to its cybersecurity strategy (2014 -2019). Its strategy focused against cybercrime and addresses issues related to the investigation and prosecution of offenders and the role of the criminal justice system, while the cybersecurity strategy focused on prevention, mitigation and defense of critical national infrastructure assets. *Cf.,* https://www.coe.int/en/web/octopus/-/mauritius

42 In 2007, it adopted its "National Strategy for Information Security and Digital Trust" which was amended in 2013 and 2020, along with the adoption of the National Directive on Information Systems Security for Critical Infrastructures. Its main instrument, the "Moroccan Law on Cybercrime" of 2003, aimed to address various aspects of cybercrime and to establish legal frameworks to deal with crimes related to information systems and automated data processing. Since then, its national rules have been amended in accordance with international standards, as Morocco signed in Strasbourg the Budapest Convention on Cybercrime and its respective protocols, including the second one of 2022, which focuses on strengthening cooperation and disclosure of electronic evidence. *Cf.*, IDRISSI, H., "Cybersecurity in Morocco: between achievements and challenges", November 2023, at https://mipa.institute/en/10778.

43 The first Cybercrime (Prohibition, Prevention, etc.) Act 2015 was enacted in 2015. Its objective was to promote cybersecurity and cybercrime prevention, and to establish obligations on the private sector to report and cooperate with law enforcement authorities and the Nigerian Computer Emergency Response Team (ng-CERT). It established a Cybercrime Advisory Council to facilitate effective enforcement, capacity building, multi-stakeholder engagement, and interagency and international cooperation. It was amended in 2024, to remove sections restricting freedom of expression and addressing "cyberbullying." Cfr., https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2024.pdf

44 Its first national law on cybercrime dates back to 2008, the main objective of which was to remedy the legal vacuum that characterized the criminal structure regarding offenses committed by cybercriminals. Since then, its Criminal Code has undergone several amendments to take into account cybercrimes, such as, for example, breach of confidentiality and integrity of computer systems (Articles 431-8, 431-9, 431-10, 431-11) and breach of computer data (Articles 418-11, 12, 13, 14, 15, 16). In 2016, it acceded to the Budapest Convention on cybercrime in December 2016 and has consequently developed, a new framework against cybercrime: Plan Sénégal Émergent (PSE 2035), which provides for the structural transformation of the economy by 2035; the adoption of the "Senegal Digital Strategy 2025" (SN2025), which promotes ICT as one of the key drivers of this economic transformation; and the development of the " National Strategy for Cybersecurity 2022 " (SNC2022) to establish digital trust.

45 South Africa enacted local legislation called the Cybercrime and Cybersecurity Act 2020, which aimed to regulate and strengthen local processes related to the investigation, prosecution and jurisdiction of local courts to adjudicate cybercrimes.

46 The Cybercrime Act 2015 is the main source of substantive law provisions and addresses all offenses listed in the Budapest Convention *Cfr.,* https://www.hrw.org/news/2023/12/19/tunisia-cybercrime-decree-used-against-critics. However, in March 2024**,** Tunisia acceded to the Council of Europe Convention on Cybercrime. All indications are that Council of Europe and Tunisian authorities will continue to cooperate with a view to further reforms of national legislation and undertake capacity building activities to facilitate the full implementation of the Convention on Cybercrime.

48 The Computer Misuse Act 2011 ("CMA") is the main general legal regime relating to computer crime and electronic evidence. In addition, there are other laws such as the Copyright and Neighbouring Rights Act 2006, the Interception of Communications Regulation Act 2010 or the Uganda Penal Code Act, which also provide for rules related to computer crimes and electronic evidence. The Electronic Signatures Act 2011 provides for and regulates the use of electronic signatures, while the Electronic Transactions Act 2011 provides a legal and regulatory framework to enable and facilitate electronic communications transactions and to give legal recognition to electronic records. *Cf., Africa Cybersecurity Report, Uganda 2019/2020, Local Perspective on Data Protection and Privacy Laws, Serianu, at*

(2017). All of these national laws are focused on cybercrime and its prosecution, but without addressing technical cyber defense measures or cybersecurity best practices.

It should be noted, however, that the Council of Europe criticized the SADC Model Law, insofar as it displaced the 2001 Convention on Cybercrime (known as the "Budapest Convention") as the model for harmonization of cybercrime standards in Africa with the rest of the States of the International Community. In fact, as of 2011, no African state had ratified it, prompting the Council of Europe to call on African states to do so. The defense of the Budapest Convention bore fruit and in 2018, Mauritius, Morocco and Senegal ratified it. The tension, however, between the leadership of the Budapest Convention or the SADC Model Law as a yardstick for national laws against cybercrime led the AU Expert Group on Cybersecurity to work on the future African Convention on Cybersecurity and Personal Data Protection, which was adopted in 2014, (better known as the Malabo Convention)[49] , which has a strong regional focus. It was able to enter into force - finally - in June 2023, once the 15 instruments of ratification were deposited . [50]

The Malabo Convention imposes behavioral obligations on signatory states to adopt binding national rules to promote cybersecurity governance and control cybercrime. It thus aims to harmonize substantive law, albeit with broader approach than the Budapest Convention, as it includes the harmonization of e-commerce laws and data protection. It also obliges signatory states to develop a national cybersecurity strategy (art. 24.2 of the Malabo Convention), which should include at least the following issues: (i) defining organizational structures for cybersecurity governance; (ii) establishing objectives and timelines for the success of the national cybersecurity police; and (iii) establishing some mechanism for the effective management of cybersecurity incidents. In other words, through the conventional route, the development of national cybersecurity strategies is required for African States to regulate national measures in the same five pillars as the Cyber Maturity Model, proposed by Oxford University.

The Malabo Convention also provides that States must establish mechanisms and institutions for the implementation of national strategies, but does not add or complete

---

49 On this issue, *cf.,* ORJI, U., Tthe African Union Convention on cybersecurity: a regional response towards cyber stability?", *Masaryk University Journal of Law and Technology*, vol. 12, 2018, pp. 91-127.

50 To date, the States that have already ratified this Convention are: Angola, Cape Verde, Côte d'Ivoire, Congo, Ghana, Guinea, Mozambique, Mauritania, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo and ZambiaCfr., https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf

any specific way to advance the real effectiveness of such national strategies. It also includes the promotion of a culture of cyberdefense (art. 26); the creation of structures or institutions for the governance of cybersecurity (art. 27); the obligation to protect the critical infrastructure of the State (art. 25.4); and that serious penalties be provided for cybercrime and other related criminal activities. To this end, art. 25.1 of the Convention provides for the criminalization of unauthorized access to network systems or data systems, and calls on signatory states to establish cooperation networks within the AU (art. 28.4 of the Malabo Convention)[51] . However, its practical results will be delayed due to the regulatory complexity involved in its application until significant progress is made in cybersecurity. The AU encourages the rest of its members to adhere to it and thus - as a first step - South Africa signed it in February 2023, but is still in the process of ratifying it.

As can be seen, the Malabo Convention does not provide major substantive innovations on how to prevent and prosecute cybercrime. Its most significant contribution is that it elevates to the rank of international obligation the usual measures and commitments in this area, already regulated previously in the Budapest Convention, and also incorporates content already suggested in the Oxford Model of Cyber Maturity. Undoubtedly, the entry into force of the Malabo Convention is an achievement for the AU, which shows the region's awareness of cybersecurity[52] , although its contents only imply behavioral obligations that signatories must develop in their national jurisdiction. The Malabo standards are more than just a guide for signatory states, they are internationally enforceable obligations that affect the development of their respective national cybersecurity regimes.

III. CYBERSECURITY APPROACHES IN LATIN AMERICA AND THE CARIBBEAN

The Organization of American States has been working for years towards the creation of a solid cybersecurity in the region through various programs and actions, which - in essence - pursue a dual objective: on the one hand, to provide itself with the necessary tools to promote the creation of a regional framework for cybersecurity; and,

51 On these issues, *see* VERNIER, S., "The Common African Position ..., *op. cit*.
52 ORJI, U., "The African Union Convention..., *op. cit*.

on the other hand, the creation of specific mechanisms for cooperation in criminal matters, aimed at counteracting cybercrime in the region . [53]

In 2003, the OAS established a new multidimensional security paradigm with the adoption of the "Declaration on Security in the Americas". This Declaration departed from a traditional conception of national security to justify the need for a new multidimensional approach, which included cybersecurity. In 2004, it approved the "Inter-American Comprehensive Strategy to Combat Threats to Cybersecurity: for the Creation of a Culture of Cybersecurity"[54] . From the combined reading of both resolutions, it is clear that there is a need to establish for the entire OAS a "comprehensive strategy for the protection of information infrastructures that adopts an integral, international and multidisciplinary approach adapted to the challenges of technological development". For the OAS, the concept of cybersecurity could not be limited solely to the prevention and criminalization of malicious acts against the security of computer systems and networks, but also encompassed the regulatory and technical aspects of cybersecurity, as central elements for the control of cybercrime.

In line with this broad vision of cybersecurity, the 2004 Strategy was built around four pillars: 1) strengthening the knowledge of Internet users and operators regarding their security and computing, threats related to the use of the network and existing tools to defend against cyberspace-related risks; 2) promoting public-private partnerships, in order to increase education, awareness and cooperation with the private sector and enable private stakeholders to effectively protect such infrastructures; 3) identifying and developing technical standards and best practices with a view to ensuring the security of information transmitted over the Internet and other communication networks ; and 4) adopting cybercrime legislation and policies aimed at safeguarding network users and preventing the misuse and criminal misuse of information and computer systems. Accordingly, the 2004 Strategy established clear mandates for the OAS and other stakeholders, in cooperation with the OAS, to design collaborative cybersecurity capacity

---

53 On these issues, *cf.,* FASCIGLIONE M. and NINO, M., "The activity of the Organization of American Stares in the field of Cybersecurity", in *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, *Rivista Trimestrale della Società Italiana per l'Organizzazione* Internazionale, 2024, pp. 249-264; HUREL, L.M., "Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America", *Global Security Review*, Volume 2, January (2022), pp. 21-31, DOI: 10.25148/GSR.2.009786.

54 Resolution AG/RES. 2004 (XXXIV-O/04) " Adoption of a comprehensive inter-American strategy to combat cybersecurity threats: a multidimensional and multidisciplinary approach to building a culture of cybersecurity" .

building activities for the region. Under this umbrella, of particular note is the work of the Inter-American Juridical Committee (CJI), on the one hand, to support the full applicability of international law to cyberspace in the international relations of the OAS and its member states; and, on the other, the work of the Inter-American Committee against Terrorism (CICTE), the Inter-American Telecommunication Commission (CITEL), the Group of Governmental Experts on Cyber-Crime, and the Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA), to establish technical standards for a secure Internet architecture for OAS members and to assure its Members of the necessary tools, both political - e.g., national cybersecurity strategies - and legal - laws against cybercrime - to protect Internet users and information networks.

Under the mandate of Secretary General Luis Almagro, the OAS promotes cybersecurity in the region with international cooperation, specifically with the Inter-American Development Bank (IDB), the Global Cyber Security Center of the University of Oxford and the Observatory for Cyber Security in Latin America and the Caribbean, in to make realistic progress in cyber defense capabilities given regional resources and constraints. The IDB's 2016[55] and 2020[56] reports reflect little progress, many shortcomings and some lessons learned. Both reports apply the Cybersecurity Capability Maturity Model for Nations (from Oxford University[57] , which comprehensively measures a state's cyber maturity . [58]

---

55 *Cfr.* 2016 Cybersecurity Report, entitled *Ciberseguridad ¿estamos preparados en América Latina y Caribe? At* https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

56 *Cf.,* Cybersecurity 2020 Report, entitled *Cybersecurity : risk, progress and the way forward, 2020,* available at https://publications.iadb.org/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

57 *Cf.,* https://gcscc.ox.ac.uk/the-cmm. The CMM was designed in 2013 by the Global Cyber Security Capability Centre (GCSCC) at the University of Oxford. To ensure that the CMM remains current and a powerful tool that captures important developments, the model undergoes periodic reviews. As capability requirements evolve, it becomes necessary to reflect this progress in the model to adequately capture developments and provide information on possible next steps for further improvement. In this regard, the model itself was updated in February 2017, in line with evolving security challenges and based on the experience of implementing the model in the field.

58 On these issues, *see* LÓPEZ-JACOISTE DÍAZ, E., "La Cooperación de la Unión Europea para la construcción de la ciberseguridad en América Latina y el Caribe", in Cervell Hortal, M. J. and Piernas López, J. J. (dirs.), *Hacia una regulación internacional para el ciberespacio,* Aranzadi, Cizur Menor 2023, pp. 317-354; MORENO, J., ALBORNOZ M. M., and MAQUEO, M. S., "Cybersecurity: state of the art in Latin America," *Revista de Administración Pública* INAP, vol. LIV, no.1, 2020, pp. 23-26, p. 32. AGUILAR ANTONIO, J. M., "La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas", *Revista de Estudios de Seguridad Internacional*, vol. 6 (2), 2020, pp. 17-43; VILA SEOANE, M., "La ciberhegemonía de EEUU en la OEA", *Estudos Internacionais,* vol. 10, 2023, pp. 91-112.

1. THE INTERNATIONAL LAW APPLICABLE TO CYBERSPACE, ACCORDING TO THE ORGANIZATION OF AMERICAN STATES

The Inter-American Juridical Committee (CJI), which is part of the organic and consultative structure of the OAS, is competent to study legal problems related to regional integration and advises the States on the possibility of standardizing their legislation, if appropriate. Thus, in the exercise of its functions, the CJI has promoted a constructive dialogue among its Member States on the full applicability of international law to cyberspace[59] . In 2018, it launched a first initiative entitled: "Enhancing Transparency: International Law and State Cyber Operations", which sought to establish clarity on how nation states understand the application of international law to cyberspace, identifying areas of convergence and divergent positions. After several meetings and seminars on the evolution of cyber conflict and international law, the Inter-American Juridical Committee presented in 2022 a second report on *International Law Applicable to Cyberspace*[60] , which reflects the common feeling of the region on this issue.

The positions of the OAS and its Member States are generally along the same lines of interpretation and application as the Tallinn Manual, the reports of the International Committee of the Red Cross or the Oxford Process on International Law Protections in Cyberspace (2020). However, for the OAS and its Members, the application of international law to cyberspace is particularly relevant for the region given the various national cybersecurity policies and challenges faced .[61]

1.1. Sovereignty and cyberspace

The principle of sovereignty implies the "right of a State to exercise State functions in that place to the exclusion of any other State"[62] , as was found in the *Isle of Palms* arbitration award. According to the OAS, state sovereignty must extend to

---

59 *Cf.,* among others, SALAZAR ALBORNOZ, M., "El Comité Jurídico Interamericano ante los retos de la era digital: las relatorías sobre privacidad y protección de datos personales y sobre el derecho internacional aplicables al Ciberespacio," *Electronic Journal of Contemporary International Law*, 2022, vol. 5, https://doi.org/10.24215/2618303Xe042

60 *Cf.,* CJI/doc. 671/22 rev.2, of 22 August 22, 2022, 101st ORDINARY SESSION OAS/Ser. Q 1 - 10 August 2022, Rio de Janeiro, Brazil: Second Report of the Inter-American Juridical Committee: International Law Applicable to Cyberspace, available at https://www.oas.org/es/sla/cji/docs/CJI-doc_671-22_rev2_ESP.pdf (hereinafter ICJ Report 2022).

61 In this paper, however, we leave aside Canada and the United States, which, although they are members of the OAS, have different political, economic and legal conditions from the rest of the OAS members.

62 *Isle of Palms* case, United States v. Netherlands, arbitral award, 1928.

cyberspace, including its physical and non-physical components, since, in the digital age, a state's sovereign powers over its territory and other objects or subjects are increasingly exercised through and dependent on ICTs.

It should be borne in mind that, for most OAS States, sovereignty is an independent rule of international law, the violation of which generates international responsibility of the State[63] . Therefore, a cyber operation coming from a third State will always be a violation of State sovereignty, even if the penetration of networks from the territory of another State does not produce even a minimum of harmful effects, which is what is called a *de minimis* approach[64] . On this point the Latin American and Caribbean States depart from the interpretation of the Tallinn Manual, which requires a certain degree of damage produced by foreign cyberoperation, i.e. when the cyberoperation exceeds a minimum threshold of damage. The non-acceptance of this threshold is based on the notion of sovereignty in the *Isle of Palms* case, which is exclusive and does not contemplate exceptions

Thus, for example, for most OAS members - except Canada and the United States - cyber espionage should be prohibited by international law, regardless of national laws. For the Costa Rican government, there is a violation of sovereignty when a third state carries out cyber operations that constitute a usurpation of inherently governmental functions, regardless of the physical or non-physical effects they may have on *hardware* or *software* located in the territory of the victim state[65] . For its part, Brazil seems to defend an intermediate position, given that interceptions of telecommunications would be considered to violate sovereignty, as would any cyber-operations against computer systems located in the territory of another State, if they cause extraterritorial effects .[66]

1.2. Prohibition of intervention in the domestic affairs of a State and its applicability to cyberspace

---

63 *Cf.,* CJI Report 2022, pp. 15 and 16.

64 ROGUSKI, P. "Application of International Law to Cyber Operations: A Comparative Analysis of States' views", *Policy Brief*, The Hague Program for Cyber Norms, Universiteit Leiden, (2020), p. 4, at https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views.

65 Point 21, of Costa Rica's position at https://cyberlaw.ccdcoe.org/wiki/National_position_of_Costa_Rica_(2023)#Applicability_of_international_law

66 CHARLITA DE FREITAS, L., IÓRIO ARANHA, A., "The instrumentalization of responsive regulation and its relative efficiency: experiences of the Brazilian National Telecommunications Agency", *Revista Latinoamericana de Economía y Sociedad Digital*, vol, 4, 2024, pp. 160-191.

For the States of the OAS, the principle of non-intervention is a fundamental principle of international law which, among other things, implies the prohibition to use any method of coercion in the internal affairs of States, including the choice of political, economic, social and cultural system and the formulation of foreign policy[67] . According to the IAJC Report, this principle applies integrally to cyberspace[68] , even if there are difficulties in discerning in a specific case, whether a cyber operation can be qualified as coercion or whether it involves an intervention in the internal affairs of the State.

For some States, the act - or cyberoperation, of whatever kind - is coercive if it is specifically designed to compel the victim State to modify its behavior on a matter that is within its *domaine reservé.* Brazil, on the other hand, qualifies that it would be sufficient even if the act effectively deprives the attacked State of its ability to control or govern matters within its *domaine reservé* (without actually seeking to compel the State to change its behavior). Moreover, it considers that cyber operations aimed at interfering in the electoral processes of another State constitute violations of the principle of non-intervention, since - without doubt - elections are the hard core of a State's internal affairs[69] , all the more so if the malicious use of ICTs against a State involves a certain level of coercion. It is not disputed, however, that if a cyber-operation interferes with and overrides the competence of a State to protect its population, for example, in the area of health, the rule of non-intervention would be violated.

1.3. Prohibition of the use of force, self-defense and cyberspace

Most of the States that have spoken at the ICJ working rounds agree that a cyber operation may violate the prohibition on the use of force provided for in Article 2.4 of the UN Charter, if certain conditions are met. Admittedly, the notion of "force" in this prohibition refers to "armed" force[70] , so it would have to be determined when a cyberoperation constitutes a prohibited use of "armed" force under that article.

Generally speaking, States in the region consider that a cyber operation would violate the prohibition on the use of force if its "scale and effects" are comparable to those of kinetic attacks, as such criteria constitute the traditional interpretation of the prohibition on the use of force under international law, which should always be assessed on a case-

67 ICJ *Reports* 1986, *Military and Paramilitary Activities in and against Nicaragua* para. 205.
68 CJI Report 2022, p. 17.
69 *Cfr.,* https://cyberlaw.ccdcoe.org/wiki/National_position_of_Brazil_(2021)#Prohibition_of_intervention
70 DELBRÜCK, J.: "Article 24", in *The Charter of the United Nations. A Commentary*, Bruno Simma (ed.), Oxford University Press, Oxford, (1995), pp. 397-407.

by-case basis[71] . In this sense, there is no difference with the Tallinn Manual in relation to the prohibition of the use of force. However, in order to measure the harm, factors such as the nature and extent of the damage or death to persons and the destruction of, or damage to, as well as the context of the event, the perpetrator of the action, the target and its location, the effects, as well as the intent of the actor, must be taken into account. Cyber operations that cause death, injury or significant destruction, or pose an imminent threat thereof, amount to a prohibited use of force.

Brazil, for its part, is cautious about drawing analogies between cyber and kinetic actions, particularly considering that - to date - no State has alleged a violation of Art. 2.4 of the Charter as a result of a cyberattack. It considers that in many cases it might be difficult to draw a direct analogy between the acts of aggression envisaged in UNGA Resolution 3314[72] and cyber-operations, and therefore advises that the multilateral understanding of what acts constitute use of force and aggression be updated to include cyber-attack scenarios. However, Guyana expressed doubts to the Inter-American Juridical Committee as to whether an isolated cyber-operation - without kinetic armed force of any kind - could be considered a prohibited use of force under Article 2.4 of the Charter, even if it generates some damage.

Another core question that arises is whether a cyberattack can give rise to the lawful exercise of self-defense, under Art. 51 of the Charter. For this, "scale and effects" of the cyber-operation must first be determined, since only the most serious uses of force[73] , those that cause death or injury to persons or damage or destruction of property will be considered as an armed attack and, therefore, will trigger the right to legitimate self-defense. This is the opinion of most of the States in the region[74] , but some of them with some nuances. Chile argues that "cyber-attacks directed against its sovereignty, its inhabitants, its physical or information infrastructures could meet the requirements to be considered as armed attacks"; while Brazil recalls that the right to self-defense is triggered by the existence of an actual or imminent armed attack, so that there is no right to preventive self-defense against a hypothetical cyber-attack. Moreover, for Brazil, self-defense can only be exercised against cyber-operations committed by state actors, but not in response to non-state actors, unless they are acting on behalf of or under the control of

71 *Cf.*, CJI Report 2022, pp. 17 and 18.
72 United Nations General Assembly, resolution 3314(XXIX), "Definition of aggression", adopted on 14 December 1974.
73 ICJ *Reports* 1986, *Military and Paramilitary Activities in and against Nicaragua,* para. 191.
74 *Cf.,* CJI Report 2022, pp. 23 and 24.

a state. On the other hand, Cuba rejects the automatic application of Art. 51 of the Charter to cyber-operations. It considers that the apparent regulatory vacuum with respect to cyberspace and the absence of consolidated concepts cannot support a definition of cyberattack that implies an unjustified extension of the notion of armed attack, in order to legitimize aggressions under the alleged argument of a right to legitimate self-defense. It argues that "there are no legal elements of weight to justify in a coherent and non-selective manner the intention to change the scope of the legal concepts of war, crime of aggression or armed attack, just to justify the use of force as legitimate self-defense against a so-called cyber-attack and ignore more urgent situations"[75] . On the other hand, Guyana clarified that cyber-only operations, which do not involve the use of physical weaponry, can never be considered as an armed attack triggering the right to self-defense.

1.4. International humanitarian law and cyberspace

The OAS States reaffirm that International Humanitarian Law (IHL) applies to cyber operations in times of armed conflict, recalling the advisory opinion of the International Court of Justice on *the legality of the threat or use of nuclear weapons*[76] . Since excluding cyber-operations from IHL would be incompatible with the intrinsically humanitarian nature of the legal principles protected in this area and which apply to all forms of combat and to all weapons, past, present and future. Brazil clarifies that IHL is applicable to cyber operations (i) when they are used as part of an ongoing armed conflict, to contribute to conventional operations, and (ii) when the cyber operation itself crosses the threshold of violence to be classified as an armed conflict. Only Cuba excludes the applicability of IHL to ICTs in the context of international security, "since that would imply the militarization of cyberspace and would be a first step towards equating a cyberattack to a traditional armed attack."[77] . Moreover, it considers that, if the targets to be attacked in a conflict are not considered legitimate or in time of war, they are targets that should be protected against all types of attacks or actions, whether cyber or not[78] . On the other hand, Brazil argues that this is not intended to legitimize illegal cyber

---

75 Item 10 of its 2024 position, available at https://cyberlaw.ccdcoe.org/wiki/National_position_of_Cuba_(2024).

76 *Cf.*, CJI Report 2022, pp. 19-22.

77 Cuba's position, first session of the OEWG of December 2021, p. 29, available at https://front.un-arm.org/wp-content/uploads/2021/04/A-AC.290-2021-INF-2.pdf.

78 Point 6 of Cuba's position in 2021, available at https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Documento_de_posici%C3%B3n_de_Cuba._Aplicaci%C3%B3n_del_Derecho_Internacional_a_las_TIC_en_ciberespacio.pdf.

operations, but only to ensure a minimum level of protection in the event of armed conflict.

For the Inter-American Juridical Committee it is crucial to determine whether a cyber-operation can constitute an "attack" for the purposes of IHL, and under what assumptions. Since Art. 49 of Additional Protocol I defines 'attacks' as "acts of violence against an adversary, whether offensive or defensive", all indications are that cyber-operations that can reasonably be expected to cause injury or death to persons or damage or destruction to objects amount to "attacks" under IHL. Moreover, Art. 36 of Additional Protocol I to the Geneva Conventions requires that the development of new weapons must pass a legal review verifying that their use complies with humanitarian principles. This legal control is mandatory and must be applied to any new weapon or method of warfare, including cyberweapons and all types of cyber operations conducted in the context of an armed conflict, provided that they may cause significant harm.

Under the principle of distinction, the parties to an armed conflict must at all times distinguish between civilian objects and military objectives and, consequently, direct their operations only against military objectives. According to Art. 52.2. of Additional Protocol I, military objectives are those which, by their nature, location, purpose or use, contribute effectively to military action and whose total or partial destruction, capture or neutralization, in the circumstances of the moment, offers a definite military advantage. Costa Rica considers that the qualification of an object as a military objective must be made on a case-by-case basis and that in practice this implies doing so from the lowest possible level. Thus, in order to assess whether cyber infrastructure is a military objective, the military advantage provided by each computer, cable, router or other specific device, which can be separated from a network or system as a whole, must be assessed .[79]

In applying these issues to the field of cyberspace, a debate arose within the ICJ as to whether cyber-hijacked data, for example, can qualify as a "good", and whether it is a military objective or a civilian good under IHL, especially if the cyber-operation does not produce harmful physical effects. For Chile, the notion of "goods" is limited to those with physical properties, which are visible and tangible in the real world, and therefore data are not goods, although this is the position of the Tallinn Manual 2.0. It recognizes, however, that an attack directed exclusively against computer data could have adverse consequences affecting the civilian population, and therefore, because of its effects, the

[79] Point 46, of Costa Rica's position, available at https://cyberlaw.ccdcoe.org/wiki/National_position_of_Costa_Rica_(2023)#Military_objectives.

principle of distinction should be taken into account and any State should refrain from attacking computer data, if it could affect the civilian population, unless such data were being used for military purposes.

2. NATIONAL CYBERSECURITY STRATEGIES IN THE AMERICAS

Any national cybersecurity strategy involves a State's roadmap for defining the objectives, ways and means of ensuring cybersecurity in its jurisdiction, affecting - therefore - both public and private bodies.

In 2020, the level of cyber maturity achieved in the Latin American region was quite precarious[80] : only 12 States had so far approved national cybersecurity strategies[81] . But no strategy had reached the highest levels of cyber maturity - the so-called strategic and dynamic levels, according to the Maturity Model of the Global Cyber Security Capability Center (GCSCC) of the University of Oxford -[82] . Only Colombia, Jamaica, Trinidad and Tobago, Panama and Uruguay expressly contemplated in their national strategies mechanisms for consultation with strategic sectors and civil society to adapt their responses to the risks and threats posed by cyberspace. According to the IDB, the Latin American and Caribbean countries were not yet prepared to face the digital divide in the region, which was subsequently aggravated by the economic slowdown caused by the pandemic. The main obstacles to progress in cybersecurity were the lack of qualified professionals, obsolete systems and software, scarcity of financial resources and the absence of adequate national legislation against cybercrime . [83]

In order to address these shortcomings, the OAS, in cooperation the National Cybersecurity Directorate of Israel, presented its member states with new guides and instruments advance cybersecurity in the region. Of particular note are the "Practical Guide with principles and rules for planning, building and editing cybersecurity

---

80 According to the Inter-American Development Bank's report entitled *Cybersecurity: Risk, Progress and the Way Forward Cfr.,* Report at https://publications.iadb.org/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

81 Namely: Colombia (2011 and 2016), Panama (2013), Trinidad and Tobago (2013), Jamaica (2015), Paraguay (2017), Chile (2017), Costa Rica (2017), Mexico (2017), Guatemala (2018), Dominican Republic (2018), Argentina (2019) and Brazil (2020),

82 MORENO, J., ALBORNOZ M. M., and MAQUEO, M. S., "Ciberseguridad: estado de la cuestión..." *op. cit*., p. 32.

83 LÓPEZ-JACOISTE DÍAZ, E., "La cooperación de la Unión Europea ....", *op. cit*., pp. 323-328.

exercises" (November 2022)[84] ; a new "Methodology in cyber defense for organizations: version 1.0" (July 2022) and in 2024, a new study on "Reducing cybersecurity risks at organizational endpoints. A technical approach Best Practices in Cybersecurity"[85] , on concrete measures to protect *endpoints* by setting up physical security circuits, access denial and privilege assurance or information protection and security *software*.

With the support of these guides, the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) assists States in establishing national cybersecurity incident response teams to build their respective national cybersecurity strategies. CICTE's support is mainly provided through three different channels: i) the dispatch of technical missions to the host State; ii) practical and policy advice to the State, but without *on-site* technical missions; and iii) indirect advice to the State through CICTE's partnership with the State's private business sector for the development of cyber trainings. Thus, for example, the Dominican Republic, Paraguay, Mexico, Costa Rica and Panama have benefited from CICTE technical assistance with formal missions and training activities for consultations with all parties involved in building national cybersecurity. Chile, on the other hand, received informal support for the development of its own cybersecurity strategy, although - like Argentina, Peru or Brazil - it is still lagging behind in the development of its cybersecurity policies, which makes it difficult to establish the complete cybersecurity map in the region

As in the case of Africa, the *Global Cybersecurity Index*[86] has also assessed the level of cybersecurity achieved in Latin America and the Caribbean in terms of existing national cybersecurity strategies in the region. According to the *Index*, the levels of cyber performance and maturity achieved in Latin America and the Caribbean have evolved favorably since 2020 and in September 2024 are as follows :[87]

National Cybersecurity Strategies in Latin America and the Caribbean
Performance levels in 2024

84 *Cf., Cyberpractice: Creating and Conducting Cybersecurity Exercise for the Organizations: cybersecurity best practices* at https://publications.iadb.org/en/cyberpractice-creating-and-conducting-cybersecurity-exercises-organization-cybersecurity-best.

85 *Cf, Reducing Cybersecurity Risks at Organizational Endpoints. A Technical Approach Cybersecurity Best Practices* (2024), available at https://publications.iadb.org/es/publications/spanish/viewer/Reduccion-de-los-riesgos-de-ciberseguridad-en-los-puntos-finales-de-la-organizacion-mejores-practicas-en-ciberseguridad.pdf.

86 *Cf.*, *Global Cybersecurity Index 2024,* available at https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

87 *Global Cybersecurity Index 2024*, p. 26.

T5: under construction	**T4: evolved**	**T3: establishing**	**T2: moving forward**	**T1: refurbished**
Antigua	Argentina	Chile	Ecuador	Brazil
	Bahamas	Colombia	Mexico	
	Barbados	Costa Rica	Uruguay	
	Belize	Cuba		
	Bolivia	Dominican Republic		
	El Salvador	Jamaica		
	Grenada	Panama		
	Guatemala	Paraguay		
	Guyana	Peru		
	Haiti	Trinidad and Tobago		
	Honduras			
	Nicaragua			
	San Cristobal			
	St. Lucia			
	Saint Vincent and the Grenadines			
	Suriname			
	Venezuela			

As can be seen, Latin American and Caribbean states are committed to developing their respective national cybersecurity strategies, although not all are advancing at the same pace, nor do they enjoy the same level of cyber performance or maturity. In general terms, the approved national strategies pursue a common goal: to protect, manage and recover from a cyber-attack in the most effective way and with the fastest possible speed, although each one takes into account the particularities of each State. Argentina, for example, prioritizes the prevention of harmful cyber actions affecting the State administration[88] , although it also contemplates specific provisions linked to

[88] *Cf.*, Office of the Chief of Cabinet of Ministers, Resolution 1/2023 of January 2, 2023, which approves the second National Cybersecurity Strategy, which "includes cybersecurity and the protection of critical information and communication infrastructures associated with the National

technological developments such as the Internet of Things, 5G or cloud services. Costa Rica, for its part, articulates its strategy under a human rights approach, which affects all stakeholders in the construction of an inclusive society in all areas of Costa Rican life .[89]

Only Brazil has achieved the highest level of performance (T1) with its national cybersecurity strategy, as it includes specific measures in the five areas studied and assessed by the *Index* that make up a solid cybersecurity strategy[90] . Among its strategic objectives, Brazil pursues a trusted digital environment, increasing resilience to cyber threats and strengthening Brazil's cybersecurity performance on the international stage[91] . To this end, it establishes ten specific strategic actions, such as strengthening cyber governance actions, raising the level of government protection, improving the legal framework, promoting the design of innovative cybersecurity solutions and increasing the level of maturity of society in cybersecurity

Ecuador, Mexico and Uruguay have reached the T2 level insofar as they satisfy the five levels of measures necessary for good cyber maturity, as assessed by the *Index*, although their respective evaluations confirm that still has room for improvement. Thus, for example, Ecuador's *National Cybersecurity Strategy (2022-2025*) has a very broad scope[92] , affecting all sectors of the country, including the National Government, control bodies, judicial institutions, decentralized autonomous governments, companies, academic entities and financial organizations. Its main objective is to generate a safe cyberspace for citizens that revolves around six lines of action: governance and national coordination; cyber resilience; cybercrime prevention; cyber defense; development of cybersecurity skills and capabilities; and international cooperation. However, national

---

Public Sector and the information and communication services defined in Article 1 of Law No. 27,078" at

89 *Cfr.*, Estrategia Nacional de Ciberseguridad de Costa Rica 2023-2027, at https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf.

90 The performance levels assess whether States provide for five types of measures in their strategies: (i) Legislative measures to harmonize practices at the regional/international level, strengthen cybersecurity systems and simplify international frameworks for combating cybercrime; (ii) Technical measures that guide national institutions with standards and technical frameworks related to cybersecurity and cybercrime; (iii) Organizational measures to promote information sharing and to assess and implement good cybersecurity practices and systems standards for secure ICT; (iv) Capacity building measures, including education programs, training of professionals and public awareness campaigns; and (v) Cooperative measures, which promote partnerships, cooperation frameworks and information sharing networks at the national, regional and global levels.

91 *Cfr.*, *Estratégica Nacional de SeguranÇa Cibernética - E-Ciber*, (Decreto Nª 10.222, de 5 de Fevreiro de 2020, Brasilia 2020) at https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf.

92 Cfr., Ecuador's National Cybersecurity Strategy at https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf.

laws to implement and develop its Strategy have yet to be passed. In similar terms, also Mexico's *National Cybersecurity Strategy (*2017)[93] identifies and establishes the actions in cybersecurity applicable to the social, economic and political spheres that allow the population and organizations to use and take advantage of ICTs in a responsible manner. To this end, it establishes five priority objectives: society and rights, economy and innovation, public institutions, public safety and national security. These objectives will be achieved through eight axes: cybersecurity culture; capacity building; coordination and collaboration; ICT research, development and innovation; technical standards and criteria; critical infrastructure; legal framework and self-regulation; and measurement and monitoring. However, it lacks a single central authority responsible for implementing the cybersecurity actions envisaged in the Strategy. Its institutional framework is highly fragmented and specific responsibilities fall on various federal and local authorities and, in addition, there are specific sectoral strategies, such as the one approved by the navy[94] , with their own objectives and responsible authorities. Mexican practice prioritizes, however, the prevention of attacks against essential State infrastructure and public services insofar as they affect national security .[95]

However, Uruguay's situation is somewhat exceptional. The Uruguayan government has a document called "Cybersecurity Framework", which, despite not being a cybersecurity strategy *per se*, does address how to reduce the risk associated with threats that may compromise information security in organizations. In September 2024, it is almost at the forefront of this T2 level, and closer to Brazil, as the next *National Cybersecurity Strategy (ENC) 2024 - 2030* will soon see the light[96] . Its architecture is

---

93 https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf and at https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

94 Secretary of the Navy, Institutional Strategy for Cyberspace 2021-2024, at

95 For further study of cybersecurity in Mexico, *see* MORALES TENORIO, I., and SALAZAR ALBORNOZ, M., "Normative Framework, Decision-Making and Responses to Cyber Operations: A View from Mexico", in *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, *Rivista Trimestrale della Società Italiana per l'Organizzazione Internazionale,* 2024, pp.181-200; R. C. BERG, H. ZIEMER, The Development of the ICT Landscape in Mexico: Cybersecurity *and Opportunities for Investment, Center for Strategic & International Studies, November 19,* 2021, in .; R. C. BERG, H. ZIEMER, *The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment*, Center for Strategic & International Studies, November 19, 2021, at

96 *Cf.*, his latest draft at https://plataformaparticipacionciudadana.gub.uy/rails/active_storage/disk/eyJfcmFpbHMiOnsibWVzc2FnZSI6IkJBaDdDVG9JYTJWNVNTSWhiM2hyT1RGeWFYZ3phREZ1YnpkamJuTnNPRGhpY1hJMVpqaHZNd1k2QmtWVU9oQmthWE53YjNOcGRHbHZia2tpQVpocGJteHBibVU3SUdacGJHVnVZVzFsUFNKQ2IzSnlZV1J2Y2lCa1pTQnNZU0JGYzNSeVlYUmxaMmxoSUVOcFltVnljMlZuZFhKcFpHRmtJRlZ5ZFdkMVlYa3VjR1JtSWpzZ1ptbHNaVzVoVldVcVBWVlVSaTA0SnlkQ2IzSnlZV1J2Y2lVeU1HUmxKVEl3YkdFbE1qQkZjM1J5WVhSbFoybGhKVEl3UTJsaVpYSnpaV2QxY21sa1lXUWxNakJWY25WbmRXRjVMbkJrWmdZN0JsUTZFV052Ym5SbGJuU

based on eight pillars: governance and regulatory framework, criminalization cybercrimes, strengthening of the cyber defense ecosystem, protection of critical information infrastructures, development of a cybersecurity culture and boosting of a national cybersecurity industry. In addition, in October 2024, the Agency for E-Government and Information and Knowledge Society (Agesic) and the United Arab Emirates (UAE) Cybersecurity Council signed a Memorandum of Understanding to strengthen cooperation between the two countries in the detection and prevention of information security incidents, facilitate the exchange of experience and knowledge, and even develop cybersecurity capabilities. Time will tell how effective this agreement will be in practice.

mZkSGx3WlVraUZHRndjR3hwWTJGMGFXOXVMM0JrWmdZN0JsUTZFWE5sY25acFkyVmZibUZ0WlRvS2JHOWpZV3c9IiwiZXhwIjoiMjAyOS0wOS0xM1QxOTozMzozMi4wOTFaIiwicHVyIjoiYmxvYl9rZXkifX0=--8bbab2adf639263c427a05e38a24947b03760b8d/Borrador%20de%20la%20Estrategia%20Ciberseguridad%20Uruguay.pdf.

As can be seen, according to the *Global Cybersecurity Index*, 10 States (Chile[97] , Colombia[98] , Costa Rica[99] , Cuba[100] , Dominican Republic[101] , Jamaica ,[102] Panama[103] , Paraguay[104] , Peru[105] and Trinidad and Tobago[106]) have already reached the T3 level, This means that national authorities are negotiating their respective national cybersecurity strategies and the national legislative and other measures that will be needed to implement the strategies, although specific legislative work has only just begun.

---

97 *Cfr., Política Nacional de Ciberseguridad 2023-2028*, from Chile at https://ciberseguridad.gob.cl/documents/4430/Pol%C3%ADtica_Nacional_de_Ciberseguridad_2023-2028.pdf.

98 *Cfr.,* Ministry of Information and Communication Technologies of the Republic of Colombia, RESOLUTION No. 00500 of March 10, 2021 "Whereby the guidelines and standards for the digital security strategy are established and the security and privacy model is adopted as an enabler of the Digital Government policy", at

99 *Cfr.*, Estrategia Nacional de Ciberseguridad, Costa Rica 2023-2027, Ministry of Science, Innovation, Technology and Telecommunications (MICITT) at

100 Since 2013, the Office of Security for Computer Networks (OSRI), attached to the Cuban Ministry of Communications, has among its missions the execution of actions aimed at minimizing the risks of Cuban computer networks and the coordination to manage computer incidents at the national level. Despite not having a formal strategy, the Cuban government has approved a whole legal framework to minimize the harmful effects on the network. Thus, for example, it has Decree 360/2019, on the Security of Information and Communication Technologies and the Defense of National Cyberspace. Decree Law 35/2021, on Telecommunications, Information and Communication Technologies and the use of the Radio Spectrum. Law 149/2022 on the protection of personal data and the compendium of rules that accompany it. Resolution 73/2021 Regulation of critical infrastructures. Resolution 105/21 Model of action in the event of cybersecurity incidents. Resolution 128/19 ICT security regulations. Resolution 129/19 Methodology for IT security management. It has also reformed its Penal Code on several occasions to include the criminalization of computer crimes.

101 *The National Cybersecurity Strategy 2030* of the Dominican Republic, which succeeds the National Cybersecurity Strategy of the Dominican Republic 2021-2024 (ENCS), establishes the lines of action to mitigate the risk, minimize the impact of cyber threats and protect the information systems and with special attention to the national critical infrastructures and the relevant IT infrastructures of the Government, to guarantee that the citizens use the services offered through ICTs, confident in their security. The Strategy has four pillars:1) Legal Framework and Institutional Strengthening, 2) Protection of National Critical Infrastructures and Government IT Infrastructures, 3) National Cybersecurity Education and Culture, and 4) National and International Alliances, which aims to establish a mechanism for dialogue and cooperation among all sectors of society to promote best practices, identify common problems and develop appropriate solutions to address cyber threats. At https://cncs.gob.do/wp-content/uploads/2022/07/Decret

102 *Cfr.,* National Cyber Security Strategy, Jamaica, at https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Jamaica%20National%20Cyber%20Security%20Strategy%20(Spanish).pdf

103 Panama's *National Cybersecurity Strategy for the period 2021-2024*, (Official Gazette Digital No. 29434-A Resolution No. 17). It has four fundamental pillars. I: Protect the privacy and fundamental rights of citizens in cyberspace. II: To deter and punish criminal behavior in cyberspace. III: Strengthen the security and resilience of our nation's critical infrastructure. IV: Foster a national culture of cybersecurity. Cfr., https://www.gacetaoficial.gob.pa/pdfTemp/29434_A/88864.pdf

104 *Cfr.*, Plan Nacional de Ciberseguridad: retos roles y compromisos , Paraguay, Secretaria General de Tecnologías de la Información y Comunicación, at .

105 *Cfr.* Estrategia Nacional de Seguridad y Confianza Digital 2021 - 2026, Presidency of the Council of Ministers of Peru, in: https:

106 *Cfr.,* National Cyber Security Strategy 2012, Republic of Trinidad and Tobago https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(Spanish).

However, some common reflections can be drawn from these 10 national strategies as a whole. First, there is no single pattern or model to follow in the articulation of the strategies. Second, the similarities mainly concern the general justification of "guaranteeing a secure and reliable cyberspace", as in the case of the Dominican Republic and Paraguay. Third, there is a diversity of priority objectives, although - logically - there are also important convergences relating to the protection of critical infrastructure (Chile, Jamaica and Trinidad and Tobago); the promotion of a culture of cybersecurity and capacity building in this area (Chile, Panama and Colombia); or the search for greater international commitment and cooperation (Chile, Panama and Jamaica). Fourth, the particularities of some States stand out, which logically respond to their social and legal conditions. For Peru, for example, it is essential to guarantee network access to all its citizens and strengthen digital talent, while Panama emphasizes the search for rapid and effective responses to cyber-attacks. Chile proposes the promotion of industry and scientific research and Costa Rica promotes international cyber-diplomacy. Finally, in fifth place, a common denominator stands out in almost all the strategies: the need to significantly strengthen the criminalization of cybercrime (as in Jamaica, Panama, Costa Rica and Trinidad and Tobago)

However, there are still 17 states in the Latin American region in the so-called T4 level of the *Global Cybersecurity Index*, as they do not have a national cybersecurity strategy in use or because they are still in the initial stages of their configuration. This is the case, for example, of Bolivia[107] , El Salvador, Haiti, Honduras, and Venezuela. For its part, the Government of Venezuela launched a "National Cybersecurity and Cyberdefense Plan" in 2016, the aim of which was to improve cybersecurity measures in the country. El Salvador also deserves a separate mention, as its national cybersecurity strategy is currently in the midst of development[108] . For its part, Belize's *Cybersecurity*

[107] Indeed, the Bolivian government has not developed an official cybersecurity strategy or policy. However, some progress has already been made in this area. In 2013, Bolivia strengthened its national IT infrastructure with the development of a national Internet Exchange Point (IXP), called PIT-BOLIVIA. Critical infrastructure operators have also implemented *ad hoc* security procedures and standards, but there is no formal collaboration between stakeholders in this regard. In 2015, the government supports the work of the Computer Forensics Division of the Technical Scientific Research Institute of the Police University (IITCUP) is in charge of national cybercrime cases. Legislative changes have been introduced in Chapter XI of the Penal Code (established in 1997), which criminalizes the manipulation or illegal obtaining of information on the Internet, and Articles 253 and 254 of the Code of Criminal Procedure establish rules for obtaining electronic evidence. *Cfr.*

[108] Indeed, last November 4, 2024, the Security and Justice Commission of the Government of El Salador initiated the study of the future Cybersecurity and Information Security Law, which aims to establish the principles, legal framework, institutional framework and protection policies that will

Strategy projects three priority pillars: i) developing a national legal framework to address cybersecurity threats; ii) building critical incident response capabilities and proper critical infrastructure protection; and iii) measures to support education, increase user and workforce awareness and develop cybersecurity policies . [109]

Guatemala's *National Cyber Security Strategy* (2022) is a first step in establishing guidelines and objectives for its technological transformation, as set out in Guatemala's National Security Policy. Its objective is to mitigate threats and attacks coming from cyberspace, without losing all the advantages of information technologies; and in case of an incident, it aims to have the necessary resilience to reestablish services in the shortest possible time, avoiding the loss of critical information and major damages. In contrast, Nicaragua's cybersecurity governance model[110] contemplates a set of tools, policies, concepts, guidelines, risk management methods, human talent training, best practices and technologies that can be used to protect the information and assets of the Nicaraguan territory and users in the national cyberspace. However, in the absence of effective preventive mechanisms to protect its critical infrastructure at the national level, the Nicaraguan government signed a cybersecurity cooperation agreement with Russia in 2022 for the period 2022-2026, which has already alarmed some partners in the region.

3. CYBERCRIME AS A FAILED DRIVER OF CYBERSECURITY IN THE OAS

As is the case in Africa, the first regulations in Latin America and the Caribbean related to cyberspace were national laws against cybercrime, but - unlike in Africa - these laws did not aspire to be "model laws" for the OAS as a whole. The first cybercrime law in the region was passed in Chile in 1993, which was strongly inspired by France's Law 88-19[111] . By 2000, Bolivia, Paraguay, El Salvador, Mexico and Peru also had their own cybercrime laws.

---

allow structuring, monitoring, regulating and controlling cybersecurity and security measures held by public institutions. *Cfr.*

109 *Cf., National Cybersecurity Strategy - Towards A Secure Cybers pace 2020-2023*, at https://www.pressoffice.gov.bz/wp-content/uploads/2019/12/belize-cybersecurity-strategy-2020-2023.pdf.

110 *Cf., National Cybersecurity Strategy 2020-2025*, September 29, 2020 of the Republic of Nicaragua, at

111 Cf. PURDON, L., VERA, F., "Regional Cybersecurity approaches in Africa and Latin America", in *Routledge Handbook of International Cybersecurity*, Eneken Tirkk (eds), Taylor&Fancis 2020, pp, 234-246, p. 239.

Beginning in 1999, the Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA) and the Group of Governmental Experts on Cyber-Crime will lead the work on cyber-crime in the region. The periodic meetings of the Group of Experts and the REMJA provide OAS Member States with concrete recommendations on how to combat cybercrime and consolidate hemispheric cooperation in crime prevention in accordance with the principle of state sovereignty, without any limitation on the type or severity of cyberdamage caused. On occasion, the REMJA has even suggested to the States national legislative changes in order to achieve an efficient, agile and effective administration of justice. Thus, for example, in the conclusions of its recent meetings, States are encouraged to establish entities specifically responsible for directing and developing the investigation and prosecution of cybercrime[112] ; to develop and implement national strategies that include efforts to prevent, investigate and prosecute cybercrime[113] or even to consider the possibility of joining the G-7's "24/7 High Tech Crime Contact Network"[114] . For its part, the REMJA Technical Secretariat has been responsible for updating the *Inter-American Cooperation Portal on Cyber-Crime*,[115] which involves the development of a common virtual space for the Americas for the exchange of experiences and best practices among the authorities designated by the States in the area of international legal cooperation for the investigation and prosecution of cyber-crime.

It should be noted, however, that the search for mechanisms to combat cybercrime is present in almost all REMJA meetings. As early as 2003, it was considered desirable to apply the principles of the Council of Europe Convention on Cybercrime (2001), and subsequently, in 2008, it proposed to the States to adhere to this Convention. Again, in 2022, OAS member states that had not yet done so were encouraged to consider acceding to the Budapest Convention and to adopt legal and other measures necessary for: i) cyber capacity building; ii) the generation of evidence on cybercrime; iii) legal cooperation on cybercrime; and, iv) regulatory development in the field .[116]

---

112 OEA/Ser.K/XXXIV CIBER-X/doc.3/22 rev.2 29 April 2022, item 1, of the Tenth Meeting of the Working Group on Cyber-Crime and Meetings of Ministers of Justice or other Ministers or Attorneys General of the Americas, at

113 *Ibid.*, point 6.

114 *Ibid*., point 8.

115 Cf., https://www.oas.org/es/sla/dlc/cyber-es/homePortal.asp

116 OEA/Ser.K/XXXIV CIBER-X/doc.3/22 rev.2 29 April 2022, item 13, of the Tenth Meeting of the Working Group on Cyber-Crime and Meetings of Ministers of Justice or other Ministers or Attorneys General of the Americas.

Acceptance of the Budapest Convention in Latin America has been slow and conflictive. At present, Argentina, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, Panama, Paraguay and Peru have formally acceded to the Convention, while Ecuador, Guatemala, Mexico and Uruguay are invited to do so. On the other hand, the States that do not intend to accede to the Convention justify this on the grounds of the markedly European nature of the conventional instrument[117] . Given this reality, and to ensure legal harmonization among the members of the OAS, REMJA does not rule out proposing to the States to identify common parameters and principles that would bind them, with the idea that in the immediate future the OAS would draw up its own regional conventional instrument, as the Council of Europe did in 2001 (Budapest Convention), and the African Union in 2014 (Malabo Convention)

This future Latin American treaty would be the culmination of the *Inter-American Comprehensive Strategy to Combat Threats to Cybersecurity: for the Creation of a Culture of Cybersecurity*[118] of 2004, and should aim to create a new legal framework to effectively combat cybercrime in the American hemisphere[119] . Now, more realistically and as a step prior to the possible future treaty, the REMJA proposed in 2021 to reconvene the Working Group on Legal Cooperation in Criminal Matters to delve into the 2015 proposal by Chile, Brazil, Canada and Peru to adopt a specific Protocol on cybercrime[120] in the context of the Inter-American Convention on Mutual Assistance in Criminal Matters Concerning the Use of New Communication Technologies and Hearing by Videoconference[121] . This proposal, however, does not seem to have taken hold in the diplomatic agendas of the American foreign ministries, at least to date.

It is clear from the above that, for Latin American and Caribbean States, the fight against cybercrime plays a central role in the context of cybersecurity[122] . However, the

---

117 *Cf.*, PURDON, L., VERA, F., "Regional Cybersecurity, ... *op. cit.,* p. 242.

118 Resolution AG/RES. 2004 (XXXIV-O/04) "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to the Creation of a Culture of Cybersecurity".

119 *Cf.,* FASCIGLIONE M., NINO, M., "The activity of the Organization of American Stares in the field of Cybersecurity", in *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*,.... *op. cit*. p. 264.

120 *Cf.,* OEA/Ser.K/XXXIV.11 REMJA-XI/DOC.2/21 rev.1 May 19, 2021, item 7. (PENAL/doc.31/15 rev. 3). of the Eleventh Meeting of Ministers of Justice or Other Ministers or Attorneys General of the Americas, at

121 Known as the Nassau Convention, the Inter-American Convention on Mutual Assistance in Criminal Matters, adopted in 1992, is the most important and most useful Convention for the criminal justice operator in the Inter-American area to request legal assistance, since it has been ratified by 27 OAS Member States and because it provides a broad legal basis for their requests for assistance.

122 *Cfr.,* SALINAS CAÑAS, S., RIQUELME RIVERA, J., "La Ciberdefensa como parte integrante de la agenda de integración sudamericana", *Línea Sur*, 2015, pp. 100-116.

REMJA recommendations on the use of technologies to make the administration of justice and the fight against cybercrime more effective, efficient and expeditious remain just that, mere recommendations for the future - real *soft law* - which are still far from becoming a Latin American legal instrument - real *hard law* - that harmonizes international and regional legal cooperation in the fight against cybercrime.

4. FINAL CONCLUSIONS

Taking into account the preceding analyses, it can be affirmed without any doubt that African and Latin American approaches to cybersecurity contribute effectively to the governance of cybersecurity and the identification of the legal regime applicable to cyberspace. This is so, because, the *African Common Position on the applicability of international law to cyberspace* represents the *opinio iuris* of 28.5% of the votes of the UN General Assembly and the 2022 report of the Inter-American Juridical Committee reflects, for its part, the position of 18% of the votes in the Assembly. Moreover - as described in the preceding paragraphs - both regions defend the full applicability of the principle of State sovereignty and the sovereign equality of States in the face of the challenges of ICTs without any restrictions whatsoever

In general terms, there has been a notable evolution in cyber maturity and a medium level of development of national cybersecurity strategies in each region, although there is still room for improvement. According to the 2024 *Global Cybersecurity Index*, 39% of African states have already developed national cybersecurity strategies, compared to 26% of Latin American and Caribbean states. These data contrast with the shares achieved in the European Union, with 76% of its Member States already having national cybersecurity strategies[123] . The main obstacles faced by the OAS are due in part to the very formalistic legal traditions of some States, which hinder collaboration between the various State actors in the absence of clear legal mandates. In the AU, the challenge focuses - now more than ever - on achieving greater investment in cyber law enforcement capabilities (people, processes and technologies), creating synergies within the cybersecurity ecosystem, raising public awareness and strengthening international and regional cooperation.

[123] *Cf., Global Cybersecurity Index 2024,* p. 11, figure 9, available at https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

African and Latin American and Caribbean states have an unwavering commitment to their cybersecurity, which takes different forms. While the African Union is committed to the adoption of mandatory and binding norms for its member states, such as the adoption of the Malabo Convention, the Organization of American States follows the path of recommendations, non-binding acts and the creation of contact groups or networks to advance collaborative and dialogic cybersecurity. In both regions, however, there is a disproportionate focus on national cybercrime legislation and a neglect of the technical aspects and good practices of actual cybersecurity. In Africa, control of the online space and surveillance is particularly sought after, rather than securing systems. In Latin America and the Caribbean, the regional emphasis is on the creation of technical response teams and capacity building based on available financial resources. As a result, all kinds of activities are being developed in both regions for cyber-skills training, thanks to international and regional cooperation to provide a united front against the global threat of cybercrime. Behind these efforts lies the geopolitics of certain states, such as China, Russia, Israel or the United Arab Emirates, to extend or consolidate their power.

However, in the face of progress in the legal shaping of a comprehensive and robust cybersecurity system, another fundamental question arises, which is still unresolved. For cybersecurity to be an essential and real part of "international peace and security", more attention should be paid to regional approaches and their particular challenges. Regional positions will always have a positive impact, as they bring diversity in responses, as was the case with the Malabo Convention. The lack of consideration of regional approaches is not a legal problem, but a political one. Other regions and large states - such as the so-called "technology giants" - refuse to move forward with international regulation of the Internet out of purely strategic interest or take advantage of local loopholes to extend their influence and dependence by supplying invasive technology without adequate safeguards.

Bibliography

AGUILAR ANTONIO, J. M., "La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas", *Revista de Estudios de Seguridad Internacional*, vol. 6 (2), 2020, pp. 17-43.

ATANDI, F., *Crossing the Digital Divide: Kenya's Cyber Security Journey*, February 24, 2024, at https://medium.com/@usalamasecure/crossing-the-digital-divide-kenyas-cyber-security-journey-322bb844e888.

BERG, R. C. and ZIEMER, H., *The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment*, Center for Strategic & International Studies, November 19, 2021, at https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment.

BUCHAN, R., and TSAGOURIAS, N., "The African Union's Statement on the Application of International Law to Cyberspace: An Assessment of the Principles of Territorial Sovereignty, Non-Intervention, and Non-Use of Force," EJIL Talk, February 20, 2024.

CERVELL HORTAL, M.J. and PIERNAS LÓPEZ, J. J. (dirs), *Hacia una regulación internacional de para el ciberespacio*, Thomson-Aranzadi, Pamplona, 2023.

CHARLITA DE FREITAS, L., IÓRIO ARANHA, A., "The instrumentalization of responsive regulation and its relative efficiency: experiences of the Brazilian National Telecommunications Agency", *Revista Latinoamericana de Economía y Sociedad Digital*, vol. 4, 2024, pp. 160-191.

DELBRÜCK, J., "Article 24", in *The Charter of the United Nations. A Commentary*, Bruno Simma (ed.), Oxford University Press, Oxford, (1995), pp. 397-407.

ENEKEN, T; MIKA, K., *Routledge Handbook of International Cybersecurity*, Routledge, 2020.

FASCIGLIONE M. and NINO, M., "The activity of the Organization of American Stares in the field of Cybersecurity", in *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, *Rivista Trimestrale della Società Italiana per l'Organizzazione* Internazionale, 2024, pp. 249-264.

GIACOMELLO, G, (ed.) *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals*. New York: Bloomsbury Academic, 2014.

HELAL, M., "Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, and all associated Communiqués adopted by the Peace and Security Council of the African Union (February 2024)", *Ohio State Legal Studies Research Paper,* No. 823*,* at https://ssrn.com/abstract=4714756 or http://dx.doi.org/10.2139/ssrn.4714756.

HELLER, K.J., "In Defense of Pure Sovereignty in Cyberspace", *International Law Studies,* vol. 97, 2021, pp. 1432-1499.

HUREL, L.M., "Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America", *Global Security Review*, Volume 2, January (2022), pp. 21-31.

LÓPEZ-JACOISTE DÍAZ, E., "La Cooperación de la Unión Europea para la construcción de la ciberseguridad en América Latina y el Caribe", in Cervell Hortal, M. J. and Piernas López, J. J. (dirs.), *Hacia una regulación internacional para el ciberespacio,* Aranzadi, Cizur Menor 2023, pp. 317-354.

MORALES TENORIO, I., and SALAZAR ALBORNOZ, M., "Normative Framework, Decision-Making and Responses to Cyber Operations: A View from Mexico", in *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, *Rivista Trimestrale della Società Italiana per l'Organizzazione Internazionale*, 2024, pp.181-200.

MORENO, J., ALBORNOZ M. M., and MAQUEO, M. S., "Ciberseguridad: estado de la cuestión en América Latina", *Revista de Administración Pública* INAP, vol. LIV, no.1, 2020, pp. 23-26.

ORJI, U., Tthe African Union Convention on cybersecurity: a regional response towards cyber stability?", *Masaryk University Journal of Law and Technology*, vol. 12, 2018, pp. 91-127.

PURDON, L. and VERA, F., "Regional Cybersecurity approaches in Africa and Latin America", in *Routledge Handbook of International Cybersecurity*, Eneken Tirkk (eds), Taylor&Fancis 2020, pp. 234-246.

ROGUSKI, P. "Application of International Law to Cyber Operations: A Comparative Analysis of States' views", *Policy Brief*, The Hague Program for Cyber Norms, Universiteit Leiden, (2020), p. 4, at https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views.

SALAZAR ALBORNOZ, M., "The Inter-American Juridical Committee facing the challenges of the digital era: the rapporteurships on privacy and protection of personal data and on international law applicable to Cyberspace," *Electronic Journal of Contemporary International Law*, 2022, vol. 5, https://doi.org/10.24215/2618303Xe042

SCHMITT M. N. and VIHUL, L., "Respect *for Sovereignty in Cyberspace," Texas Law Review*, vol. 95, 2017, p. 1639.

SCHMITT, M. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.

Id. "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chinese Journal of International Law*, vol. 19, 2018, pp. 30, 40, 42-43.

TERRY, P. C., " Cyber Espionage and Public International Law: The African Union Rejects the Tallinn Manual's Relativist Approach to Cyber Sovereignty," *Online Scholarship, Perspectives*, dated May 4, 2024, at https://journals.law.harvard.edu/ilj/2024/05/cyber-espionage-and-public-international-law-the-african-union-rejects-the-tallinn-manuals-relativist-approach-to-cyber-sovereignty/.

TSAGOURIAS, N. and BUCHAN, R. (eds.), *Research Handbook on International Law and Cyberspace,* Edward Elgar Publishing, UK 2021.

VAN DER BERG, B., *Governing cyberspace: behavior, power and diplomacy*, Lanham; Boulder; New York; London: Rowman & Littlefield, 2020.

VERNIER, S., "The Common African Position on the Application of International Law to the use of information and Communication technologies in cyberspace", *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, *Rivista Trimestrale della Società Italiana per l'Organizzazione Internazionale*, 2024, pp. 291-308.

VILA SEOANE, M., "La ciberhegemonía de EEUU en la OEA", *Estudos Internacionais,* vol. 10, 2023, pp. 91-112.

VON HEINEGG, W., *Territorial Sovereignty and Neutrality in Cyberspace*", *International Law Studies*, vol. 89, 2013, p. 123.

YILMA, K.M., "Ethiopia`s new cybercrime legislations: some reflections", *Computer Law & Security Review*, vol. 33, 2, April 2017, pp. 250-255.

Sino-Russian strategic partnership in the "information space".

Irene Vázquez Serrano
Permanent Lecturer in Public International Law and International Relations
University of Murcia

SUMMARY. I. INTRODUCTION. II. RUSSIAN AND CHINESE STRATEGIES ON CYBERSPACE. 1. The Information Security Strategy of the Russian Federation. 2. China's International Strategy for Cooperation in Cyberspace. III. IS IT POSSIBLE TO AFFIRM THE EXISTENCE OF A STRATEGIC CHINESE-RUSSIAN PARTNERSHIP IN CYBERSPACE? IV. A BRIEF (BUT OBLIGATORY) LOOK AT THE RUSSIAN "SPECIAL MILITARY OPERATION" IN UKRAINE THROUGH CYBERSPACE. V. CONCLUSIONS. VI. BIBLIOGRAPHY.

I. INTRODUCTION

The new cybernetic domain, known in the West as *cyberspace*, is known in the Asian region under the name of domain or *information space*[1] . In relation to international law, there are several aspects that today can be analyzed from this new *binomial*[2] , not

[1] "At no time do the Chinese leaders or military use the term "cyberspace", it being clear from Chinese theoretical discourse that, while the West considers that there are five domains (land, sea, air, space and cyberspace), in China, for its part, cyberspace is distinguished as the union and interaction of two distinct areas: on the one hand, as it refers to electromagnetic *space* (*electromagnetic space*), and on the other, from the perspective of informatization (*informationization*; *xinxihua*). In this respect, electromagnetic space would include all those aspects linked to electronic systems (linked to electronic warfare -*electronic* or *electromagnetic dominance*-; *zhi dianzi quan*); and informationization would include the integration of information technology systems from a broad perspective. In summary, we could state that China understands cyberspace under the term "information domain" (*zhi xinxi quan*); which includes the "computer network domain" -electromagnetic- (*zhi wangluo quan*) and the informatization domain (*informationization*; *xinxihua*) (...).In synthesis, we can affirm that China understands the interaction of kinetic, political and information domain activities as a unified whole in the projection of its military muscle, as the Asian giant understands that future conflicts will take place in a multi-domain environment. Mainly, there are three Chinese concepts to be taken into account in the doctrine of the Asian giant regarding its information domain (zhi xinxi quan) -translated in the West as cyberspace: "informationized warfare" (xinxihua zhanzheng), "information warfare" (information warfare) and "information operations" (information operations)" (EXPÓSITO, J., "El dominio de la información: el ciberespacio visto desde China. Estudio sobre las implicaciones geopolíticas del dominio de la información", *Ejércitos. Revista digital sobre defensa, armamento y fuerzas armadas*, no. 66, 2023, available at https://www.revistaejercitos.com/articulos/el-dominio-de-la-informacion-el-ciberespacio-visto-desde-china/).

[2] "We are facing a new challenge (one more) that today's international society is facing: the new *international law-cyberspace* binomial. A binomial that demands increasingly urgent attention, either to develop specific rules that address the most innovative issues that arise in cyberspace, or to implement an adaptation of existing rules to the peculiar characteristics of this" (VÁZQUEZ

only because of the peculiarities that cyberspace presents in relation to the classic domains, but also because of the particular vision that the different States have expressed in relation to application of international law to it.

In recent years, this domain has been (and, we predict, will continue to be) a challenge for States, which will entail major security challenges not only nationally, but also globally, given the interconnection and absence of borders in this domain, which will allow even States with unequal capabilities to act. Thus, the main threats of concern in terms of cybersecurity can be centered on cyberattacks, control of information by certain state actors and disinformation . [3]

Cybersecurity has therefore become one of the primary concerns for international society and China and Russia have not been left out of the threats and challenges posed by the new pairing, hence their eagerness to "develop hegemony" over the cyber domain by establishing "strict cybersecurity laws in order to have greater control over the flow of information on the network to safeguard national interests"[4] , investing a large amount of national budget for this purpose[5] . Their cybersecurity policies, as it will be seen, are close in many aspects, being the Shanghai Cooperation Organization (hereinafter, SCO)[6] , the

SERRANO, I., *Una aproximación al concepto de neutralidad en el ciberespacio*, Tirant lo blanch, Valencia, 2025, in press).

3 SCHREIBER, Ch., "The Future of China and Russia as Allies in Cyberspace," *Journal of International Security Studies*, no. 2, 2019, available at https://www.seguridadinternacional.es/?q=es/print/1606. Indeed, in a 2018 joint statement on information and telecommunications, Canada, Japan, New Zealand and several other states emphasized that "cyber threats should not be used to [...] hinder the free flow of information" (*Joint Statement on Information and Telecommunications in the Context of International Security*, Government of Canada, Press Release, 26 October 2018, available at https://www.international.gc.ca/world-monde/international_relations-relations_internationales/un-onu/statements-declarations/2018-10-26-info_telecommunications.aspx?lang=eng).

4 SCHREIBER, Ch., *op. cit*, note 3. In fact, both Russia and China have seen in cyberspace "the ideal terrain to attack a superior enemy in classical terms of military power such as the United States, and more importantly, to do so in peacetime without elevating the conflict to the category of war" Thus, "cyberspace constitutes an ideal arena for the application of gray zone conflict, as it allows states to achieve their foreign policy objectives without getting directly involved in a conflict, acting through non-state actors (hacker-for-hire groups) or taking advantage of the difficulty of attributing authorship of a cyber-attack" (EXPÓSITO, J., "El dominio de la información...", *op. cit*., note 1).

5 "Russia-China to invest in hi-tech development," *Reuters*, September 11, 2018, available at https://www.reuters.com/article/us-russia-china-investment/russia-china-to-invest-in-hi-tech-development-idUSKCN1LR03F/; and ZILBERMAN, B., "Don't Underestimate Economic Side of Russia's Cyber Warfare," *The Cipher Brief*, June 25th, 2018, available at https://www.thecipherbrief.com/column_article/dont-underestimate-economic-side-russias-cyber-warfare.

6 The Shanghai Cooperation Organization, founded in Shanghai on June 15, 2001, is an intergovernmental organization currently comprising eight member states (China, India, Kazakhstan, Kyrgyzstan, Russia, Pakistan, Tajikistan and Uzbekistan), four observer states interested in full membership (Afghanistan, Belarus, Iran and Mongolia) and six "Dialogue Partners" (Armenia, Azerbaijan, Cambodia, Nepal, Sri Lanka and Turkey). Among its main functions is regional security

means that both States have chosen to make their proposals[7] , not only to the rest of the member States of that organization, but also to those of the United Nations (hereinafter, UN)[8]

China and Russia, along with the United States, have been considered "cyber standards entrepreneurs"; that is, actors who often offer their own versions of standards, actively participate in Internet governance discussions in various forums, and seek allies to support their positions[9]

However, it is unlikely that a single comprehensive regime on *the rules of the game* for cyberspace will be achieved soon due to persistent disagreement among UN member states.

---

and development, focusing on issues such as combating regional terrorism, ethnic separatism and religious extremism (available at https://dppa.un.org/es/shanghai-cooperation-organization).

7 "China and Russia have promoted their preferred norms in the SCO, while the United States and its partners have advanced their vision of cyber norms through the Tallinn Manual, which outlines the applicability of international law in cyberspace" (POETRANTO, I., LAU, J. & GOLD, J., "Look south: challenges and opportunities for the 'rules of the road' for cyberspace in ASEAN and the AU", *Journal of Cyber Policy*, vol. 61, 2021, pp. 318-339, p. 325, available at https://www.tandfonline.com/doi/full/10.1080/23738871.2021.2011937). "States generally seek to promote the version of the rules that best suits their interests. But states' views of the ICT environment depend, at least in part, on their levels of economic development and their cybersecurity capabilities. That is, the more a state's economy depends on ICT and the more capacity it has in ICT use in general, the more likely it is to invest in standards discussions. This strategic calculus may also lead governments to use different forums to develop and socialize norms or to focus on specific norms, or aspects of certain norms, rather than others (FINNEMORE, M. & HOLLIS, D. B., "Constructing Norms for Global Cybersecurity," *American Society of International Law*, vol. 110, no. 3, 2016, pp. 425-479, p. 466, available at https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf)."

8 Thus, already in 2015 the SCO published the *Rules of Conduct in the Area of Information Security*, which includes the general lines relating to information security or cybersecurity. This document describes the objective of the proposal: to identify the rights of States in cyberspace, to promote and build responsible behavior in cyberspace, to cooperate for the resolution of similar problems in the field of information and communication technologies in order to facilitate social development, the welfare of people and ensure peace and security (*Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, UN General Assembly, session no. 69, item no. 91, p. 4 available at https://digitallibrary.un.org/record/786846?v=pdf).

9 MURER, T. & MORGUS, R., "Tiping the Scale: An Analysis of Global Swing States in the Internet Governance Debate," *Global Commission on Internet Governance*, No. 2, June 2014, pp. 1-32, p. 13, available at https://www.cigionline.org/static/documents/gcig_paper_no2.pdf). States may choose to be norm entrepreneurs to shape the framework or interpretation of norms, but those that are highly connected to the Internet would also have an incentive to be cyber norm entrepreneurs, as they face greater risks (as well as reap enormous benefits) from the development and use of ICTs. Standards entrepreneurs may emerge to promote agreement when standards are tested, due to the lack of a universally accepted set of standards, disagreement about the key concepts that make up the standard or how to implement them (FINNEMORE, M. & HOLLIS, D. B., *op. cit*., note 7, pp. 437-438, available at https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf). Non-compliance with cyber norms by certain actors and the lack of clear mechanisms to monitor and report on compliance also discourages compliance (BROWN, D., ESTERHUYSEN, A. & KUMAR, S., "Unpacking the GG's framework on responsible state behavior: Cyber norms", *Global Partners Digital*, 2019, pp. 1-9, p. 2, available at https://www.gp-digital.org/wp-content/uploads/2019/12/unpacking_gge_cyber-norms.pdf).

"Therefore, fragmented efforts can be expected to continue, in addition to the challenges posed by fragmentation of authority and accountability."[10] .

In the following, without intending to be exhaustive, we will focus on the analysis of those issues that both China and Russia have highlighted in their official positions in relation to the regulation of cyber domain by international law in order to then focus the study on those points that separate them and thus assess the existence of a possible cyber alliance between the two States.

II. RUSSIAN AND CHINESE STRATEGIES ON CYBERSPACE

Since the 1990s, the Internet began to be increasingly commercialized and used. It was then that the governments of most states began to understand that there was a need to establish a set of rules and principles that could ensure the accountability of state actions in the new cyber domain.

On December 4, 1998, Russia became the first state to push for a resolution at the UN General Assembly calling on member states "to promote multilateral consideration of current and potential dangers in the field of information security"[11] . Two years later, the Secretary General of the United Nations reported on the "Principles concerning international information security" that had been submitted by only three states, namely the Russian Federation, Jordan and Qatar. These principles included the principle of non-interference in the internal affairs of states and the request that the UN "identify the defining characteristics of information warfare and classify them"[12] .

In 2004, the UN General Assembly created the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of

---

10 DUNN CAVELTY, M. & WENGER, A., "Cyber security meets security politics: complex technology, fragmented politics, and networked science," *Contemporary Security Policy*, vol. 41, no. 1, pp, 5-32, p. 24, available at https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1678855.

11 In the above-mentioned resolution, the General Assembly "invites all Member States to provide the Secretary-General with their views and comments on the following issues: (a) general assessment of information security problems; (b) identification of basic criteria related to information security, in particular unauthorized interference with or unlawful use of information and telecommunication systems and information resources; c) desirability of developing international principles to enhance the security of global information and telecommunication systems and to assist in combating terrorism and information crime", further deciding to include the item at its next session (*Developments in the field of informatization and telecommunications in the context of international security*, Resolution adopted by the General Assembly, 4 January 1999, A/RES/53/70, available at https://documents.un.org/doc/undoc/gen/n99/760/06/pdf/n9976006.pdf).

12 *Developments in Computerization and Telecommunications in the Context of International Security,* Report of the Secretary-General, 10 July 2000, A/55/140, available at https://undocs.org/Home/Mobile?FinalSymbol=A%2F55%2F140&Language=E&DeviceType=Desktop&LangRequested=False.

International Security (hereinafter GGE), in a further attempt to develop a set of principles for responsible state behavior in cyberspace, which states joined on the basis of equitable geographical representation and to which they traditionally send expert representatives[13] . The work of the GEG has laid the groundwork for the *rules of the game* applicable in cyberspace, noting in its 2013 report the applicability of international law to state cyber actions[14] and in the 2015 report a draft with eleven voluntary, non-binding norms for state behavior in cyberspace .[15]

---

13 "The GGE has included the five permanent members of the UN Security Council, liberal democracies, and nonaligned nations" (HURWITZ, R., "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interest*, vol. 36, 2014, pp. 322-331, p. 325).

14 "International law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment" (*Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98, June 24, 2013, para. 19, available at www.un.org/ga/search/view_doc.asp?symbol=A/68/98). See, also, Gary CORN and Robert TAYLOR ("Both *jus ad bellum*, reflected in Article 2(4) of the UN Charter, and customary international law and the rule of non-intervention in international law are well-recognized binding norms applicable to inter-State relations. There is general consensus that *jus ad bellum* fully applies to cyber activities that rise to the level of use of force") "Sovereignty in the Age of Cyber", *American Journal of International Law Unbound*, No. 111, pp. 207-212, pp. 207-209 and BERMEJO GARCÍA, R. and LÓPEZ-JACOISTE DÍAZ, E., *La ciberseguridad a la luz del Jus ad Bellun y del Jus in Bello*, Eunsa, Navarra, 2020, pp. 16 et seq. On the unquestionable application of international law to cyberspace, see: GUTIÉRREZ ESPADA, C., "La ciberguerra y el Derecho internacional", in MARTÍNEZ PÉREZ, E. J. (coord.), MARTÍNEZ CAPDEVILA, C., ABAD CASTELOS, M. and CASADO RAIGÓN, R. (dirs.), *Las amenazas a la seguridad internacional hoy*, Tirant lo Blanch, Valencia, 2017, pp. 205-233; by the same author, "¿Existe (ya) un Derecho aplicable a las actividades en el ciberespacio?", in CERVELL HORTAL, Mª. J. (dir.), *Nuevas tecnologías en el uso de la fuerza: drones, armas autónomas y ciberespacio*, Aranzadi, Cizur Menor, 2020, pp. 225-248, pp. 238-244; KETTEMAN, M. C., "Ensuring cybersecurity through international law", *Revista Española de Derecho Internacional*, vol. 69, no. 2, 2017, pp. 281-289, p. 286; NEUMAN, N., "Neutrality and Cyberspace: Bridging the Gap between Theory and Reality", *International Law Studies*, vol. 97, 2021, pp. 765-802, p. 799, pp. 779; and SEGURA SERRANO, A., "Ciberseguridad y Derecho internacional", *Revista Española de Derecho Internacional*, vol. 69, no. 2, 2017, pp. 291-299, p. 292.

15 "Building on the work of the previous Groups, and guided by the Charter and the mandate contained in General Assembly resolution 68/243, the present Group offers the following non-exhaustive views on how international law applies to the use of ICTs by States: (...) (d) The Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction" (*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, 22 July 2015, para. 28, available atwww.un.org/ga/search/view_doc.asp?symbol=A/70/174). While some States have spoken out against the application of IHL to cyberspace: "This was, in fact, one of the grounds for the failure to reach a consensus report in the 2017 meeting of this forum. *See*, *e.g.*, The Ministry of Foreign Affairs of the Russian Federation, Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere, June 29, 2017, available at https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288; Michael RODRIGUEZ, Representative Of Cuba, Declaration at the Final Session Of Group Of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Just Security*, June 23, 2017, https://www.justsecurity.org/wp-content/up-loads/2017/06/Cuban-Expert-Declaration.pdf; SCHMITT, M. N. & VIHUL, L., "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norm," *Just Security,* June 30, 2017, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/; SCHMITT, M. N., "Norm-Skepticism in Cyberspace? Counter-Factual and

However, under the German chairmanship, the GEG failed in 2017 to reach consensus for the conclusion of the report, primarily in relation to "how international law applies to the use of information and communications technologies by states" in cyberspace. Specifically, Cuba[16] , Russia and China opposed the issues of self-defense, International Humanitarian Law (hereinafter IHL) and countermeasures to cyberattacks[17] , understanding that including provisions on these issues "would lead to a militarization of cyberspace", betting on "peaceful settlement of disputes and conflict prevention" and requesting a "legally binding international instrument" in the face of Western states pointing out that.

> "clear statements of international legal frameworks would precisely help reduce the risk of conflict by creating state expectations of how states can and cannot respond to cyber incidents they face"[18] .

In December 2018, the UN General Assembly adopted two new resolutions: one to re-establish the GEG[19] and the other to constitute the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter OEWG)[20] , which concluded its sessions in 2021 with

---

Counterproductive," *Just Security,* February 28, 2020, https://www.justsecurity.org/68892/norm-skepticism-in-cyberspace-counter-factual-and-counter-productive/ . On the principles contained in the 2015 GEG report, see: CERVELL HORATL, M.ª J., "Normas internacionales para el ciberespacio: tan lejos, tan cerca", BERTOT TRIANA, H. (dir.), *El Orden Jurídico Internacional ante las vicisitudes del siglo XXI*, Tirant lo blanch, Valencia, 2024, pp. 17-38, pp. 31 et seq.

16 Only Cuba made public the statements made by its representative: https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf.

17 The application of countermeasures, especially collective countermeasures, in cyberspace (their nature and scope, as well as substantive and procedural requirements) has been analyzed by Professor Juan Jorge PIERNAS LÓPEZ who, contrary to the positions held by Russia and China, concludes that they are lawful and must comply with the requirements of international law" (*El Derecho internacional y las contramedidas cibernéticas*, Navarra, Aranzadi, 2025).

18 These differences could mark "the end of years of slow but steady progress, something that will be more than desperately needed in light of the differences that led to the outcome of the current GGE (KORZAK, E., "UN GGE on Cybersecurity: The End of an Era? What the apparent GGE failure means for international norms and confidence-building measures in cyberspace," *The Diplomat*, July 31, 2017, available at https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/).

19 *Promoting Responsible State Behavior in Cyberspace in the Context of International Security*, Resolution adopted by the General Assembly on 22 December 2018, A/RES/73/266, available at https://documents.un.org/doc/undoc/gen/n18/465/05/pdf/n1846505.pdf.

20 The OEWG was created "with a view to making the United Nations negotiating process on security in the use of information and communication technologies more democratic, inclusive and transparent, an open-ended working group, acting by consensus, which will further elaborate as a matter of priority the rules, norms and principles of responsible behaviour of States (....) as well as related implementation modalities" (*Developments in the field of information and telecommunications in the context of international security*, Resolution adopted by the General Assembly on 5 December 2018, A/RES/73/27, available at https://documents.un.org/doc/undoc/gen/n18/418/08/pdf/n1841808.pdf). While the GEG 2019-2021 limits the number to twenty-five rotating member states, the OEWG allows

a report adopted by all member states that, however, did not lead to progress in the adoption of global norms about the regulation of cyberspace due to varying state positions.

> "While China, Russia and their partners want a binding framework to govern state behavior, the United States, Canada and their allies argue that UN member states should focus on building on the existing *body of* international law and voluntary, non-binding norms."[21] .

Later, in 2021, the General Assembly approved,

> "with a view to ensuring the uninterrupted and continuous nature of the democratic, inclusive and transparent process of negotiation on security in the use of information and communication technologies, under the auspices of the United Nations, a new open-ended working group on security and the use of information and communication technologies for the period 2021-2025"[22] .

---

the participation of all interested UN member states. Of the 193 UN member states, only forty states have participated in the GEG, and only half of them have been members of more than one GEG (TIKK, E. & KERTTUNEN, M., *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, Cyber Policy Institute, 2017, pp. 38-39, available at https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf). The OEWG thus greatly expands the opportunity for all governments to gain knowledge and exchange ideas on cyberspace security issues.

21 This OEWG report was an achievement due to the large number of governments and actors involved, which had "analysis from Indonesia, Kenya, Singapore and South Africa, as well as ASEAN and the AU", noting that what is offered in this document is only a first step towards a better understanding of the regional challenges and opportunities for advancing the "rules of the game" for cyberspace. A more thorough examination of the positions of other regional institutions and countries of the Global South in the OEWG and their potential impact on the future of cyberspace governance is needed" (POETRANTO, I., LAU, J. & GOLD, J., *op. cit.*, note 7, p. 332). Thus, the report failed to meet the main objectives that the OEWG had set for itself: to "further develop the rules, norms and principles of responsible behaviour by States [...] and the means for their implementation" (UN General Assembly 2018, 5). Perhaps the most glaring omissions in the OEWG consensus report are the lack of references to international responsibility and IHL, both of which are fundamental to preserving security and stability in cyberspace (POETRANTO, I., LAU, J. & GOLD, J., *op. cit.*, note 7, pp. 318 and 321-322).

22 The group, which will operate by consensus, has among its functions to further develop, as a matter of priority, the rules, norms and principles of responsible behaviour of States, as well as the modalities of implementation thereof, and, if necessary, to introduce changes or develop additional rules of behaviour; to examine the initiatives of States aimed at ensuring security in the use of information and communication technologies; to engage, under the auspices of the United Nations, in a regular institutional dialogue with broad participation of States; to continue to study, with a view to promoting common understanding, current and potential threats in the field of information security, including data security, and possible cooperative measures to prevent and counteract such threats, and how international law applies to the use of information and communication technologies by States, as well as confidence-building and capacity-building measures; and to submit to it at its eightieth session, for adoption by consensus, annual progress reports and a final report on the results of its work." In addition, the OWG 2021-2025 may decide to establish thematic subgroups, as deemed necessary by Member States, with a view fulfilling its mandate and facilitating the exchange of views among States on specific issues related to its mandate, and may decide to interact, as appropriate, with other stakeholders, including business, non-governmental organizations and academia (*Advances in the field of information and telecommunications in the context of international security*, resolution adopted by the United Nations General Assembly, 31 December 2020, pp. 3 and 4, paras. 1 and 4, A/RES/75/240, available at https://documents.un.org/doc/undoc/gen/n21/000/29/pdf/n2100029.pdf).

However, in parallel to the work carried out by the groups established within the United Nations and in view of the lack of consensus in the OEWG, other regional international organizations make other *forums* available to various state and non-state actors to continue debating the regulation of cyber domains, making an effort to continue the deliberations on a smaller and more manageable scale and, although they cannot replace the UN mandate, they can help to adopt more specific agreements that, in any case, could lead to the adoption of global agreements . [23]

1. THE INFORMATION SECURITY STRATEGY OF THE RUSSIAN FEDERATION

The first *Information Security Strategy of the Russian Federation* (hereinafter referred to as ESNR) was published in 2016 and described Russia's interests in cyberspace[24] . Specifically, it states that the Russian interest is focused on (i) protecting human and civil constitutional rights and their freedoms and mechanisms of interaction with the state; (ii) keeping the information infrastructure, especially the critical information of the Russian Federation and the telecommunication network operational during peace and in case of a threat of aggression during war; (iii) continuing the development of the information and communication technologies (hereinafter, ICT) sector and improving production, research, social and scientific communities in the sector, and providing information security services; (iv) to also provide the Russian and international community with reliable information on the state policies of the Russian Federation and its official position on significant events in Russia and the world and to use information technologies to ensure the national security of the Russian state in the sphere of culture; and (v) to facilitate the development of information security

---

23 This has resulted in other groups of states such as the SCO, the Association of Southeast Asian Nations (hereafter ASEAN) or the African Union (hereafter AU) itself and even individual states making progress on the challenges but also opportunities presented by cyberspace. However, "substantial progress at the regional level is difficult to achieve, due to differing attitudes and levels of technological development among states, concerns about state sovereignty and the vital role of a highly motivated and well-resourced regional actor in advocacy" which does not preclude opportunities, as regional international organizations "offer avenues to leverage existing cybersecurity partnerships and build confidence in the region" (POETRANTO, I., LAU, J. & GOLD, J., *op. cit.*, note 7, pp. 318 and 320)

24 *Doctrine of Information Security of the Russian Federation*, December 5, 2016, available at http://www.scrf.gov.ru/security/information/DIB_engl/. As Christian SCHREIBER notes, "the Russian government is concerned about interference by other states in its country's socio-political relations. He further adds that it is important to safeguard national security against counterintelligence services and cyberterrorism, as well as its territorial integrity and prevention of military cyber threats. They also seek a strategic advantage in this area and to position themselves as one of the most developed states in this area" (*op. cit*., note 3).

internationally, create strategic alliances in the area of cyberspace and protect the information sovereignty of the Russian Federation.

Later, on July 2, 2021, Russian President Vladimir Putin presented a new updated version: the *National Security Strategy of the Russian Federation*[25] . In it, the concept of security has been challenged as it includes not only national security issues but also such topics as the economy, the environment, national defense and even one's own spiritual and moral values as the main national interests:

> "(i) to save the Russian people and develop their human potential; (ii) to protect the constitutional system, sovereignty, independence and territorial integrity; (iii) to develop a safe information space, protect Russian society from destructive information and psychological impact, while defending the sustainable development of the Russian economy on a new technological basis; (iv) protecting the environment, conservation of natural resources and adaptation to climate change; (v) strengthening the traditional spiritual and moral values of the nation and preserving the cultural and historical heritage of the Russian people; and (vi) maintaining strategic stability, strengthening peace and security and the legal foundations of international relations"[26] .

To preserve these national interests, the ESNR establishes nine priorities and their objectives, along with the ways and means to carry them out, which are contrasted in the following table with the 2015 ESNR. New in the 2021 ESNR is the importance it gives to "information security", noting that there is a "confrontation" with the West that would justify its cyber-interference in certain electoral processes. As for the measures envisaged to maintain "information security" we find the strengthening of safeguards against cyber-attacks, the systematic development of Russian proprietary technologies and, in general, the establishment of "forces and means of information confrontation"[27] .

---

25 *National Security Strategy of the Russian Federation*, July 2, 2021, available at https://rusmilsec.blog/wp-content/uploads/2021/08/nss_rf_2021_eng_.pdf.

26 The strategy mentions that Russia seeks to maintain strategic stability and international cooperation: first, by deepening with the countries of the Commonwealth of Independent States and the Greater Eurasian Partnership (a project that was pushed by Moscow); second, by developing a comprehensive partnership and strategically interacting with China and India; and, third, by deepening cooperation with the SCO and BRICS nations (LABORIE, M., "The National Security Strategy of the Russian Federation (July 2021): a manifesto towards confrontation with the West," *Global Strategy Report*, No. 36, 2021, available at https://global-strategy.org/la-estrategia-de-seguridad-nacional-de-la-federacion-rusa-julio-2021-un-manifiesto-hacia-la-confrontacion-con-occidente/#_edn1).

27 "New information technologies are increasingly used to interfere in the internal affairs of the country. Thus, Russian sovereignty is threatened by the "dissemination of false information". Likewise, the use of the Internet to mobilize mass events, as well as the manipulation of history for "political purposes" constitute dangers to national security. (...) measures aimed at countering this foreign threat will extend through education, culture, religion, science and the media and social networks. The list is so wide that these practices will certainly involve a very significant interference in the private lives of citizens by the State." (LABORIE, M., *op. cit.,* note 26).

ESNR 2015	ESNR 2021
National Defense	Preservation of the Russian people and development of human potential
Public and State Security	National defense
Improved standard of living	State and public safety
Economic growth	Information security
Science, technology and education	Economic security
Health	Scientific and technological development
Culture	Environmental safety and management
Ecology and rational use of natural resources	Protection of traditional Russian spiritual and moral values, culture, and historical memory
Stability and strategic partnership among peers	Strategic stability and mutually beneficial international cooperation

Source: Mario LABORIE, 2021

In parallel to the 2021 ESNR, Russia submitted its contribution, on a voluntary basis, in the official GEG compendium also of 2021 concerning the application of international law[28] . Russia is part of the group of States that accept the application of the principles and norms of international law in cyberspace or information space[29] ; consensus that was reached in the UN GEG report of 2013, in that of 2015 (already noted),

[28] "International obligations of States, including those arising from international treaties as the primary sources of international law, are presumed to be applicable in the information space" (*Official Digest of Voluntary National Contributions on the Question of How International Law Applies to the Use of Information and Communication Technologies by States, submitted by the Governmental Experts on Promoting Responsible State Behaviour in Cyberspace in the Context of International Security,* established pursuant to General Assembly resolution 73/266 of 13 June 2021, pp. 79-81, available at https://documents.un.org/doc/undoc/gen/n21/189/51/pdf/n2118951.pdf).

[29] "The principles enshrined first and foremost in the Charter of the United Nations and in the Declaration on Principles of International Law, Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations of 24 October 1970. These include, in particular, the principles of sovereign equality of States, the prohibition of the use or threat of force, the settlement of international disputes by peaceful means, non-interference in the internal affairs of States, the obligation of States to cooperate with each other, equality of rights and self-determination of peoples, fulfillment in good faith of the obligations of international law, the inviolability of State borders and the territorial integrity of States (*Official Digest of Voluntary National Contributions on the Question of the Application of International Law to the Use of Information and Communication Technologies by States, submitted by the Governmental Experts on Promoting Responsible State Behavior in Cyberspace in the Context of International Security, op. cit. cit,* p. 79).

in the OEWG report of 2021 and in the General Assembly resolution (A/RES/73/27, para. 17 preambular) which, proposed by Russia, was adopted in 2018. Now, the Russian Federation points out,

> "given the specific legal nature of the information environment, in particular the fact that activities in it may be anonymous, the application of international law to the use of information and communication technologies (ICTs) should not be automatic and should not be carried out by simple extrapolation. There is a need to substantially discuss the question of how specific instruments of existing international law apply to the sphere of ICTs, as well as to elaborate a universal approach to this issue under the auspices of the UN"[30] .

In this regard, Russia lists those issues that, in its opinion, should be analyzed in depth under the prism of international law[31] . First of all, the Russian Federation points out the possibility of attributing to States the responsibility for particular actions in the information space, but understanding that this requires a more detailed study on the basis of current international law, where the international responsibility of a State is conditional on the commission of an internationally wrongful act by this State. Thus, according to the *Draft Articles on Responsibility of States for internationally wrongful acts*[32] , a State commits an internationally wrongful act when its conduct, act or omission, is attributable to the State under international law and constitutes a breach of an existing international legal obligation. In any case, Russia points out, the determination of a State act as internationally wrongful is governed by international law, without being affected by domestic law.

Second, with regard to countermeasures, Russia asserts that countermeasures that may be taken by an injured State against a State responsible for an internationally wrongful act shall not affect the obligation to refrain from the threat or use of force enshrined in the *Charter of the United Nations*, obligations to protect fundamental human rights, obligations of a humanitarian nature prohibiting retaliation, as well as other obligations under peremptory norms of general international law.

Thirdly, the Russian Federation points out that, according to customary international law, a State shall be responsible for those activities carried out by its institutions and subjects acting under its control. However, he points out, in cyberspace it

---

30 *Ibidem*, p. 79.
31 *Ibidem,* pp. 79-81.
32 *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, adopted by the ILC at its 53rd session (A/56/10) and annexed by the GA in Resolution 56/83 of 12 December 2001.

can be difficult to establish whether an individual carrying out an internationally wrongful act is acting under the control of a State or with its acquiescence, . In this regard, it is important to formalize the standard noted 2015 GEG report which states that "all allegations of organization and execution of unlawful acts brought against States must be substantiated" and, in any case, refrain from publicly imposing responsibility for an incident in cyberspace or information space on a particular State without providing sufficient technical evidence. The promotion of the peaceful use of ICTs and the prevention of conflict in this area are in the interests of all states, adds[33]

Finally, Russia believes that the international community should continue to study in depth all controversial issues related to the international legal regulation of the ICT sphere, as well as to develop new standards, on a universal and genuinely democratic basis, within the framework of the new OEWG for the period 2021-2025 (resolution 75/240 adopted by the General Assembly, cited above). The creation of a thematic subgroup (with the participation of international legal experts and academics) will help to organize a specific debate on this issue . [34]

On December 4, 2024, the Russian delegation to the OEWG 2021-2025, in its submission on how to apply international law to the use of ICTs, noted that

> "to create a fair and equitable system of international information security, a comprehensive approach to the development of universal legal instruments regulating the activities of States in the information space is necessary"[35] .

Thus, the Russian Federation considers that the principles of prevention and peaceful settlement of disputes, sovereign equality of States and indivisible security are the basis for the above-mentioned international legal instruments and, to this end, "the new standards should address the unique technical and legal features of the ICT environment"; in particular, its cross-border nature, anonymity of use, hidden malicious functions and vulnerabilities of hardware and *software*.

---

33 These basic principles of States' activities in the information space are enshrined in the aforementioned GEG reports of 2013 and 2015 and the OEWG report of 2021, as well as in General Assembly resolutions adopted by the majority of UN Member States (namely A/RES/73/27, A/RES/73/266, A/RES/74/29, A/RES/75/32, A/RES/75/240 and others).

34 *Developments in the Field of Information and Telecommunications in the Context of International Security*, *op. cit*.

35 *How international law applies to the use of ICTs,* Statement by the Russian Interagency Delegation at the ninth session of the UN Open-Ended working group on security of and in the use of ICTS 2021-2025, Permanent Mission of the Russian Federation to the United Nations, New York, 4 December 2024, pp. 1-3, p. 2, available at https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-__statement_-_international_law_-_ENG.pdf.

Furthermore, in this regard, Russia supports the statements by Iran, China and Pakistan and the statement made by the Cuban delegation, on behalf of Cuba, Venezuela and Nicaragua, on how international law applies to the use of ICTs. It adds:

> "We have noted that some States, as well as the Chair, continue to try to draw OEWG participants into further discussions on whether or not the development of legally binding agreements in the field of international information security should take place. The very formulation of the question is inappropriate. The answer to this question has already been received. In August 2024, all UN member states agreed on a draft Convention against Cybercrime, which, once adopted by the General Assembly, will become the first international treaty in the field of international information security. We are convinced that this is the first step towards a universal international legal regulation of the use of ICT"[36] .

Insisting on the *Draft UN Convention on international information security* presented by the group of states, Russia suggests considering the proposal as a basis for discussing the elements of a future treaty in this sphere. The document reflects the common understanding of the countries on the applicability of universally recognized principles of international law to the use of ICT (in particular, sovereign equality, prohibition of the use or threat of force, respect for the territorial integrity of States, peaceful settlement of international disputes, non-interference in internal affairs, good faith compliance with obligations under international law and inter-State cooperation), with the Russian Federation requesting that the initiative be thoroughly studied and discussed within the OEWG[37] . It adds that in order to fill the legal "gaps" in the field of international information security, a separate thematic subgroup on international law within the future mechanism should be created within the current OEWG, as provided for in its terms of reference

Finally, Russia supports the initiatives of the President of Belarus presented at the II International Conference in Minsk[38] : on the one hand, to create a surveillance system and, on the other hand, to adopt an international legal pact of non-aggression in the digital sphere that would allow not only to formalize the rights and obligations of States in the information space, but also to solve the problem of political attribution of the above-mentioned cyber attacks . [39]

---

36 *Ibidem,* pp. 1-2.
37 *Ibidem*, pp. 1-3.
38 II Minsk International Conference on Eurasian Security, October 31, 2024.
39 "The priorities are to contribute to the prevention of conflicts in the use of ICTs and to the peaceful use of these technologies, to strengthen cooperation between countries in international information

In parallel with the communication of the Russian delegation, in the *Joint Declaration of the First Ministerial Conference of the Russia-Africa Partnership Forum on measures to create a fair and equitable system of International Information Security*[40] , the Ministers of Foreign Affairs of the Russian Federation and African states confirmed the importance of further strengthening cooperation between the Russian Federation and African states in the field of security in the use of ICT, the formation of a fair and equitable security system in terms of their use, with the aim of preventing and peacefully resolving conflicts in the digital sphere, as well as those actions that hinder the maintenance of international peace, security and stability. At the same time, they also recognized the need to improve the legal framework among States in the field of security in the use of ICTs at the bilateral, regional and global levels and reaffirmed the importance of observing the generally recognized principles of international law and the development of a binding universal legal framework in the field of security in the use of ICTs under the auspices of the United Nations . [41]

Finally, emphasize that both Russia and African states advocate the internationalization of Internet governance, ensuring the equal participation of countries in this process, while guaranteeing integrity, stability and security of national segments of the Internet, as well as strict observance of the principles of the *UN Charter* and national legislation of states by technology monopolies and their responsibility in relation to the security of personal data and privacy of users. They further note their concern about the disruptive effect of unlawful unilateral coercive measures, which undermine the *UN Charter* and further restrict the technological development of Member States, reaffirming their commitment to promote respect for State sovereignty and sovereign equality in the ICT environment, opposing unilateral actions that could undermine international cooperation in this field .[42]

---

security, while strictly respecting the fundamental principle of the United Nations Charter: the sovereign equality of States" (*ibidem,* p. 3).

40 In accordance with the decisions of the Second Russia-Africa Summit (St. Petersburg, July 27-28, 2023) and the Declaration of the Second Russia-Africa Summit on Cooperation in the Field of International Information Security (*Joint Declaration of the First Ministerial Conference of the Russia-Africa Partnership Forum on Measures to Create a Fair and Equitable System of International Information Security*, Russian Federation, Federal Territory of Sirius, November 10, 2024, https://mid.ru/en/foreign_policy/russia_africa/1980864/).

41 Thus, Russia and African states welcome the decision reached in the OEWG on ICT Security 2021-2025 on the establishment of a permanent one-track negotiating mechanism at the United Nations (*Joint Statement of the First Ministerial Conference of the Russia-Africa Partnership Forum on Measures to Create a Fair and Equitable System of International Information Security*, *op. cit.,* note 40).

42 *Ibid.*

2. CHINA'S INTERNATIONAL STRATEGY FOR COOPERATION IN CYBERSPACE

China, along with Russia, India and Iran, is part of a bloc of emerging economic forces that has reinforced *the multipolarity* of international relations in order to obtain its own benefits. In order to emerge from geopolitical decline, China understood that it had to find an element that would strengthen its capabilities: the "technological revolution". However, the leaders of the Chinese Communist Party (hereinafter, CPP) considered it necessary to restrict access to the Internet and try to create a cybernetic ecosystem of its own, isolated from the rest of the world, which would allow the party to have control over Chinese society itself in the domain and regulation of Chinese national security. In other words, they implicitly assumed that information warfare would be one of the pillars of their military transformation[43] . Thus, starting in 1990 and with the aim of censoring Internet content in the Chinese space, the CCP developed the Great Firewall[44] . Thus, along these lines of isolation and protection of its sovereignty, China

> "monitors all traffic in Chinese cyberspace and allows the authorities to both deny access to a variety of selected websites and disconnect all Chinese networks from the global Internet network"[45] .

Now, although its policies and strategies on cyberspace are little known, the Cyberspace Administration of China published the 2017 *International Strategy for Cooperation in Cyberspace*[46] , which sets out the Chinese government's objectives

---

43 "Cyberspace and information technologies have been of interest to the Chinese Communist Party elites ever since Deng Xiaoping made it clear that China had to embark on a process of modernization, end isolation and open its doors to trade. However, it was not until Jiang Zemin's government (1989-2002) that China understood that it had to connect to the global network through the Internet (...). It understood that computerized warfare should be the hallmark of the Information Age (just as mechanized warfare was in the Industrial Age), since the new technologies constituted a threat to Chinese national security due to their destabilizing potential and placed the Asian country in a relationship of technological dependence with respect to the US (...)" (EXPÓSITO, J., *op. cit*., note 1).

44 "This great *Firewall* is the combination of legislative actions and technologies applied by the CCP; its function is to block access to selected foreign websites and slow down cross-border internet traffic. That effect includes limiting access to foreign information sources and blocking foreign internet tools" (VARGAS CHAPARRO, N. E., "China's cybergeopolitics: a strategic state interest", *Studies in Security and Defense*, August 17, 2022, available at https://esdegrevistas.edu.co/index.php/resd/article/view/328/551#content/citation_reference_25).

45 In addition, it has also created the "Golden Shield", managed by the Ministry of Public Security and other national departments and local agencies, consists of a "domestic surveillance system" (BRIZ ACEVES, P., "La nueva Gran Muralla de China... en el ciberespacio", *Global Affaires and Strategic Studies*, University of Navarra, available at https://www.unav.edu/web/global-affairs/detalle/-/blogs/la-nueva-gran-muralla-de-china-en-el-ciberespacio).

46 *International Strategy for Cooperation on Cyberspace*, March 1, 2017, available at http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm.

regarding cybersecurity, international cooperation and how to carry them out. Divided into five chapters, the strategy defines cyberspace as "the common space of activities for humanity", noting that (i) it is committed to the application of the principle of sovereignty (which will be defended by the Chinese military) and security in cyberspace, stating against any supranational interference that seeks to establish regulation of the new domain; (ii) it supports international regulation; (iii) promotes transparent, multilateral and democratic governance, so that all states participate equally and fairly; (iv) promotes the transit of information as long as public and national interests are ensured; (v) the promotion of cooperation in digital economy and trade; and (vi) proposes the creation of a platform to exchange healthy cyber culture in society .[47]

However, its isolationist and censorship aspirations do not end there. In 2020, the CCP planned the *New IP* or *cyber sovereignty*: "a network very similar to the Internet, in its own image, likeness and needs, a unified global network where citizens could be forced to connect to a national Internet mosaic regularized by the States", having to create an alternative network to the Internet: *New IP*[48] . In this sense,

> "the Beijing government understands that it can and should leverage its own capabilities in cyberspace to create advantages and influence events in all operational environments through it, as an instrument of power"[49] .

Alongside this virtual dimension, China also seeks to control the physical dimension or infrastructure of the Internet. To this end, it has projected the *Digital Silk Road* (hereafter DRS), presented by the Chinese government's *Official White Paper* in 2015:

---

47 "These six points may sound somewhat contradictory, but they promote Chinese interests in cyberspace, especially if one speaks of international governance between countries without any interference in the citizens of each country, i.e. at the national level. This perspective is especially reinforced by the fourth point that talks about a free Internet as long as it complies with the parameters of national interest (SCHREIBER, Ch., *op. cit*., note 3).

48 *New IP* (*Internet Protocol*) aims to eliminate the Internet as we know it and replace it with "a top-down governance model, in which governments have the ability to regulate everything that circulates in cyberspace". To do this, China needs the support of the UN, which it has tried to persuade on more than one occasion, and the International Telecommunication Union (hereafter ITU), which "in its early days oversaw the first international telegraph networks. It has since grown from 40 nations to 193, and has become the *de facto* standardization body for telecommunications networks. The standards produced there legitimize new technologies and new systems in the eyes of certain governments; particularly those in the developing world that do not participate in other Internet bodies. With this in mind, the CCP has already presented the ITU with the New IP with the image of a digital world in 2030, where virtual reality, life-size holograms, autonomous cars and remote surgery are omnipresent, and for which the current network is "not suitable" (VARGAS CHAPARRO, N. E., *op. cit*., note 44).

49 *Ibid*.

> "a brand of business operations related to telecommunications, data or product sales by technology companies based in China, to Africa, Asia, Europe, Latin America, the Caribbean and the United Kingdom"[50] .

Later, in October 2021, the People's Republic of China, through its Ministry of Foreign Affairs, expressed its *opinio iuris* on the law applicable to cyberspace:

> "The phenomenal development of the information technology revolution and digital economy is exerting far-reaching influence on the social and economic development of states and human civilization. All parties should uphold multilateralism, ensure equity and justice, place equal emphasis on security and development, intensify dialogue and cooperation, promote global governance and international rule-making, and build a community of shared future in cyberspace."[51] .

Firstly, China has expressed its views not only on the opportunities for development, but also on the *challenges and risks* posed by the connection between physical space and cyberspace . In this regard, it is highly critical of the attitudes of some states that use cyberspace as a "new battlefield", increasing the risk of conflict and endangering international peace and security. In view of the vulnerability of critical infrastructures .[52]

Second, the Chinese state points out that the international community should develop universally accepted norms, rules and principles within the UN framework to jointly address risks and challenges and defend peace, security and prosperity in cyberspace. To this end, it should conduct discussions on how international law applies to the use of ICTs by states, taking into account the unique attributes of ICTs, and further develop common understandings on this subject, with the *UN Charter* and the principles enshrined therein (sovereign equality, the refraining from the use or threat of force, the settlement of international disputes by peaceful means and non-intervention in the

---

50 "Initially focused on investments in fiber optic cables and telecommunications networks. With the DRS, a large number of Chinese technological players expanded globally, with more economic than geopolitical purposes, and which included: e-commerce, cloud services (...)" (VARGAS CHAPARRO, N. E., *op. cit*., note 44).

51 *China's Position on International Rules-making in Cyberspace*, Ministry of Foreign Affairs of the People's Republic of China, October 2021, p. 1, available at https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf. A month later, it outlined its views on the application of the principle of sovereignty in cyberspace (*China's Views on the Application of the Principle of Sovereignty in Cyberspace,* Ministry of Foreign Affairs of the People's Republic of China, available at https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf).

52 *China's Position on International Rules-making in Cyberspace*, *op. cit*., note 5, p. 1.

internal affairs of other states), noting that the application of these principles is a cornerstone of peace, security and stability in cyberspace. And it was, with the aim of promoting international efforts, that China presented to the UN General Assembly in 2020 the *Global Initiative on Data Security*[53] and, later, the *Global Security Initiative*, during the 2022 Asian Annual Conference[54] ; of a *soft law* nature, both documents highlight the commitment to build a global security governance system[55] . In any case, China considers that the following norms, rules and principles should be observed: (i) the promotion by States of a cyberspace characterized by peace, security, openness, cooperation and order, with the use of ICTs compatible with the maintenance of international peace and security. (ii) The application of the principle of sovereignty by states in cyberspace, with states exercising jurisdiction over ICT infrastructure, resources and data, as well as over ICT-related activities in their territories, having the right to protect their information systems and data from cyberthreats or cyberattacks, and refraining from using ICTs to interfere in the internal affairs of other states and undermine their stability, security or interests, whether political, economic or social. In addition, states should participate in the management and distribution of international Internet resources on an equal footing and build a system of global Internet governance based on multilateralism, democracy and transparency. (iii) States should improve the protection of critical ICT infrastructure and oppose activities that could harm it, whether their own or those of other states, as well as

---

53 *Global Initiative on Data Security*, 2020, "The initiative, a clear response to the US "Clean Network Program", uses language familiar from previous occasions on which China articulated its vision for data security: strong localization requirements and the right for different jurisdictions to govern data and the digital economy as they wish, based on "mutual respect". Foreign Minister Wang Yi called for global data governance rules based on multilateralism and "fairness and justice (...) Beijing will likely seek to take advantage of transatlantic divisions on data governance to present China as a trusted partner for the EU. Beijing's proposal implicitly engages with European sensitivities about US digital surveillance of foreign citizens, coming less than two months after a landmark decision by the Court of Justice (CJEU) that invalidated the mechanism for transferring personal data from the EU to the US. Beijing might also point out that its new privacy protection framework took inspiration from Europe's General Data Protection Regulation (GDPR). But transatlantic divergences will arguably do little to ease growing European concerns around China's intrusive surveillance state" ("China's Global Initiative on Data Security has a message for Europe", *Merics*, September 24 2020, available at https://merics.org/en/comment/chinas-global-initiative-data-security-has-message-europe).

54 An initiative that has had a vital impact on the development of the basic principles of contemporary international law (XU, K., LV, Z. & LI, J., "Global Security Initiative and the Development of Contemporary International Law," *Transactions on Social Science, Education and Humanities Research*, vol. 8, 2024, pp. 64-71 , available at https://wepub.org/index.php/TSSEHR/article/view/1946/2154).

55 As Professor María José CERVELL points out, (...) these documents could "be the germ of certain norms which, if expressly accepted as such by the States (*opinio iuris*), would be susceptible to acquire that binding nature through their consolidation as international customs ("¿Un *soft law* para el ciberespacio? (De las normas no vinculantes y otras iniciativas)", in CERVELL HORTAL, Mª. J. and PIERNAS LÓPEZ, J. J., *Hacia una regulación internacional para el ciberespacio*, Aranzadi, 2023, pp. 123- 158, pp. 130 and 131; and *op. cit*., note 15, pp. 32 and following).

increase their information (legislation, best practices and technologies) related to the protection of critical ICT infrastructure. (iv) States should manage data security in a comprehensive, objective and evidence-based manner, fostering an open, fair and non-discriminatory business environment, and maintain an open, secure and stable supply chain of global ICT products and services, taking measures to prevent and stop activities that endanger personal information, opposing mass surveillance against other states and the unauthorized collection of personal information of other states using ICTs as a tool. (v) States should intensify cooperation against cyber-terrorism. To this end, they should prohibit terrorist organizations from using the Internet to create websites, online forums and blogs, including the manufacture, publication, storage and transmission of audio and video documents, dissemination of violent terrorist ideologies, fundraising, recruitment, incitement to terrorist activities.... In addition, states should conduct intelligence exchanges and law enforcement cooperation, and develop cooperative partnership with international organizations, enterprises and citizens to combat cyber terrorism[56] . (vi) Finally, China supports the establishment of an inclusive and sustainable process with broad participation of all states within the UN framework to address the issue of cybersecurity, and welcomed the 2021 report of the OEWG, noting that states should observe and implement previous international consensuses, including norms, rules and principles for responsible behavior of states, and formulate new international norms and rules, concluding that.

> "China is willing to work together with all parties to promote the positive progress of the 2021-2025 Open Composition Working Group and build a community of shared future in cyberspace"[57] .

III. IS IT POSSIBLE TO AFFIRM THE EXISTENCE OF A *STRATEGIC* CHINESE-RUSSIAN *ALLIANCE* IN CYBERSPACE?

56 *China's Position on International Rules-making in Cyberspace*, *op. cit*., note 51, pp. 2-3.

57 *Ibidem,* p. 4. In the same vein, the Chinese president again spoke out at the World Internet Conference, an event organized by the Cyberspace Administration of China, "advocating for an inclusive cyberspace," in an event that "reflects Beijing's strategy to consolidate its Internet governance model, characterized by strict state control and exclusion of foreign platforms" ("China advocates global cooperation in cyberspace in the face of AI challenges," *NCCC*, January 20, 2024, available at https://noticiasncc.com/cartelera/articulos-o-noticias/01/20/china-aboga-por-cooperacion-global-en-ciberespacio-ante-desafios-de-la-ia/).

In 2016, the presidents of the People's Republic of China and the Russian Federation, issued a joint statement regarding cooperation in the development of the information space where they advocated, among other things,

> "the principle of respecting national sovereignty in the information space; support the reasonable demands of each nation to maintain its own security and development; advocate the construction of a peaceful, secure, open and cooperative information space; and explore the possibilities of developing universal rules of responsible behavior in the information space within the framework of the United Nations (...) Advocate the equal rights of all countries to participate in Internet governance and recognize the right to ensure national security in the information space based on their own laws and state system. Support the initiative to build a multilateral, democratic and transparent global Internet governance system and maintain the important role of the United Nations in establishing global Internet governance mechanisms"[58] .

The points in common that they point out in their joint declaration could give rise to a possible strategy between the two States. Firstly, the model of governance in cyberspace. At present we can observe the participation of various entities such as States, international organizations, agencies and private entities in everything related to the development of standards, protocols and norms, without any of them being able to exercise total control over cyberspace. This is a decentralized model of cyber governance. However, not all states agree with decentralization and it is here, especially, where China and Russia converge, as both states seek to have an influence on cyberspace, not only at their national but also at the international level, seeking to expand the mandate of the International Telecommunication Union to increase its competencies in Internet governance[59] . Second, both China and Russia advocate the development of a legally

---

58 JINPING, X. & PUTIN, V. V., 'The Joint Statement between the Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development", *China Daily*, June 26, 2016, available at https://www.chinadaily.com.cn/china/2016-06/26/content_25856778.htm. Even in relation to the principle of sovereignty, China a year later expanded its position in the *International Strategy of Cooperation on Cyberspace*, stating that the principle of sovereignty gave the right to states to "protect their ICT systems and resources from threat, disruption, attack and destruction" ("International Strategy of Cooperation on Cyberspace," *Xinhua Net*, March 1, 2017, available at http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm).

59 NEUMAN, N., *op. cit.,* note 14, pp. 774-779. "The global governance, development, and maintenance of cyberspace is decentralized and involves multiple types of stakeholders. Whereas Russia and China would prefer an intergovernmental model of governance, many Western and like-minded States support multistakeholderism based on the premise that it furthers innovation, growth, and freedom of expression. However, this also means that there are a few private institutions outside of a neutral's territory that could theoretically restrict its ability to remain impartial" (CORDEY, S. & KOHLER, K., *The Law of Neutrality in Cyberspace. Cyberdefense Report*, Center for Security Studies, ETH Zürich, Zürich, December 2021 , pp. 58). In the same sense, VARGAS CHAPARRO, N. E., *op. cit.*, note 44.

binding international instrument to regulate cyberspace[60] . Thirdly, both states advocate the application of the principle of sovereignty in cyberspace, understood as a broader concept than the strict concept of sovereignty and which would also include territorial sovereignty, and its application could be transferred to cyberspace[61] , being totally against the interference of other states in their national affairs [62] . And, fourthly, the application of the due diligence principle. China defended its position that no state shall knowingly allow its territory or ICT facilities, data and information under the control of its government to be used for ICT activities that undermine national security or interests .[63]

But it is not only in their joint declaration that we find common ground. There are, in addition, reasons that lead both States, indeed, to establish an alliance, indefinite or temporary[64] , in cybersecurity matters. Firstly, they would enhance their cyber capabilities and consolidate their cooperation with the aim of not competing on a global level, as their security priorities are different: Russia with NATO and China with the United States, so

---

60 However, in the opinion of Professor María José CERVELL, "it is unlikely, in fact, that it will ever see the light of day and (...) it may even be desirable that it should do so, because the legal problems involved are so wide-ranging, varied and give rise to so much debate that it seems that any attempt to impose a global treaty would in fact be unfeasible". However, the idea has been advocated by Russia, with the support of China, and "consists in the drafting of a Convention to ensure the security of international information" (*op. cit*., note 15, pp. 18 and 35 et seq.).

61 In fact, it is currently not questioned that sovereignty applies to those persons involved in cyber activities or to cyber infrastructures located in the territory of the sovereign State and/or, in short, to any cyber activity happening in or through that territory, but there are difficulties for its application in cyberspace (VÁZQUEZ SERRANO, I., *op. cit.,* note 2), sovereignty being considered one of the so-called *grey zones* of international law (SCHMITT, M. N., "Grey Zones in the International Law of Cyberspace", *Yale Journal of International Law Online*, vol. 42, no. 2, 2017, pp. 1-21, p. 4) and, although there is consensus on its application, this is *controversial*, with the doctrine debating about its nature as a primary norm or rule of DI, whose breach would give rise to a wrongful act (CERVELL HORTAL, Mª. J., "Ciberinjerencias en procesos electorales y principio de no intervención (una perspectiva internacional y europea)", *Revista Electrónica de Estudios Internacionales*, no. 45, June 2023, pp. 1-33, pp. 5-7).

62 "They argue that all states should be treated equally when creating a universal law. [i.e.] any act that happens in cybersecurity should be dealt with at the national level, rather than subjecting national jurisdiction to extraterritorial standards and regulations. In this way they ensure that they can carry out their own information security policies at the national level without being accountable to any external and alien body, entity or country, and they ensure that there is no regulatory body against their national positions, as these same tools can be used to destabilize the societies and politics of both" (SCHREIBER, Ch., *op. cit*., note 3).

63 China therefore declares that the principle of due diligence in cyberspace is mandatory (*China's Position on International Rules-making in Cyberspace*, *op. cit*., note 51, pp. 1-2). Regarding the principle of due diligence in cyberspace, as Professor Juan Jorge PIERNAS LÓPEZ points out, despite the *opinio iuris* of some States (United States or United Kingdom) it is "an international obligation based on the customary rule of application to activities occurring in and from cyberspace". This is how the ICJ and most States have referred to the principle ("The international law principle of due diligence and its application to the cyber context", *Annals of Law*, vol. 41, 2024, pp. 66-95, pp. 66 and 67, available at https://revistas.um.es/analesderecho/article/view/594441/357291). See also, by the same author, *El Derecho internacional y las contramedidas cibernéticas, op. cit.,* note 17, pp. 47-61.

64 SCHREIBER, Ch., *op. cit.,* note 3.

a collision of interests does not seem likely[65] . Secondly, both Russia and China seek to establish strict cybersecurity laws order to have greater control over the flow of information on the network to safeguard national interests; laws that have been raised in the SCO and have sought to push them for the rest of the members to adopt. In fact, Russia has aligned itself with China to promote such approaches to the SCO at the last UN General Assembly meeting[66] . Thirdly, economic interdependence must be taken into account: while Russia is an exporter of raw materials with a deficit in industrial technology, China is a major consumer of raw materials (gas and oil in the energy sector), but possesses industrial technology. Fourthly, both states share political objectives: they value stability, certainty of results and, above all, maintaining their power, bearing in mind that both countries are permanent members of the UN Security Council[67] . And, finally, they share being "recipients of US hostilities"[68]

Now, although they have aligned themselves to give impetus to their positions, there are also considerable differences in the interests of the two states in terms of forming an alliance. Thus, there is the potential for conflict in the future: for example, they may compete for hegemony in cyberspace and it may work as long as they do not play off against each other. But, in addition, there are other situations in which tensions could develop .[69]

---

65 Although U.S. Secretary of Defense James MATTIS noted that such an alliance would not last long given the mutual distrust that exists, the strategic alliance is a counterweight toward U.S. hegemony (GABUEV, A., "Why Russia and China Are Strengthening Security Ties" *Foreign Affairs*, September 24, 2018, available at https://www.foreignaffairs.com/articles/china/2018-09-24/why-russia-and-china-are-strengthening-security-ties).

66 SCHREIBER, Ch., *op. cit*., note 3.

67 GABUEV, A., *op. cit*., note 65.

68 SCHREIBER, Ch., *op. cit.,* note 3. However, it is not in Russia's interest to come to China's rescue in case of a confrontation with the USA, nor is it in China's interest to support Russia and enter into conflict with other countries because of its actions in Southwest Asia or Europe (GABUEV, A., *op. cit*., note 65).

69 Chinese migrants living on Russian territory that could present a territorial dispute problem, China's theft of military technology from Russia in 2005, and China's rapid expansion in Central Asia, historically influenced by Russia, thanks to its New Silk Road project. Also, the annexation of Crimea put Russia in a difficult and not so friendly position vis-à-vis Europe and the United States, opting to turn its attention to China as an escape route; Russian organizations genuinely questioned the alliance and the risks it might incur, although it turned out at the time that there would be more benefits that way. However, what would happen if Europe managed to reach an agreement with Russia and Russia would again benefit from Europe? Would there be a rupture in the relationship? Although Russia has accepted that the realization of the New Silk Road is highly probable and that it will pass through Central Asia, Russia could tolerate it as long as China does not interfere and gain control of the area, especially since it is the territory where the Russian project of the Eurasian Union operates and has its influence; there may be a new configuration in the countries that influence the region, since it is in China's interest to control the area (GABUEV, A., *op. cit.,* note 65). Finally, China intends to expand into the Arctic, a territory highly protected by Russian sovereignty and, if China does not yield to its intentions, a dispute could break out in which the alliance breaks down or one or the other will have to exchange certain areas of influence, such as giving China certain permits to operate in the Arctic in

All this leads us to think that the alliance between China and Russia in cyberspace exists, yes; but it is also weak, and both actors must handle it with care because, if one of the parties no longer has any use for the alliance and considers that it will obtain greater benefits by breaking it, it will not hesitate to do so .[70]

IV. A BRIEF (BUT OBLIGATORY) LOOK AT THE RUSSIAN "SPECIAL MILITARY OPERATION" IN UKRAINE THROUGH THE CYBERSPACE

For more than a decade, Russia has been systematically and gradually using cyberspace as a "battlefield" against Ukraine through acts such as cyber espionage, cyber sabotage, disinformation, propaganda and cyber attacks, giving rise to the so-called *fifth generation wars*[71] , a combination of hybrid[72] and cognitive warfare . [73]

In fact, at the beginning of the conflict, Russia's attitude made one think that Russia would deploy all its cyber capabilities[74] as, since 2014, Ukraine had become the

exchange for the cessation of Chinese influence in Central Asia, for example" (SCHREIBER, Ch., *op. cit.,* note 3).

70 "Political stability is the primary factor for the alliance to be sustained, given that as long as V. Putin and Xi Jinping are in power, it is doubtful that there will be any radical shift in their foreign policies. In addition, both countries have begun to have a technological and information exchange in this sphere in recent years, so it could be said that there is an information interdependence that they would hardly want to sacrifice in the event of a rupture, in addition to becoming the counterweight to the US and the European Union" (SCHREIBER, Ch., *op. cit*., note 3).

71 "Fifth-generation wars are characterized by the fact that the scenarios of confrontation have expanded into cognitive and technological domains, such as cyberspace. Likewise, the actors that can conduct the war are no longer necessarily the States, because private military security companies appear, which end up exercising roles and missions related to security and defense, and cities have become the centers of gravity of this type of wars. Moreover, this fifth generation conflict has evolved and one of the fields of confrontation is the cognitive space, where the actors involved in it seek strategies to control the information flows of public opinion in order to maintain the legitimacy of the wars" (SANTOS BARÓN, M. A., "The conflict between Russia and Ukraine: a fifth generation war", *Opera*, no. 35, pp. 37-61, pp. 56 and 57).

72 Hybrid warfare can be defined as "the coordinated and synchronized use of all the capabilities of a State - economic, military, information, diplomatic, etc. - to combat and erode an opponent without ever exceeding the umbra that could trigger the right of response in self-defense and even making any kind of response impossible" (CUBEIUS, 2001). to combat and erode an opponent without ever exceeding the umbra that can trigger the right of response in self-defense and even making any kind of response impossible" (CUBEIRO CABELLO, E., "El ciberespacio en la guerra de Ucrania", *Instituto Español de Estudios Estratégicos*, no. 32, 2022, pp. 1-14, p. 3).

73 Cognitive warfare has been defined as one in which "the human mind becomes the battlefield. The goal is to change not only what people think, but also how they think and act. In its extreme form, it has the potential to fracture and fragment an entire society so that it no longer has the collective will to resist an adversary's intentions" (HOPKINS, J., "Countering cognitive warfare: Awareness and resilience", *NATO Review*, 2021, available at https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html).

74 As it had done in previous situations against Estonia, Georgia and Kyrgyzstan (see: GUAYARA ARCINIEGAS, J. A., "Strategies of cyberwarfare: Israel and Russia", *Perspectives in Intelligence*, vol. 10, no. 19, 2018, pp. 57-69, pp. 64-67 and KOZLOWSKI, A., "Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal*, vol. 3, 2014, pp. 237-245, available at: https://eujournal.org/index.php/esj/issue/view/120), although these cyberattacks

test laboratory where Russia tested its cyber weapons, as well as disinformation and propaganda, assuming Russian superiority in cyberspace[75] . However, the intensity of the Russian cyberwar against Ukraine has been changing. At the beginning of the conflict, the successes achieved were not what was expected[76] , to the point that some authors stated: "we have encountered the most conventional conflict of the last decades"[77] , asking whether Russia had not been able to deploy all its cyber capabilities or whether it had not really wanted to turn cyberspace into a "battle space"[78] , as it has maintained in its security strategy[79] . However, the number of Russian cyberattacks against Ukraine has been

have not been acknowledged by Russia, as "Russia has an excellent alibi (...): the nature of the attack is so simple that it can be attributed to ordinary people, which in fact seems to be the Russian *modus operandi* to leave no clues, only it is quite suspicious when the same method is used to cover up the most corrupt elections since the fall of the USSR, a target that could only be pursued by the government. Even also, when looking at the attack on Estonia, one can notice a high degree of synchrony and planning in the attacks, an almost military strategy; but again this is only conjecture, none of this can be proven yet" (GUAYARA ARCINIEGAS, J. A., *op. cit.,* note 74, pp. 65-68).

75 "Russian weapons may be losing effectiveness because they are already too well known (...) The troll armies and their official means of disinformation seem not to be as effective as in past times" (CUBEIRO CABELLO, E., *op. cit.,* note 72, p. 11).

76 "The Russian case is quite elementary. When their acts of aggression in cyberspace are analyzed, they seem more like acts of vandalism than real attacks in the strictly military sense of the term. DDoS is the usual Russian technique, which consists in the use of a large network of infected computers called *Botnet*, where each of the computers that are part of this network have been previously infected with some malicious code, usually a Trojan. These computers are called *zombies*, since they are under the control of the *hacker* who is carrying out the attack, who makes use of his vast network to make multiple requests to the web page to be disabled (...). It is a very simple cyberattack, usually practiced by hacktivists, its impact is usually mediatic and somewhat psychological rather than effectively an attack with military connotations, as evidenced in the case of Georgia" (GUAYARA ARCINIEGAS, J. A...., op cit, *op. cit.,* note 74, pp. 67-68).

77 "In short, what was predicted was that Russia would employ simultaneously, and in a phase beginning some days, weeks, in advance of the military invasion, a wide range of actions in and through cyberspace. Among them: - Activation of *malware* previously positioned on targets of interest (primarily for sabotage purposes). - Massive Distributed Denial of Service (DDoS) cyberattacks against Ukrainian websites. - Massive cyber-attacks against critical infrastructure and essential services of Ukraine (*wipers, ransomware,* DDoS). Massive *defacements* on official Ukrainian websites. - Massive *phishing* campaigns. - Massive phishing campaigns in social networks (RRSS). Distribution of highly sophisticated *malware* (*wipers, ransomware,* Trojans, *exploit kits*). - Powerful disinformation and propaganda campaigns. - Initiative, management and control of the narrative" (CUBEIRO CABELLO, E., *op. cit.,* note 72, p. 4). The Swiss NGO Cyberpeace Institute notes that by 2023 there had been 636 cyberattacks against Ukraine and 331 against Russia, with the most targeted Ukrainian sectors being public administration, media, ICT, financial and trade. However, this number dropped in the second quarter of 2023 ("Cyber Dimension of the armed conflict in Ukraine," *Cyberpeace Institute*, 2023, available at https://cyberpeaceinstitute.org/wp-content/).

78 "Because it is strange that, if he had this capability in his hands, Putin would not have already used it extensively and decisively to prevent the prolongation of a conflict that is increasingly contested throughout the world (including Russia) and which kills dozens, if not hundreds, of Russian soldiers every day" (CUBEIRO CABELLO, E., *op. cit*., note 72, p. 12). However, there are those who think that, in reality, Russia has already reached the peak of its cyber capabilities (WOLF, J., "Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine", *Time,* March 2, 2022, available at: https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/).

79 Whether or not Russia has exhausted its capabilities in cyberspace, there are several reasons that lead it to renounce the use of weapons in cyberspace: the possibility of a third State being affected and triggering the clause of Article 5 of the NATO Treaty or the lack of cybersecurity in its own

increasing[80] , which leads us to believe that Russia is now using all kinds of weapons and strategies, including in cyberspace, to achieve victory.

IV. CONCLUSIONS

In general terms, at present, we can affirm the existence of a *strategic alliance* between Russia and China in relation to cyberspace, taking into account that the approaches taken by both states in their respective strategies, as analyzed above, are similar. Thus, the Russian government and the Chinese government share the same concerns in relation to the consequences that may arise from the use made of cyberspace, hence the importance of its regulation and governance, understanding that it would not only affect their security but also their economic interests and political stability.

However, the answer to how stable this alliance is will depend on whether the interests of both states could be altered and give rise to clashes and clashes, something that does not seem likely given the stability of both governments and the policies they have been developing to date, an indispensable element in this union being the fact that both governments share an objective: to avoid U.S. hegemony in cyberspace.

If both governments allow it, especially the Chinese government and the imposed isolation, the various proposals regarding the digital sovereignty of China and Russia should be closely monitored and the various factors noted that could end the symbiosis regarding cyber dominance between China and Russia should be analyzed but, for the time being, it does not appear that changes will occur in the near future.

Bibliography

BERMEJO GARCÍA, R and LÓPEZ-JACOISTE DÍAZ, E., *La ciberseguridad a la luz del Jus ad Bellun y del Jus in Bello*, Eunsa, Navarra, 2020.

infrastructures (compared to other States) so that, in the event of a conflict, it could suffer significant damage (CUBEIRO CABELLO, E., *op. cit.,* note 72, pp. 1-14, p. 14).

[80] In 2024 alone, the number of cyberattacks in Ukraine increased by almost 70% over the previous year - reaching 4,315 incidents, compared to 2.541 in 2023- (...) the scope of this parallel war is "massive" and its consequences affect everyone, not just the invading country [warning] that by 2025 they expect attacks to continue and cyberspace to remain a focus of a key war for Russia in its attempt to destabilize Ukraine" ("La guerra cibernética se intensifica entre Rusia y Ucrania", *El País*, January 19, 2025).

BROWN, D., ESTERHUYSEN, A. & KUMAR, S., "Unpacking the GG's framework on responsible state behavior: Cyber norms", *Global Partners Digital*, 2019, pp. 1-9.

CERVELL HORTAL, Mª. J., "Un *soft law* para el ciberespacio? (De las normas no vinculantes y otras iniciativas)", in CERVELL HORTAL, Mª. J. and PIERNAS LÓPEZ, J. J., *Hacia una regulación internacional para el ciberespacio*, Aranzadi, 2023, pp. 123-158.

ID. "Normas internacionales para el ciberespacio: tan lejos, tan cerca", BERTOT TRIANA, H. (dir.), *El Orden Jurídico Internacional ante las vicisitudes del siglo XXI*, Tirant lo blanch, Valencia, 2024, pp. 17-38.

CORDEY, S. & KOHLER, K., *The Law of Neutrality in Cyberspace. Cyberdefense Report*, Center for Security Studies, ETH Zürich, Zürich, December 2021.

CORN, G. & TAYLOR, R, "Sovereignty in the Age of Cyber", *American Journal of International Law Unbound*, No. 111, pp. 207-212.

CUBEIRO CABELLO, E., "El ciberespacio en la guerra de Ucrania", *Instituto Español de Estudios Estratégicos*, no. 32, 2022, pp. 1-14.

DUNN CAVELTY, M. & WENGER, A., "Cyber security meets security politics: Complex technology, fragmented politics, and networked science", *Contemporary Security Policy*, vol. 41, no. 1, pp, 5-32.

EXPÓSITO, J., "El dominio de la información: el ciberespacio visto desde China. Estudio sobre las implicaciones geopolíticas del dominio de la información", *Ejércitos. Revista digital sobre defensa, armamento y fuerzas armadas*, núm. 66, 2023.

FINNEMORE, M. & HOLLIS, D. B., "Constructing Norms for Global Cybersecurity," *American Society of International Law*, vol. 110, no. 3, 2016, pp. 425-479.

GABUEV, A., "Why Russia and China Are Strengthening Security Ties," *Foreign Affairs, September 24, 2018.*

GUAYARA ARCINIEGAS, J. A., "Cyberwar strategies: Israel and Russia," *Perspectives in Intelligence*, vol. 10, no. 19, 2018, pp. 57-69.

GUTIÉRREZ ESPADA, C., "La ciberguerra y el Derecho internacional", in MARTÍNEZ PÉREZ, E. J. (coord.), MARTÍNEZ CAPDEVILA, C., ABAD CASTELOS, M. and CASADO RAIGÓN, R. (dirs.), *Las amenazas a la seguridad internacional hoy*, Tirant lo Blanch, Valencia, 2017.

ID., "¿Existe (ya) un Derecho aplicable a las actividades en el ciberespacio?", in CERVELL HORTAL, Mª. J. (dir.), *Nuevas tecnologías en el uso de la fuerza: drones, armas autónomas y ciberespacio*, Aranzadi, Cizur Menor, 2020, pp. 225-248.

HOPKINS, J., "Countering cognitive warfare: Awareness and resilience", *NATO Review*, 2021.

HURWITZ, R., "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interest*, vol. 36, 2014, pp. 322-331.

KETTEMAN, M. C., "Ensuring cybersecurity through international law", *Revista Española de Derecho Internacional*, vol. 69, no. 2, 2017, pp. 281-289.

KORZAK, E., "UN GGE on Cybersecurity: The End of an Era? What the apparent GGE failure means for international norms and confidence-building measures in cyberspace", *The Diplomat*, July 31, 2017.

KOZLOWSKI, A., "Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal*, vol. 3, 2014, pp. 237-245.

LABORIE, M., "The National Security Strategy of the Russian Federation (July 2021): a manifesto towards confrontation with the West," *Global Strategy Report*, no. 36, 2021.

MURER, T. & MORGUS, R., "Tiping the Scale: An Analysis of Global Swing States in the Internet Governance Debate," *Global Commission on Internet Governance,* no. 2, June 2014, pp. 1-32.

NEUMAN, N., "Neutrality and Cyberspace: Bridging the Gap between Theory and Reality," *International Law Studies*, vol. 97, 2021, pp. 765-802.

SEGURA SERRANO, A., "Ciberseguridad y Derecho internacional", *Revista Española de Derecho Internacional*, vol. 69, no. 2, 2017, pp. 291-299.

PIERNAS LÓPEZ, J. J., "The international law principle of due diligence and its application to the cyber context", *Anales de Derecho*, vol. 41, 2024, pp. 66-95.

ID., *El Derecho internacional y las contramedidas cibernéticas*, Navarra, Aranzadi, 2024.

POETRANTO, I., LAU, J. & GOLD, J., "Look south: challenges and opportunities for the 'rules of the road' for cyberspace in ASEAN and the AU", *Journal of Cyber Policy*, vol. 61, 2021, pp. 318-339.

SANTOS BARÓN, M. A., "El conflicto entre Rusia y Ucrania: una guerra de quinta generación", *Opera*, núm. 35, pp. 37-61.

SCHREIBER, Ch., "The Future of China and Russia as Allies in Cyberspace," *Journal of International Security Studies*, no. 2, 2019.

SCHMITT, M. N., "Grey Zones in the International Law of Cyberspace," *Yale Journal of International Law Online*, vol. 42, no. 2, 2017, pp. 1-21.

ID, "Norm-Skepticism in Cyberspace? Counter-Factual and Counterproductive," *Just Security,* February 28, 2020.

SCHMITT, M. N. & VIHUL, L., "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norm," *Just Security,* June 30, 2017.

TIKK, E. & KERTTUNEN, M., *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, Cyber Policy Institute, 2017.

VARGAS CHAPARRO, N. E., "China's cybergeopolitics: a strategic state interest," *Studies in Security and Defense*, August 17, 2022.

VÁZQUEZ SERRANO, I., *Una aproximación al concepto de neutralidad en el ciberespacio*, Tirant lo blanch, Valencia, 2025.

XU, K., LV, Z. & LI, J., "Global Security Initiative and the Development of Contemporary International Law," *Transactions on Social Science, Education and Humanities Research*, vol. 8, 2024, pp. 64-71.

The applicability of international law to the cyber domain: national positions and strategies of the United States of America

Mónica CHINCHILLA ADELL
Profesora Ayudante Doctora
Universidad de Navarra

SUMMARY: I. INTRODUCTION. II. THE UNITED STATES' POSITION ON THE APPLICABILITY OF INTERNATIONAL LAW TO CONFRONT CYBERSECURITY THREATS. 2.1 The applicability and adaptability of international law to the cyber domain. 2.2 The development of non-legally binding norms and confidence building measures. 2.3 Peacetime cyber espionage and great power competition. 2.4 Due diligence and state responsibility. III. THE VARIOUS CONTRIBUTIONS TO NATIONAL CYBER SECURITY STRATEGIES. 3.1 The George W. Bush administration (2001-2009): some prevention and many good intentions. 3.2 The Barack Obama administration (2009-2017): from defensive to offensive. 3.3 The Donald Trump administration (2017-2021): the centrality of power? 3.4 The Joe Biden administration (2021-2024): a shift to a more regulation-focused approach. IV. LOOKING AHEAD: PROSPECTIVE DEVELOPMENTS IN THE NEW TRUMP ADMINISTRATION. V. FINAL CONCLUSIONS.

I. Introduction

The rapid technological advances of the last decades have brought cyberspace to center stage at a national and international level. While cyber-attacks have gradually increase, both state and non-state actors have been at the forefront of such attacks[1]. For instance, in Russia's ongoing war on Ukraine, Russia has allegedly used cyber means to gain advantage over its opponent and cause harm to civilian infrastructure and governmental services[2]. The government of Costa Rica declared a national emergency when the "Conti" and the "Hive" groups –non-state actors based in the Russian Federation– attacked various public institutions and caused disruption and severe economic losses[3].

[1] *Cfr*. WEAVER, J. M. *The U.S. Cybersecurity and Intelligence Analysis Challenges*, Palgrave Macmillan, 2022, p. 5.

[2] *Cfr*. TIDY, J. "Ukraine cyber-attack: Russia to blame for hack, says Kyiv", *BBC*, 14 January 2022, available at: https://www.bbc.com/news/world-europe-59992531. Also, *Cfr*. US DEPARTMENT OF DEFENSE, "2023 Cyber Strategy of the Department of Defense. Summary", September 2023, p. 4.

[3] *Cfr*. ASSOCIATED PRESS, "Costa Rica, 'under assault' is a troubling test case on ransomware attacks", NBW News, 17 June 2022, available at: https://www.nbcnews.com/news/latino/costa-rica-assault-troubling-test-case-ransomware-attacks-rcna34083.

The international implications of cyber-attacks in an interdependent and interconnected international community seem obvious. States have reached certain agreements to confront cyber-threats, mainly the *United Nations Convention against Transnational Organized Crime*, which entered into force in 2003, and obliges States Parties to train law enforcement agencies and assist other states to combat "transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology" (article 29). In the absence of a more recent consensus on international legally binding norms, the *Handbook on International Law Applicable to Cyber Operations*, or the Tallinn Manual, became the main non-legally binding guidance document for countries to confront cyber threats in a coordinated manner. Despite this, disagreements between states have been frequent in the most basic terms: is existing international law sufficient, or are new legal instruments necessary for the sake of cybersecurity?

International law has an undeniable settled role to guide states' behavior for the sake of international stability, also in the cyberspace realm. At the same time, "the uniqueness and rapidly evolving nature of cyberspace will place adaptive pressure on most of the existing international legal framework"[4], as Colonel Gary Corn anticipated. However, the development of international obligations has been slow and contested, leading to uncoordinated measures and the prioritization of national interests[5]. While some argue that "the law falls silent in the face of the challenges of the digital age"[6], others believe that existing international law applies to the digital domain[7]. In practice, the United States (US) and the European Union (EU) have generally favored the development of existing international law, while countries like Russia or China would rather opt for new regulations[8]. Divergent views are worth studying, especially when the US recently reckoned that China, for instance, "poses a broad and pervasive cyber espionage threat", and conducts constant cyber activity against the US interests and its citizens[9].

---

4 CORN, G. "Tallin Manual 2.0 – Advancing the Conversation", *Just Security*, 15 February 2017, available at: https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.

5 *Cfr*. WEAVER, J. M. *The U.S. Cybersecurity and Intelligence Analysis Challenges*, *op. cit*., p. 3.

6 KOENDERS, B. "Foreword", in Schmitt, Michael, N. (eds.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, p. xxv.

7 *Cfr*. *Ibid*.

8 *Cfr*. SNYDER, O. "The U.S. Cyber Security and International Law", *Embry-Riddle Aeronautical University*, 15 December 2022, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4501857.

9 *Cfr*. US DEPARTMENT OF DEFENSE, "2023 Cyber Strategy of the Department of Defense. Summary", *op. cit.*, p. 4.

In light of rapid technological development and the risks associated, the existing great power competition, and the previous and succeeding analyses that conform this book, the US perspective on cybersecurity and the application of international law is of great relevance to address present and future cyber threats. To this end, this chapter is structured as follows: in the first place, the successive US positions on the applicability of international law to the cyber domain, which were presented between 2012 and 2024, are considered. In this manner, the main legal and political standpoints of the government along the years can be assessed and compared. In the following section, this chapter describes and evaluates the contribution of each US administration since President George W. Bush adopted the *National Strategy to Secure Cyberspace* in 2003, and until the 2023 Department of Defense (DoD) Cyber Strategy was presented under the Joe Biden administration. Along this section, multiple policy instruments are analyzed in order to highlight similarities and differences characterizing US policies and strategies to confront cyber threats during all different administrations. After all this, a brief look into the US future perspectives on cybersecurity are provided in light of the unstable and rapidly changing security realm. And, lastly, this chapter concludes recapitulating the main ideas covered to shed some light into the potential future direction of the role of international law and cyber security in the US.

II. The United States' position on the applicability of international law to confront cybersecurity threats

According to John D. Negroponte, who was the first US Director of National Intelligence between 2005 and 2007, a *strategy* can be defined as "a statement of fundamental values, highest priorities, and orientation toward the future… and it is an action document as well"[10]. Along the past 25 years, the White House has developed national strategies regarding cyber security and its relationship with existing and prospective international law, which is based on the premise of a stable international environment where the cyberspace can be beneficial –and not damaging– for states[11].

While countries generally agree on the applicability of existing international law to the cyber domain, it is difficult to comprehend how law applies to particular cyber activities.

[10] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, "The National Intelligence Strategy of the United States of America. Transformation Through Integration and Innovation", October 2005, p. 2.

[11] *Cfr*. EGAN, B. J. "Remarks on International Law and Stability in Cyberspace", *US Department of State*, 10 November 2016, available at: https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.

Hence, the public presentation of states' positions is rather important to promote discussions and enhance cooperation[12]. In the last years, the US has made some efforts to publicly present the country's views regarding the application of international law to cyber activities. In this manner, the country sheds some light regarding its political and strategic stance in the case of an attack against the US.

2.1 The applicability and adaptability of international law to the cyber domain

In 2012, the Legal Advisor of the US Department of State, Harold Hongju Koh, presented the US position during the USCYBERCOM Inter-Agency Legal Conference at Ft. Meade (Maryland). Professor Koh affirmed that, according to the US perspective, established principles of international law are applicable in the cyber domain. However, he recognized the existence of differing opinions among states, and referred to the importance of building consensus to develop common understandings for the sake of stability in the international cyberspace.

According to the US position, cyber-attacks imply a use of force when the physical consequences are similar to a "traditional" armed attack, and hence, the US also reserves its right to self-defense in case of a cyber armed attack. These ideas are also applicable in the International Humanitarian Law realm, where both military and civilian objectives must be considered in order to evaluate consistency with the principles of distinction and proportionality, which "continue to guide the planning and execution of military cyber operations, even outside the context of armed conflict"[13]. In terms of attribution, professor Koh affirmed that cyber operations conducted by non-state actors are attributable to a state when such actors act under the State's direction or control, as established under the 2001 *Draft articles on Responsibility of States for Internationally Wrongful Acts* (article 8).

Professor Koh ended his speech in a more poetic tone to affirm that international law is not a straitjacket or purely a constrain, but "a body of 'wise restraints that make us free'"[14]. In other words, security in cyberspace is not just about the US compliance towards international law, but understanding how other countries understand the relationship between cyber issues and international law. To this end, "smart power", or

---

12 *Cfr. Ibid.*

13 KOH, H. H. "International Law and Cyberspace", *US Department of State*, USCYBERCOM Inter-Agency Legal Conference, 18 September 2012, available at: https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.

14 *Ibid*.

diplomatic efforts, are key to engage other countries in these debates and deal with the adaptation of international law to new domains with a multilateral approach.

2.2 The development of non-legally binding norms and confidence building measures

In 2016, US Legal Advisor Brian J. Egan presented a new and extended national position, and highlighted three main pillars in the US cyber security strategy, including: i) the *applicability of existing international law* to State activity in cyberspace in both peacetime and during armed conflict; ii) the development of international consensus on *non-binding norms of responsible State behavior* in cyberspace during peacetime; and iii) the development and implementation of practical *confidence-building measures* to facilitate inter-State cooperation on cyber-related matters[15].

i) Professor Egan reaffirmed the *applicability of existing international law* and the foundational elements of the US cyber strategy as previously stated by Professor Koh. Additionally, Professor Egan built on some of Professor Koh's ideas: regarding states' sovereignty in the cyberspace, he declared that "whenever a state contemplates conducting activities in cyberspace, the sovereignty of other states needs to be considered"[16]. However, he noted that "intelligence collection abroad" is not a violation of another state's sovereignty, but a "widespread and perhaps nearly universal practice"[17], which differs from cyber operations. He also signaled the fine line between lawful cyber operations and the international prohibition on unlawful intervention, which should be further clarified by states. And, he further emphasized the role of proxy actors or non-state actors and the need to target online criminal activities without violating International Human Rights Law. The 2012 US position regarding countermeasures was, in this same line, fully consistent with existing international law in the matter[18], and allowed for cyber-based countermeasures or non-cyber-based countermeasures, depending on states' discretion and the particular circumstances.

ii) According to Professor Egan's remarks, the US established a series of *voluntary non-binding norms*, hoping that these would guide states' responsible

---

15 *Cfr*. EGAN, B. J. "Remarks on International Law and Stability in Cyberspace", *op. cit.*

16 *Ibid*.

17 *Ibid*

18 This is, countermeasures require a prior internationally wrongful act that is attributable to another State. Such countermeasures must be directed only at the State responsible for the wrongful act and must meet the principles of necessity and proportionality, including the requirement that must be designed to cause the State to comply with its international obligations.

behavior and would create standards that may in the future crystallize into generally-binding customary international law. Among these, it is worth recalling the US promotion of national and economic security when encouraged states not to conduct or knowingly support cyber-enabled theft of intangible goods, activities potentially damaging critical infrastructure or causing harm.

iii) In order to understand states' divergent opinions regarding the role of international law in the cyberspace, the US promoted the implementation of *confidence building measures* leading to a reinforced cooperation between states. More specifically, Professor Egan commented on the role of requests for assistance from states in need to properly investigate cyber-crimes, including, for instance, the collection of electronic evidence, or the mitigation of malicious cyber activity from its territory. Without further specification, the US demanded transparency from states, which should openly share their national positions on the application of international law in cyberspace to make cooperation possible.

2.3 Peacetime cyber espionage and great power competition

In 2020, Hon. Paul C. Ney, Jr., General Counsel of the US US Department of Defense ("DoD"), placed particular emphasis on the relationship between the US cyber policy and international law regarding peacetime cyber espionage, which is not expressly prohibited under international law "even when it involves some degree of physical or virtual intrusion into foreign territory"[19]. In the absence of an international anti-espionage treaty, Ney put forward the fact that many countries carry out these cyber espionage actions, which proves that there is no customary international law norm against them. As a response, the most suitable strategy is "persistent engagement" in order to "defend forward" or, in other words, "conducting operations in cyberspace to disrupt and defeat malicious cyber activity that is harmful to U.S. national interests"[20]. This is especially true in the case of great power competition and the use of cyber capabilities, which would most notably justify the conduct of military cyber operations against Russia and China, but also North Korea and Iran in light of previous cyber-attacks against US national interests[21].

---

[19] NEY, JR., P. C. "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference", 2 March 2020, available at: https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

[20] *Ibid*.

[21] *Cfr*. *Ibid*.

As a final remark, it is also worth mentioning Ney's reference to the importance of non-binding norms, like the Tallinn Manual[22], in order to promote responsible State behavior in cyberspace, such as the norm relating to activities targeting critical infrastructure. Despite these being political commitments, they can help states providing security in the cyber realm. However, there has been little progress since Professor Egan introduced the idea of non-binding agreements in cyberspace in his 2016 speech, so these should be further integrated into tactical-level operations[23].

2.4 Due diligence and state responsibility

Soon after, in 2021, the US submitted its national position regarding the application of international law to the cyber domain to the 2019-2021 United Nations Group of Governmental Experts (UNGGE) on Advancing Responsible State Behavior in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266. Besides reiterating the US compromise towards the application of international law and its principles –the use of force, self-defense, sovereignty, the principle of intervention– to the cyber domain, the Biden administration in this case introduced the idea of *due diligence*, meaning that:

> "States have a general international law obligation to take steps to address activity emanating from their territory that is harmful to other States, and that such a general obligation applies more specifically, as a matter of international law, to cyber activities"[24].

Despite the lack of a customary international norm, the US understands that reasonable action must be taken in order to confront any harmful activity emanating from its territory. At the same time, the US recognized, as previously stated by Ney, that "remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a per se violation of international law"[25]; there is no explicit prohibition, but a slight interference in states' sovereignty as a result of the interconnected nature of the internet. There is a customary international norm, however, in terms of state

---

22 *Cfr*. SCHMITT, M. N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.

23 *Cfr*. *Ibid*.

24 Doc. A/76/136, *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*, General Assembly, 13 July 2021, p. 141.

25 *Ibid*.

responsibility for internationally wrongful acts, which is also applicable to the cyber domain according to the US national position, even when internationally wrongful cyber acts are perpetrated through proxies or non-state actors, but under the State's direction or control pursuant to the 2001 Draft articles on Responsibility of States for Internationally Wrongful Acts (articles 8-11).

In light of these various national positions, it can be affirmed that the US has always declared itself in favor of the applicability of international law in the cyber domain, so follows a coherent line of thought. Despite this clear posture, the US has also concretized particular aspects in every national position, in order to clarify and respond to the changing needs and developments of the international order.

III. The various contributions to national cyber security strategies

When considering the role of international law in the cyber domain, there are two competing rights whose importance might differ depending on the political dominant perspective: national security, likely supported by republican policymakers, and personal freedom, likely supported by liberal policymakers[26]. In this sense, it would be expected that different presidential administrations make different choices compared to their predecessors, have different priorities regarding security threats, and possibly choose to change policies.

On 22 May 1998, the Clinton administration published the Presidential Decision Directive 63, the first-ever national cyber policy in the United States. On 2 March 2023, the Biden administration published the latest White House cyber strategy, the National Cybersecurity Strategy (NCS). Interestingly, and considering political changes in between, a broad cyber-policy consensus is observed, despite political and ideological differences between the three Democratic and the two Republican administrations that have ruled the country during that period of time. However, there are various issues that have been more frequently discussed, or have been characterizing topics, regardless ideologies or the particular political tide. Ever since 1998 and until 2023, there has been an increasing perception of the threat posed by activities in the cyberspace; the US government has usually considered the –sometimes differing– role of markets and legislation to deliver security; the relationship and participation of the public and private

[26] *Cfr*. WEAVER, J. M. *The U.S. Cybersecurity and Intelligence Analysis Challenges*, *op. cit*., p. 4.

sectors has regularly been at the center of attention; and US administrations have constantly considered the role played by allies and adversaries[27].

Within this background, this section identifies and analyzes the main policies and lines of action defined by each administration separately to understand the varying US positions regarding the cyber domain and the relationship between international law and national legislation in this matter. It is worth mentioning in the first place that the Clinton administration (1993-2001) ruled during a naïve time technology-wise, when the Internet was still revolutionizing our lives. Hence, despite initiatives such as the Presidential Decision Directive 63[28], or the 2000 national plan[29] to address the problem of cyber security, it was not until the next presidential mandate that the importance of cyber security was more seriously addressed.

3.1 The George W. Bush administration (2001-2009): some prevention and many good intentions

The 9/11 attacks marked a turning point in the US security policies. Not only the role of armed non-state actors was highlighted but, soon after, the cyber domain acquired significant prominence as technology developed and sophistication increased[30]. The threat of a physical attack on US soil became global –in geographic terms– due to the lack of territorial borders in the cyber domain, which comprises a wide array of national infrastructures: access to clean water, public health, information and telecommunications, energy infrastructures or various forms of transportation, among others, could be damaged and directly jeopardize national security.

Within this context, the Bush administration adopted the *National Strategy to Secure Cyberspace* in 2003, which was meant to be an implementing guide for the National Strategy for Homeland Security, also complemented by the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. One of the main objectives of this guide was to coordinate efforts at all levels of society to confront cyber threats and vulnerabilities. While it was recognized that cyber-attacks can have an impact at any level –ranging from home users and small businesses to the whole international society–, at

[27] *Cfr*. HEALEY, J. "Twenty-Five Years of White House Cyber Policies", *Lawfare*, 2 June 2023, available at: https://www.lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies.

[28] *Cfr*. THE WHITE HOUSE, "Presidential Decision Directive 63/NSC-63", 22 May 1998, available at: https://irp.fas.org/offdocs/pdd/pdd-63.htm.

[29] *Cfr*. THE WHITE HOUSE, "National Plan for Information Systems Protection", 2000.

[30] *Cfr*. THE WHITE HOUSE, "The National Strategy to Secure Cyberspace", February 2003, pp. 5-6.

this point in time, the US government considered that large enterprises, and critical sectors and infrastructures should have a greater implication in confronting cyber threats, together with national issues and vulnerabilities to a lesser extent[31].

Briefly summarizing the main points, the 2003 National Strategy to Secure Cyberspace covered five priorities to guide cyber actions nation-wide:

> i) Priority I called for a *Security Response System* and, to that end, it highlights the role of public-private engagement to confront the coordination problem and enable rapid identification, information exchange, and remediation of malicious cyber activity.
>
> ii) Priority II called for a *Security Threat and Vulnerability Reduction Program*. On the one hand, it included strengthening law enforcement. On the other hand, it aimed at assessing and reducing vulnerabilities, and improving control systems and physical security by sharing best practices and evaluating and implementing new technologies.
>
> iii) Priority III called for *Security Awareness and Training Program*, which emphasized the importance of both public and private training to promote awareness at all levels.
>
> iv) Priority IV called for *Securing Governments' Cyberspace* focusing, again, on public-private cooperation, information sharing and assessment of threats and vulnerabilities.
>
> v) Priority V called for *National Security and International Cyberspace Security Cooperation*, in other words, improving capabilities and coordination closely working with industry and international organizations, including the *Council of Europe Convention on Cybercrime*.

In more concise terms, this strategy had three key objectives: improving the US response to cyberthreats (Priority I), reducing the threat (Priorities II, III and IV) and preventing it (Priority V), while considering that "the Strategy is not immutable; actions will evolve as technologies advance, as threats and vulnerabilities change, and as our understanding of the cybersecurity issues improves and clarifies"[32]. The Bush administration was fully aware of the need to adjust and amend the strategy over the years in order to properly confront vulnerabilities and avoid –to the extent possible– any potential disruption of US critical infrastructures, economy, or national security.

[31] *Cfr*. *Ibid*., p. 9.
[32] *Ibid*., p. 2.

However, the 2003 strategy lacked any kind of guidance establishing the importance of objectives and/or the implementation of priorities, so it has been referred to as a "market-reliant (or perhaps regulation-shy) approach"[33], or "just lists of actions, with little connection and with few ways to prioritize between them"[34], which were proof of good intentions but limited practical realization. It was affirmed in this sense that the 2003 National Strategy to Secure Cyberspace "was largely ignored"[35].

It is surprising that, later, the 2005 *National Intelligence Strategy* did not refer to cyber-threats in any way. The strategy recognized terrorism and weapons of mass destruction as main threats, and considered technology as a challenge and cooperation as an opportunity to confront transnational menaces. There is continued allusion to the "intelligence community", and one particular reference to the "intelligence '*cyber* community'"[36], but in no way revolving around the cyber-threat and cybersecurity idea, as herein set forth.

From an international standpoint, it is worth recalling that it was in 2001, during the Bush administration, when the *Budapest Convention on Cybercrime* was adopted as the first international treaty addressing cyber threats and seeking to harmonize national laws and cooperation among states. As a Council of Europe observer state, the US participated in the elaboration of the treaty, which entered into force on 1 July 2004. It wasn't until August 2006 when the US Senate unanimously ratified the convention, and finally entered into force on 1 January 2007 in the US. However, such ratification was not without controversy. On the one hand, critics considered this treaty unnecessary, since the US law already contained some of its cyber security obligations. While states are encouraged to cooperate for common purposes, such international cooperation does not require "dual criminality", and the Electronic Privacy Information Center considered the treaty "vague and weak" in its privacy protections[37]. On the other hand, praisers placed value on the attempt to harmonize national cyber norms. The treaty also provided useful exceptions to international cooperation in order to prevent abuses; the US could always refer to "essential interests" to deny cooperation in case of violation of the US

---

33 HEALEY, J. "Twenty-Five Years of White House Cyber Policies", *op. cit*.

34 *Ibid*.

35 NAKASHIMA, E. "Obama to Name Howard Schmidt As Cybersecurity Coordinator", *The Washington Post*, 22 December 2009, available at: https://www.washingtonpost.com/wp-dyn/content/article/2009/12/21/AR2009122103055.html.

36 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, "The National Intelligence Strategy of the United States of America. Transformation Through Integration and Innovation", October 2005, p. 15

37 *Cfr*. MCCULLAGH, D. "Senate Ratifies Controversial Cybercrime Treaty", *CNET*, 7 August 2006, available at: https://www.cnet.com/tech/tech-industry/senate-ratifies-controversial-cybercrime-treaty/.

Constitution. Hence, such faulty treaty was better than dealing with cybercrimes without an international legal framework[38].

Within this context, and despite confrontations between civil liberties and privacy concerns, the US fully participated in the treaty negotiation, which was entirely supported by the Bush administration and some groups from the industry sector[39]. However, it has been admitted that the novelty of technological advancements and the unawareness of cyberthreats by that time certainly were an obstacle for any international consensus among states on cybersecurity[40].

3.2 The Barack Obama administration (2009-2017): from defensive to offensive

After the promising but unfruitful efforts during the Bush administration, the 2010 National Security Strategy (NSS) addressed securing cyberspace as one of the country's interest for the sake of national and international security. Even though it was briefly mentioned, the Obama administration recognized the existing opportunities and threats derived from technological advances, and made two straightforward suggestions to enhance cyber security, these being "investing in people and technology" and "strengthening partnerships". As for the former, the 2010 NSS merely mentioned the importance behind cooperation between public and private entities and investment in research and development to improve resilience and raise awareness towards cyber security. As for the latter, the public-private nexus was reinforced, and the further development of laws and norms of conduct was brought to the table, what happened to be a main focus of attention for the Obama administration[41]. From the concise reference to cyber security, it can be extracted that cooperation and norms were the US main strategies to confront cyber threats at the beginning of the Obama administration. While diplomacy and international law were considered a preferred choice for dispute resolution, the use of force was not completely discarded, at least as a measure of last resort[42].

---

38 *Cfr* ANDERSON, N. "'World's Worst Internet Law' Ratified by Senate", *Ars Technica*, 4 August 2006, available at: https://arstechnica.com/uncategorized/2006/08/7421/.

39 *Cfr. Ibid*.

40 *Cfr.* LEWIS, J. A. "U.S. International Strategy for Cybersecurity"*, Testimony before the Senate Foreign Relations Committee: Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*, Center for Strategic and International Studies (CSIS), 14 May 2015, p. 1.

41 *Cfr.* THE WHITE HOUSE, "National Security Strategy", May 2010, pp. 27-28.

42 *Cfr*. *Ibid*., p. 22.

Shortly after these broad and still unspecific considerations, in July 2011, the US Department of Defense released its first Strategy for Operating in Cyberspace focusing on five initiatives[43]:

i) To treat cyberspace as an operational domain. The objective was to organize, train, and equip so that the US DoD could take full advantage of cyberspace's potential. As Lewis affirmed during Obama's presidency, "the use of cyber tools and techniques as an instrument of national power is now the norm"[44] so, despite awareness of risks attached, the potential benefits of the cyberspace, especially in terms of state power and competition, were at the center of attention during this time[45]. In line with the 2010 NSS, the strong focus on norms and legalism of the Obama administration presented an obstacle to properly respond to cyber-attacks, and raised concerns about the likely violation of national sovereignty in case of retaliatory acts against cyber-attacks[46].

ii) The DoD recognizes the need to constantly develop defense operating concepts to protect DoD networks and systems, which are highly dependent on cyberspace, which in turn is highly vulnerable. There is a strong focus on defense intended to prevent intrusions and act against potential adversary activities on DoD networks and systems. To this end, the Obama administration highlights the idea of "cyber hygiene" as a comprehensive effort to control DoD networks and systems and ensure their security and integrity[47].

iii) Enhancing partnership with other US government departments and agencies, particularly the Department of Homeland Security (DHS), and the private sector to enable a whole-of-government cybersecurity strategy[48]. Also in line with the 2010 NSS, the US government recognized "substantial progress" engaging the private industry and the rest of the government in working together towards the same ends[49]. Effective communication and sharing of information between the

---

43 *Cfr*. STEGON, D. "DoD Releases First Cyberspace Strategy", *Fedscoop*, 14 July 2011, available at: https://fedscoop.com/dod-releases-first-cyberspace-strategy/.

44 LEWIS, J. A. "U.S. International Strategy for Cybersecurity", *op. cit*., p. 1.

45 *Cfr*. *Ibid*., pp. 1-2.

46 *Cfr*. LEWIS, J. A. "Risk, Resilience, and Retaliation. American Perspectives on International Cybersecurity" in *Routledge Handbook of International Cybersecurity*, Tikk, E. and Kerttunen, M. (eds.), Routledge, 2020, p. 255.

47 *Cfr*. US DEPARTMENT OF DEFENSE, "Department of Defense Strategy for Operating in Cyberspace", July 2011, p. 7.

48 *Cfr*. *Ibid*., p. 8.

49 *Cfr*. STEGON, D. "DoD Releases First Cyberspace Strategy", *op. cit*.

public and private sectors were pinpointed as key activities to defend critical infrastructures and networks[50].

iv) To build robust relationships with US allies and international partners to strengthen collective cybersecurity. The 2011 DoD was meant to support the US *International Strategy for Cyberspace*, a diplomatic strategy to win support from key allies and emerging powers –like Brazil or India– to confront "enemies" or "potential dangers". The Obama administration chose to combine diplomacy, to strengthen partnerships; defense, to dissuade and deter; and development, to build prosperity and security, with the purpose of achieving "a peaceful and reliable cyberspace in that same spirit of cooperation and collective responsibility"[51].

v) Recruiting an exceptional cyber workforce providing education and training activities to cope with rapid technological innovation and cyber threats.

With these initiatives, the 2011 DoD Cyber Strategy appropriately expanded the 2010 NSS in terms of cyber-related issues, and did not contradict the previously stated (and very general) lines of action as established by the recently-elected Obama administration.

In the midst of this US cyber security strategic situation, various successive international cyber incidents took place and damaged the US increasingly strong cybersecurity appearance. In April 2013, for instance, the US National Public Radio website and Twitter account were hacked, false information was posted and confident data released as a result of the outbreak of the Syrian war[52]. Shortly after, the New York Times webpage and the Wall Street Journal twitter account, among other newspapers, were defaced by the Syrian Electronic Army (SEA)[53]. Another surprising event took place in November 2014, when it was discovered that a hacker group of the Democratic People's Republic of Korea (DPRK) had allegedly hacked Sony Pictures Entertainment (SPE) because of a soon to be released film, "The interview", in which the DPRK leader Kim Jong-un was to be assassinated[54]. The cyber-attack caused operation damage to Sony systems, and resulted in a massive data theft, and soon questions were raised about the feasibility of deterrence in cyberspace. Even though deterrence had been key in US

---

[50] *Cfr*. US DEPARTMENT OF DEFENSE, "Department of Defense Strategy for Operating in Cyberspace", *op. cit*., p. 8.

[51] THE WHITE HOUSE, "International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World", May 2011, p. 11.

[52] *Cfr*. BAEZNER, M. and ROBIN, P. "The Use of Cybertools in An Internationalized Civil War Context: Cyber Activities in The Syrian Conflict", *Center for Security Studies (CSS)*, 2017, p. 23.

[53] *Cfr*. *Ibid*., pp. 24 and 26.

[54] *Cfr*. HAGGARD, S. and LINDSAY, J, R. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace", *East-West Center*, Asia Pacific Issues, No. 117, May 2015.

strategy for a long time, the international context had changed significantly by that time, and armed non-state actors, as well as cyber threats posed additional challenges, which meant that deterrence was not such a useful strategy anymore[55]. As a matter of fact, it was soon recognized that the 2011 DoD Strategy for Operating in Cyberspace needed "significant reconsideration" because of constant challenges arising in a changing context where power competition was manifest and evidently growing[56].

In light of these events, the US had true reasons to fear the capabilities of the cyber domain and the malicious intentions of some of its main rivals: Russia and China were particularly active in military and economic cyber espionage, respectively; North Korea and various non-state actors demonstrated cyber-attack capabilities; and Iran also displayed its cyber developments and inflicted political pressure on the Obama administration. As a result, the US government disguisedly directed several cyber-attacks to Iran's main nuclear enrichment facilities, also known as the Natanz plant. The so-called Stuxnet "worm" –a type of malware– was supposed to signify the US first use of cyberweapons at such level, whose intentions apparently began during the previous Bush administration[57].

Stuxnet evidenced the reality behind cyber-attacks and the potential consequences to national critical infrastructure, and "the harbinger of a new generation of cyberthreats"[58]. Despite the 2010 NSS understanding of the use of force as a measure of last resort, the Obama administration allegedly acted against Iran's nuclear intentions for the sake of its own national and regional interests. Sanger affirmed to this respect, that:

> "Mr. Obama, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons –even under the most careful and limited circumstances– could enable other countries, terrorists or hackers to justify their own attacks"[59].

---

55 *Cfr.* LEWIS, J. A. "U.S. International Strategy for Cybersecurity", *op. cit.*, p. 3.
56 *Cfr. Ibid*., p. 4.
57 This operation was known as *Olympic Games*, which allegedly began during the Bush administration. *Cfr*. SANGER, D. E. "Obama Order Sped Up Wave of Cyberattacks Against Iran", *The New York Times*, 1 June 2012, available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.
58 WEINBERGER, S. "Is This the Start of Cyberwarfare?", *Nature*, Vol. 474, 9 June 2011.
59 SANGER, D. E. "Obama Order Sped Up Wave of Cyberattacks Against Iran", *op. cit*.

In other words, President Obama was fully aware that the US administration was using force, as commonly understood and generally prohibited by international law, against a potentially nuclear enemy. In this same line, the 2012 national position of the US regarding cyber law expressly considered "operations that trigger a nuclear plant meltdown" as cyber activity that constitutes a use of force[60]. However, the Obama administration did not hesitate to use cyber weapons against Iran despite its incompatibility with international law and the risky consequences to the US own security.

As a continuation of this perceived shift in the US cyber position, the institutional 2015 *DoD Cyber strategy* was explicitly defined as "an aggressive, specific plan for achieving change"[61], which sought to be ready to confront the increasing use of cyberattacks by both states and non-state actors. The new course of action included technical objectives, such as developing new tools and approaches, but also proactive strategic objectives, such as "control conflict escalation and shape conflict environment at all stages"[62]. Besides, building alliances and partnerships was a sustained purpose, which included strengthening the US cyber dialogue with China in light of the advanced cyber capabilities of the country[63].

It is remarkable, though, that the 2016 national position of the US regarding cyber law excludes any reference to the use of force, except for the following statement: "In certain circumstances, one State's non-consensual cyber operation in another State's territory *could* violate international law, even if it falls below the threshold of a use of force"[64]. Such vague assertion, which is full of potential nuances, apparently seeks to excuse US past activities, and allows for exceptions and permitted uses of force under the cyber domain.

The initial broadness and vagueness of the Obama administration towards cyber activity soon turned into action as a result of the rapidly changing international environment, which was posing major threats to the US. Despite the strong focus on legalism and defensive strategies, the US position on the use of force with regards to the cyber domain shifted towards a more offensive strategy in the interest of national security.

---

60 *Cfr*. KOH, H. H. "International Law in Cyberspace", *op. cit*.
61 US DEPARTMENT OF DEFENSE, "The DoD Cyber Strategy", April 2015, p. 33.
62 *Ibid*., pp. 14 and 26.
63 *Cfr*. *Ibid*., p. 27.
64 EGAN, B. J. "Remarks on International Law and Stability in Cyberspace", *op. cit*.

3.3 The Donald Trump administration (2017-2021): the centrality of power?

In January 2017, Donald Trump became the US President, precisely when Russia was being accused of hacking the recently held US presidential elections. Even though Russian cyber-attacks were not so much partisan, but a display of power[65], it was widely understood that Russia violated basic principles of international law by interfering in US politics and cyber security[66]. As Donald Trump did not recognize Russia's intervention, his response posed additional questions on how, or to what extent, would this event impact the US policy on cybersecurity.

Considering the tumultuous cyber environment of the time[67], and the dubious and unclear response to cyberthreats from the Obama administration, the following Trump administration adopted the first National Security Strategy in order to "keep America safe in the cyber era"[68], among other objectives, which presented a strong focus on American sovereignty and national security interests, while portraying a firmly patriotic stand:

> "The Internet is an American invention, and it should reflect our values as it continues to transform the future for all nations and all generations. A strong, defensible cyber infrastructure fosters economic growth, protects our liberties, and advances our national security"[69].

To that end, the 2017 National Security Strategy acknowledges, once more, the importance of the public-private partnerships to confront the cyber-threat from a comprehensive perspective, and prioritized the protection of critical infrastructure, among other things[70]. Despite the existing role of the government to enforce the rule of law, the republican Trump administration supported the "limited" participation of the state[71]. From an international standpoint, the role of state and non-state actors in the cyber domain was recognized, and –unsurprisingly– China and Russia were identified as competitors, and Iran and North Korea as rogue states to fight back[72]. Even though compliance with

---

65 *Cfr*. KOH, H. H. "The Trump Administration and International Law", *Washburn Law Journal*, Vol. 56, 2017, p. 451.

66 *Cfr. Ibid*., p. 450.

67 It is worth remembering the 2014 North Korean cyberattack on Sony Pictures and the Iranian cyberattack on the casino company Sands Las Vegas Corporation. Also, both Chinese and Russian hackers increased their cyber activity during that time. *Cfr*. PAGLIERY, J. "Iran Hacked an American Casino, U.S. Says", *CNN Business*, 27 February 2015, available at: https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html.

68 The White House, "National Security Strategy of the United States of America", December 2017, p. 12.

69 *Ibid*., p. 13.

70 *Cfr*. *Ibid*., p. 12.

71 *Cfr*. *Ibid*., p. 13.

72 *Cfr*. *Ibid*., p. 25.

international law is broadly assumed, the US government recalled that "will use all of its instruments of power to defend US interests and to ensure common domains –including the cyber domain– remain free"[73]. It is worth stating, however, that this National Security Strategy, as such, comprises a range of broad priorities and objectives without clear and specific application guidelines.

Soon after, in September 2018, Trump signed the National Cyber Strategy, which was considered by the government itself "the first fully articulated cyber strategy for the United States since 2003"[74]. The Trump administration integrated the National Cyber Strategy in a larger political context as part of the National Security Strategy, illustrating the increasing role of states' involvement in cyberspace[75].

The 2018 National Cyber Strategy was based on four fundamental pillars, including: Protecting the American People, the Homeland, and the American Way of Life (Pillar I); Promoting American Prosperity (Pillar II); Preserving Peace Through Strength (Pillar III); and Advancing American Influence (Pillar IV). Among the multiple policies considered, the Strategy highlighted the so-mentioned importance behind cooperation between the public and private sectors, risk management approaches, securing physical infrastructure or encouraging the implementation of best practices among stakeholders[76]. However, the Trump administration opposed the previous Obama administration on various areas, which are reflected in the 2018 National Security Strategy:

i) Obama's legalism vs Trump's imposition of consequences: there is a significant shift between administrations, as the former focused on developing norms while the latter focused on implementing them, and imposing consequences in case of violations (Pillar III), also referred to "response and retaliation"[77]; previous efforts to create norms should be secondary, while imposing consequences should come first[78].

---

[73] *Ibid*., p. 45.

[74] THE WHITE HOUSE, "President Trump Unveils America's First Cybersecurity Strategy in 15 Years", 20 September 2018, available at: https://trumpwhitehouse.archives.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.

[75] LEWIS, J. A. "Risk, Resilience, and Retaliation. American Perspectives on International Cybersecurity", *op. cit*., p. 253.

[76] ATKINSON, Jr., W. H. "A Review of the Trump Administration's National Cyber Strategy: Need for Renewal and Rethinking of the Public-Private Partnership in U.S. National Security Policy", *Institute of World Politics*, 22 October 2020, available at: https://www.iwp.edu/active-measures/2020/10/22/a-review-of-the-trump-administrations-national-cyber-strategy-need-for-renewal-and-rethinking-of-the-public-private-partnership-in-u-s-national-security-policy/#_ftn42.

[77] LEWIS, J. A. "Risk, Resilience, and Retaliation. American Perspectives on International Cybersecurity", *op. cit*., p. 253.

[78] *Cfr*. *Ibid*., p. 256.

Despite previous tedious efforts to reach a cyber agreement among the United Nations, the Trump philosophy was based on the centrality of power, which reflected a unilateral approach, although including joint actions with close allies, or like-minded countries (Pillar IV). Instead of coordination and cooperation, the US security policy strongly focused on national interests and rights, while avoiding and withdrawing from multilateral treaties[79], despite the changing international environment becoming conflictive and unstable[80]. Considering Trump's nationalistic ideas and approaches, the US government believed that "the goals of its cyber opponents for an agreement on cybersecurity are largely intended to impede the US and its allies more than themselves"[81], so distrust and punishment seemed to be the order of the day. One positive note is that the Trump administration continued with Obama's conversations on cyber security with Chinese counterparts, that covered objectives such as countering economic espionage or further developing international norms on cyber security[82].

ii) Obama's indecision and diplomacy vs Trump's deterrence policies: unlike the uncertainty and indecisiveness characterizing the Obama administration, the Trump administration established a more robust approach to cybersecurity, more particularly, a US-led international cyber deterrence initiative (Pillar III) to develop a common approach among like-minded countries to respond to malicious cyber-attacks[83]. Instead of a diplomatic approach, the US government shifted towards a deterrence approach against competitors, including cyber operations among military operations[84]. With this strategy, the Trump administration was determined to guide states' actions on what constitutes responsible state behavior in cyberspace to deter and punish in case of malicious cyber activity. As a matter of fact, the US government implemented significant cyber operations against Russian authorities,

---

79 Regarding the Trump administration's withdrawal from multilateral treaties, see Bellinger III, J. B. "The Trump Administration's Approach to International Law and Courts: Are We Seeing a Turn for the Worse?", *Case Western Reserve Journal*, Vol. 51, Issue 1, 2019, pp. 21-24.

80 *Cfr*. LEWIS, J. A. "Risk, Resilience, and Retaliation. American Perspectives on International Cybersecurity", *op. cit*., p. 254.

81 *Ibid*.

82 *Cfr*. EGAN, B. J. "Remarks on International Law and Stability in Cyberspace", *op. cit*, p. 144.

83 Such nuclear concepts could have been misleading in the cyber domain, since these are very different kinds of "weapons". *Cfr*. LEWIS, J. A. "Risk, Resilience, and Retaliation. American Perspectives on International Cybersecurity", *op. cit*., p. 256.

84 *Cfr*. NEY, JR., P. C. "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference", *op. cit*.

after the interference in the 2018 presidential elections, and Iranian authorities, after a US drone was brought down and oil tankers were attacked[85].

On a positive side, the Trump administration surprisingly committed to "encourage universal adherence to cyber norms, international law, and voluntary non-binding norms to achieve predictability and stability in cyberspace" in Pillar III, while working with "foreign government partners" and other stakeholders in Pillar IV[86]. There have been various opinions regarding Trump's commitment to international law during his administration: while Koh referred to "the relative defiance of the US administration toward international law since the election of President Donald Trump"[87], Ney's statement signaled the US proper application of international law in the cyber domain as "a Nation dedicated to the rule of law"[88]. The truth is that, perhaps contrary to the expectations, the importance of cyberspace and the role of international law was taken into consideration. A good example of this was the adoption of a set of cybersecurity principles for space technology to enforce security and resilience into space systems or, as the US Department for Homeland Security posed it, "the first comprehensive cybersecurity policy for systems used in outer space and near space today"[89]. Also worth recalling is the US active role in the United Nations Group of Governmental Experts (GGE) on information and telecommunications, which started during Obama's administration and continued during Trump's administration, in which states came to agreements on soft law initiatives to guide states' behavior in cyberspace[90].

Lastly, it is also worth mentioning the 2019 National Intelligence Strategy (NIS), which prioritizes cyber-threats over terrorism and the proliferation of weapons of mass destruction, and entrusts National Intelligence services to collect information and hence address cyber security threats from state and non-state actors. Even though objectives are only broadly stated and no specific implementation approach is specified, the cyber activities of the 2019 NIS generally match the 2018 National Security Strategy, including

---

85 *Cfr*. FIDLER, D. P. "President Trump's Legacy on Cyberspace Policy", *Council on Foreign Relations*, 2 December 2020, available at: https://www.cfr.org/blog/president-trumps-legacy-cyberspace-policy.

86 *Cfr*. ATKINSON, Jr., W. H. "A Review of the Trump Administration's National Cyber Strategy: Need for Renewal and Rethinking of the Public-Private Partnership in U.S. National Security Policy", *op. cit*.

87 KOH, H. H. "The Trump Administration and International Law", *op. cit*., p. 413.

88 NEY, Jr., P. C. "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference", *op. cit*.

89 US DEPARTMENT OF HOMELAND SECURITY, "Trump Administration Launches First Cybersecurity Principles for Space Technologies", 4 September 2020, available at: https://www.dhs.gov/archive/news/2020/09/04/trump-administration-launches-first-cybersecurity-principles-space-technologies.

90 *Cfr*. EGAN, B. J. "Remarks on International Law and Stability in Cyberspace", *op. cit*., pp. 141-142.

the purpose to "deter, disrupt, and defend against threats from foreign intelligence entities and insiders to protect U.S. national and economic security"[91].

Up to this point, the US cybersecurity strategy has dealt with the "promise/peril dilemma", in which perils –or threats– of new information technologies have exceeded prospective promises –or opportunities–. Also, and despite particularities, the Trump and previous administrations' positions remained generally consistent: besides distinctive approaches and other unpredictable and controversial international actions, international law and institutions have been generally respected, and it has been a generalized opinion that existing international law applies to state conduct in cyberspace. In particular, the Trump administration has been regarded as "consequential but not transformative"[92], which proves that, in practice, US national approaches to cyber-threats have slightly evolved, but have been similar overall.

3.4 The Joe Biden administration (2021-2024): a shift to a more regulation-focused approach

When President Joe Biden reached the presidency in January 2021, three main lines of action were established in the cybersecurity realm. First, considering the rapid technological development, the US administration placed emphasis on modernizing national defenses. Second, as a global threat, the US sought to confront cybercrime from an international perspective, enhancing collective defense and cooperation. Third, the US positioned itself as a powerful counterpart as a result of great power competition and the geopolitical context of the time. The US Senior Administration Official, who was briefing to the press, placed particular emphasis in the protection of critical infrastructure, which, to his view, was not strict enough to address the increasing cyber-threats[93].

In light of existing weaknesses, the Biden administration presented the Industrial Control System Cybersecurity Initiative –or ICS initiative– as voluntary measures to enhance a whole-of-nation approach for the public and private sectors to cooperate for the sake of cybersecurity. Despite previous administrations' statements regarding the protection of critical infrastructure and the importance of the public-private relationship, the US Senior Administration Official admitted that there is "no strategic, coordinated

---

91 THE WHITE HOUSE, "National Intelligence Strategy of the United States of America", 2019, p. 14.

92 FIDLER, D. P. "President Trump's Legacy on Cyberspace Policy", *op. cit*.

93 *Cfr*. THE WHITE HOUSE. "Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure", 28 July 2021, available at: https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/28/background-press-call-on-improving-cybersecurity-of-u-s-critical-infrastructure/.

requirement for the cybersecurity of critical infrastructure", which leads to questioning whether the Biden administration was aiming for different, practical results, somehow differing from previous efforts[94].

In 2022, the Biden administration adopted the National Security Strategy (NSS) and the National Defense Strategy (NDS) to confront a "decisive decade", in which deterrence and the People's Republic of China (PRC) posed the greatest challenges[95]. Within the 2022 NDS, the cyberspace was transversally represented and highlighted as a threatening domain because of "unclear norms of behavior and escalation thresholds, complex domain interactions, and new capabilities"[96], so the importance of clear and common standards was portrayed. In this same line, the 2022 NSS already mentioned that the Biden administration was committed to the promotion of the UN General Assembly-endorsed framework of responsible state behavior in cyberspace, supporting common standards in the cyber domain[97]. Hence, building resilience through deterrence was a priority for US national security, also in the cyberspace domain[98], which was also aimed at countering competitors' malicious cyber activity[99].

Besides these broadly established strategies, in March 2023, the Biden-Harris Administration released a more specific National Cybersecurity Strategy (NCS) to replace the 2018 NCS, which considered some previous steps taken in order to enhance security in the cyberspace[100]. This guiding document –also– highlights the importance of the public-private partnership, or how the public and the private sector must collaborate in the interest of securing cyberspace. While cybersecurity responsibilities have been traditionally placed on individuals and small companies, the 2023 NCS calls for a shift in the burden, which should fall on bigger and more capable organizations to reduce cyber risks. Besides roles and responsibilities, resources must also be looked after. The

---

94 *Cfr*. *Ibid*.

95 *Cfr*. US DEPARTMENT OF DEFENSE, "The 2022 National Defense Strategy of the United States of America. Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review", 2022, p. III.

96 *Ibid*., p. 6.

97 *Cfr.* THE WHITE HOUSE, "National Security Strategy", October 2022, p. 34.

98 *Cfr.* US DEPARTMENT OF DEFENSE, "The 2022 National Defense Strategy of the United States of America. Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review", *op. cit*., p. 8.

99 *Cfr. Ibid*., p. 12.

100 These steps include the National Security Strategy, Executive Order 14028 (Improving the Nation's Cybersecurity), National Security Memorandum 5 (Improving Cybersecurity for Critical Infrastructure Control Systems), M-22-09 (Moving the U.S. Government Toward Zero-Trust Cybersecurity Principles), and National Security Memorandum 10 (Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems).

guidelines argue in favor of long-term investments that consider both current and upcoming threats, referring to a "resilient future"[101]. More particularly, the 2023 NCS consists of five main pillars, which set out priorities in the cybersecurity domain, including the following:

(1) *Defend critical infrastructure*: it calls for new cybersecurity requirements and, more specifically, the need to "construct consistent, predictable regulatory frameworks"[102] in order to secure critical infrastructure from a preventive –instead of reactive– point of view. One only needs to highlight the almost tragic events that took place in February 2021 in Oldsmar (Florida), when unknown hackers remotely accessed the water supply system and attempted to inject lye into the local water[103]. In this vein, the US government aims at harmonizing regulations according to international and federal standards, hence avoiding duplication and further harm.

(2) *Disrupt and dismantle threat actors*: the public-private partnership is also highlighted when dealing with the threat posed by non-state actors, especially for information sharing and adaptation purposes. Collaborative disruption operations are meant to enhance collective awareness and quicker identify any malicious use of US-based infrastructure. Particular mention is made to the fight against ransomware and its potential impact on critical infrastructure. To this end, the US Administration focuses on the importance of international cooperation and the detection of illicit cryptocurrencies exchanges[104].

(3) *Shape market forces to drive security and resilience*: a regulatory framework is also to be adopted for personal data protection, which has been particularly vulnerable in the case of Internet of Things (IoT) devices that are increasingly present in our day-to day lives. The US Administration is committed to shifting liability onto software companies –instead of end-users– that are called to develop competitive, but also safer products[105]. Among other public

[101] THE WHITE HOUSE, "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy", 2 March 2023, available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

[102] THE WHITE HOUSE, "National Cybersecurity Strategy", *op. cit*., p. 7.

[103] *Cfr*. KLAAS, B. "We're Sleepwalking Toward a Cyber 9/11", *The Washington Post*, 14 September 2021, available at: https://www.washingtonpost.com/opinions/2021/09/14/were-sleepwalking-toward-cyber-911/.

[104] *Cfr*. THE WHITE HOUSE, "National Cybersecurity Strategy", *op. cit.*, p. 17.

[105] *Cfr*. *Ibid*., p. 20.

responsibilities, offering federal grant programs, improving accountability and developing a federal insurance response to catastrophic cyber events, are suggested[106].

(4) *Invest in a resilient future*: leading the innovative technology sector equally requires investment in security. The federal research, development and demonstration (RD&D) investments, in collaboration with the private sector, are aimed at securing innovation and opportunities offered, for instance, by quantum computing, whose applications jeopardize data protection. This is also the case in the energy sector, where investment in new infrastructure requires investment in secure, interoperable networks. As identity thefts are increasingly common, digital identity policies and technologies are generally encouraged. And, all these advancements and investments clearly require a suitable and well-trained American cybersecurity workforce[107].

(5) *Forge international partnerships to pursue shared goals*: the US Administration shows wide understanding of the international dimension of cybercrimes and cybersecurity. By means of various international agreements, the US seeks collaboration with its allies and partners in order to confront threats arising from states –such as China– and non-state actors. As a two-way relationship, the US aims at assisting and strengthening the capacity of its partners according to the national interest. International strategic collaboration is meant to reinforce global norms and secure global supply chains[108].

On this occasion, the Biden administration sets more concrete and functional priorities, trying to increase the plausibility of overall objectives. In more specific terms, there are five aspects of the cyber strategy that clearly differ from that of previous administrations:

i) The preceding market-focused approach shifts towards a regulation-focused approach, as demonstrated by strategic objective 1.1 of the 2023 NCS:

> "While voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes. Today's marketplace insufficiently rewards—and often disadvantages—the owners and operators of

[106] *Cfr*. *Ibid*., pp. 21 and 22.
[107] *Cfr*. *Ibid.*, pp. 23-27.
[108] *Cfr*. *Ibid.*, pp. 29-33.

critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cyber incidents"[109].

The importance placed on cyber security regulation –or regulation in general– is one of the key aspects that differentiate the Republican administrations' approach from the Democratic administrations' approach: while the former perceive new regulation as problematic for markets, the latter consider the potential failure of markets and hence the need for new regulation. In this sense, the Bush and the Trump administrations reflect a more market-focused approach, and the Obama and the Biden administrations reflect a more regulation-focused approach.

Even though the 2023 NCS replaces the 2018 NCS, and despite this policy shift, it "continues many of its priorities" and "carries forward and evolves many of the strategic efforts initiated"[110]. In other words, the latest NCS is a continuity strategy, respectful towards previous efforts, which does not seek to abruptly break with the past, despite changes in Government.

ii) The Biden administration introduced changes in the public-private partnership in order to reallocate responsibility, that had usually fallen on individual users and small organizations. Instead, the 2023 NCS stated, that great efforts should come from "the most-capable and best-positioned cyber actors to make our digital ecosystem secure and resilient"[111], like the Federal Government. Also, the 2023 NCS describes a model of "collaborative defense" in which risk and responsibility are equally distributed.

Collaboration between public and private agencies is key to define sector-by-sector needs and assess gaps by means of technology solutions –such as improved cloud-based services– for information sharing and coordination. However, the Federal Government commits itself to be a "model for private sector emulation", providing a unified, coordinated, whole-of-government response, while modernizing technology systems to appropriately protect the National Security Systems' (NSS) most sensitive data[112].

Therefore, the Biden administration went beyond previous administrations in developing the public-private partnership, and assigned an increased responsibility

[109] *Ibid*., p. 8.
[110] HEALEY, J. "Twenty-Five Years of White House Cyber Policies", *op. cit*.
[111] THE WHITE HOUSE, "National Cybersecurity Strategy", *op. cit.*, p. 4.
[112] *Cfr*. *Ibid*., p. 13.

between the public and the private sectors in their activities in the cyber domain. It is important to recall that, as both sectors operate differently in the day-to-day running of their functions, balancing responsibilities might take years, even if they work in the same directions towards the same objectives[113].

iii) Generally, all different US Administrations before had focused on the "promise/peril dilemma". However, President Joe Biden's strategy set aside threats and focused on the opportunities of a properly implemented cybersecurity policy. The 2023 NCS marked a turning point in this sense, and recalled the importance of "investing in and building toward a future digital ecosystem that is more inherently defensible and resilient"[114]. More specifically, long-term investment in areas of research and development is promoted, while coordination is also considered necessary. In order to avoid criticism from private companies against state intervention, the 2023 NCS also signaled, that "minimally invasive actions will produce the greatest gains in defensibility and systemic resilience"[115]. To these ends, the Federal Government offered federal grant programs to the private sector in order to make the most of opportunities and build a stronger partnership and enhance security[116].

iv) Besides this list of priorities, the 2023 NCS stands out for establishing an "actual" strategic concept for the first time, instead of just "a laundry list of needed actions"[117]. Professor Jason Healey, member of the Office of the National Cyber Director, which was in charge of drafting the 2023 NCS, believes that strategic concepts are meant to be simple, short and expandable, this meaning that "practitioners can take the basic strategic idea and unpack it to develop deeper objectives in line with the established concept"[118]. The lack of connection between actions and objectives was more evident in previous strategies, where there was no guidance into how to implement policies in a practical and realistic manner. However, the Biden administration aimed at improving this by building a strong

[113] *Cfr*. HEALEY, J. "Twenty-Five Years of White House Cyber Policies", *op. cit.*
[114] THE WHITE HOUSE, "National Cybersecurity Strategy", *op. cit*., p. 5.
[115] *Ibid*.
[116] *Cfr*. *Ibid*., p. 21. Also, *Cfr*. HAMIN, M. *et. al*, "How will the US counter cyber threats? Our experts mark up the National Cybersecurity Strategy", *Atlantic Council*, 3 March 2023, available at: https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/the-us-national-cybersecurity-strategy-mark-up/.
[117] HEALEY, J. "Twenty-Five Years of White House Cyber Policies", *op. cit.*
[118] *Ibid*.

foundation or, in this case, a simple but unifying strategy[119]. As also observed in the previous focus on opportunities, the US government presented a forward-looking strategy to be applicable in the long-run.

v) Instead of disrupting or deterring adversaries, the Biden administration focused on "countering adversaries", which implies a more proactive stance. US adversaries have not changed, though. The 2023 NCS identifies China, Russia, Iran and North Korea as countries that are not only using the cyber domain with malign purposes, but have also shown a lack of respect towards the rule of law and human rights, also in the cyber domain, which certainly threatens both U.S. national security and economic prosperity[120]. It is well admitted that "the People's Republic of China (PRC) now presents the broadest, most active, and most persistent threat to both government and private sector networks…"[121]; but Russia does not lag behind, since cyberattacks have been lately used to coerce sovereign countries, or harbor transnational criminal actors, as observed in recent events, such as the 2022 invasion of Ukraine. For their part, Iran and North Korea should not be underestimated, as their sophistication and willingness to conduct malicious activity in cyberspace is reinforced…"[122].

While the 2023 NCS has been defined as "commendable", the need for continuing work has also been recognized[123], and others considered this strategy as "extremely conservative"[124]. Again, the insufficient reference to specific actions and policies has been recalled. Besides, the strategy also fails to properly cover the impact of cyber activity in the international realm, in which cooperation among states and private companies could play a greater role in granting cyber security in the national realm[125]. However, the 2023 NCS was a symbol of continuity with respect to previous administrations' strategies, whether Republican or Democratic, which, at least, shows some willingness to build

---

[119] *Cfr*. HEALEY, J. "A One-Page Cyber Strategy", 9 November 2020, available at: https://www.sipa.columbia.edu/sites/default/files/2023-03/One-Page%20Cyber%20Strategy_9Nov2020.pdf.

[120] *Cfr*. HEALEY, J. "Twenty-Five Years of White House Cyber Policies", *op. cit*.

[121] THE WHITE HOUSE, "National Cybersecurity Strategy", *op. cit.*, p. 3.

[122] *Ibid*.

[123] *Cfr*. HAMIN, M. *et. al*, "How will the US counter cyber threats? Our experts mark up the National Cybersecurity Strategy", *op. cit*.

[124] WHYTE, C. "How the US DOD Cyber Strategy changes national cyber defense", *CSO*, 19 October 2023, available at: https://www.csoonline.com/article/655937/how-the-us-dod-cyber-strategy-changes-national-cyber-defense.html.

[125] *Cfr*. HAMIN, M. *et. al*, "How will the US counter cyber threats? Our experts mark up the National Cybersecurity Strategy", *op. cit*.

strong foundations for cyber security policies to endure and positively impact the cyber domain.

IV. Looking ahead: prospective developments in the new Trump administration

On 12 September 2023, still under the Biden administration, the US Department of Defense (DoD) presented an unclassified summary version of the classified 2023 DoD Cyber Strategy to broadly inform about the government's line of action to implement the existing national cybersecurity strategies[126]. The DoD highlighted the importance of the geopolitical environment, and recalled the role played by great power competition and, more precisely, by Russia and China as US adversaries with malicious purposes[127].

At the national level, and in line with the 2023 NCS, the DoD stood for a whole-of-government approach and public-private partnerships to jointly work for the sake of national interests, and committed to the investment in trained people, innovative reforms and strengthening cyber capabilities. In this sense, the 2023 DoD strategy has been referred to as "the best federal promise of real assistance the private sector has ever seen"[128], thus recognizing the so-long intended cooperation between the public and private sectors for cyber security purposes. At the international level, the view was also shared in between strategies: the DoD was said to work towards increasing capacities and capabilities in a two-way relationship with allies and partners, who opt for technical cooperation and the reinforcement of norms in the cyber domain. Interestingly, the DoD effectiveness assessment has been based on past experiences, which has led to the conclusion that cyber capabilities must be used in concert with other instruments of national power for an appropriate deterrent effect or, in other words, by means of an integrated deterrence[129].

Lastly, it is also worth referring to the 2024 Report on The Cybersecurity Posture of The United States, which was adopted by the National Cyber Director, Harry Coker, Jr., in May 2024, in the last months of the Biden Administration. This report is innovative in that it gathers implementation efforts, accomplishments and trends from the previous year

[126] The 2023 DoD Cyber Strategy implements the priorities of the 2022 National Security Strategy, 2022 National Defense Strategy (NDS), and 2023 National Cybersecurity Strategy. Also, it builds upon and supersedes the 2018 DoD Cyber Strategy.

[127] *Cfr*. US DEPARTMENT OF DEFENSE, "2023 Cyber Strategy of the Department of Defense. Summary", *op. cit*., p. 4.

[128] WHYTE, C. "How the US DOD Cyber Strategy changes national cyber defense", *op. cit.*

[129] *Cfr*. US DEPARTMENT OF DEFENSE, "2023 Cyber Strategy of the Department of Defense. Summary", *op. cit*., p. 2. Also, *Cfr*. WHYTE, C., "How the US DOD Cyber Strategy changes national cyber defense", *op. cit.*

in order to show that the Biden administration has been proactive and concerned with strategies of the cyber domain[130]; it is a first-time explanation of how cyber policies have been implemented and what are the main areas of future focus.

Whether the next US administration might bring changes in the cyber domain is yet something to be seen. As a result of the recently held elections, Donald Trump will be holding the US presidency once again, so it is worth asking what will the following years look like for the cyber domain in the US. It might be the case that the Trump administration decides to implement major changes. Potential shifts revolve around creating voluntary –hence, not compulsory– standards for companies and other stakeholders in the private sector[131]. The non-regulatory market-based approach could place a strong burden on the industry, while enhancing conflicting roles between private objectives and public needs, or private investments and national security. The development of the public-private partnership is certainly a relevant aspect to keep an eye on. However, it might also be the case that the Trump administration decides to leave things as they are. This is a fairly reasonable option, since the Biden administration did not implement major changes, but maintained many of the first Trump's administration cyber policies, such as the increasing concern for the protection of critical infrastructure.

Great power competition will definitely be another aspect to consider closely. It has already been suggested that the Trump administration is likely to change the focus from Russia and North Korea to China and Iran[132], even more in response to international events, such as Iran's intervention in the Israeli-Palestinian conflict, and their impact on the US national security. Trump has already publicly supported Israeli settlers, Russia's annexation of parts of Ukraine, and high tariffs on Chinese goods, all of which are likely to increase cyber threats[133]. Hence, for the time being, an increased destabilization seems more plausible than continued stabilization.

V. Final conclusions

[130] *Cfr*. THE WHITE HOUSE, "2024 Report on the Cybersecurity Posture of the United States", May 2024, p. 2.

[131] *Cfr.* SABIN, S. "How Trump Could Change Cybersecurity", *AXIOS*, 3 September 2024, available at: https://www.axios.com/2024/09/03/donald-trump-2024-cybersecurity-agenda.

[132] For instance, *Cfr*. SABIN, S. "Trump, Biden, Harris Targeted in Iran Phishing Campaign, Google Finds", *AXIOS*, 14 August 2024, available at: https://www.axios.com/2024/08/14/google-biden-harris-trump-iran-cyberattacks.

[133] *Cfr*. LEMOS, R. "Trump 2.0 May Mean Fewer Cybersecurity Regs, Shift in Threats", *Dark Reading*, 15 November 2024, available at: https://www.darkreading.com/cloud-security/trump-20-mean-cybersecurity-regs-shift-threats.

The international community has not been able to appropriately adapt to the rapidly changing environment, strongly influenced by the threats posed by new technologies. In light of this difficulty, cyber strategies have been mostly considered at the national level, where national actions and self-interest have been prioritized[134]. As a result, cyber confrontations between states could certainly lead to uncertainty regarding differing interpretations of existing norms, even more considering the existing great power competition scenario[135], in which the US plays an influential role.

Despite this, the periodic US national positions to date have always been in favor of the applicability of international law to the cyber domain. Consistency with international law has been a characterizing remark, aimed at promoting stability in the cyber domain and adherence to international norms. Hence, national positions have reiterated the US compromise towards the application of international law and its principles –the use of force, self-defense, sovereignty, the principle of intervention– to the cyber domain, while have also introduced mechanisms, such as non-binding agreements and due diligence, to progressively adapt to the changing needs.

The US national strategy for the cyber domain has experienced slight changes along the years. While Democratic administrations have emphasized the importance of norms, Republicans have traditionally preferred market-focused approaches, which translated into high expectations placed in the private sector. However, in practice, US public strategies and cyber-related policies pretty much show a continuum of broadly-established measures with a lack of a learning from experience mindset.

One of the main problems identified seems to be that national strategies do not include a proper mechanism to measure their performance, and there is no analysis comparing the resources invested and the results obtained[136]. To these ends, creating a new office of cyber-regulation strategy has been suggested as an opportunity to improve security. Such office could be in charge of drafting the strategy, but also developing a proper implementation plan and monitoring enforcement[137].

---

[134] *Cfr*. WEAVER, J. M. *The U.S. Cybersecurity and Intelligence Analysis Challenges*, *op. cit*., p. 3.

[135] *Cfr*. DELERUE, F. *Cyber operations and International Law*, Cambridge University Press, 2020, p. 21.

[136] *Cfr*. US GOVERNMENT ACCOUNTABILITY OFFICE, "The U.S. Now Has a National Cybersecurity Strategy, but Is It as Strong as It Could Be?", 21 March 2024, available at: https://www.gao.gov/blog/u.s.-now-has-national-cybersecurity-strategy-it-strong-it-could-be.

[137] *Cfr*. HEALEY, J. "What the White House Should Do Next for Cyber Regulation", *Dark Reading*, 7 October 2024, available at: https://www.darkreading.com/vulnerabilities-threats/what-white-house-next-cyber-regulation.

Despite all the strategies considered at the national level, and the US prospective cooperation with partners and allies at the international level, the key question still might be when will the next cyber-attack take place. The lack of international standards and the broad (although not so disparate) cyber strategies adopted in the US give rise to doubts about whether a "cyber Pearl Harbor"[138] or a "cyber 9/11"[139] will at some point occur. One only needs to remember the ransomware attack launched in February 2024 to Change Healthcare, the largest health care payment processer in the United States, affecting administrative services, carried out, to a great extent, through the internet, and even disrupting patient care[140].

It seems evident that the second Trump administration will be less willing to regulate than the former Biden administration, as also observed during the first Trump administration. However, some kind of cybersecurity plan will be needed and demanded, considering the still evolving cyber threats and the unstable international context. While a national security focus is more likely than an international security focus in the upcoming years, the new Trump administration might find engagement with allies necessary, particularly cooperation with regional forces, such as the European Union. But, in light of unexpected actions in the previous Trump administration, upcoming strategies and policies in the cyber domain are rather difficult to predict.

VI. Bibliography

ALDER, S. "Change Healthcare Cyberattack Affected 100 Million Individuals", *The HIPAA Journal*, 24 October 2024, available at: https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/.

ANDERSON, N. "'World's Worst Internet Law' Ratified by Senate", *Ars Technica*, 4 August 2006, available at: https://arstechnica.com/uncategorized/2006/08/7421/.

ASSOCIATED PRESS, "Costa Rica, 'under assault' is a troubling test case on ransomware attacks", NBW News, 17 June 2022, available at: https://www.nbcnews.com/news/latino/costa-rica-assault-troubling-test-case-ransomware-attacks-rcna34083.

[138] BULLIMER, E. and SHANKER, T. "Panetta Warns of Dire Threat of Cyberattack on U.S.", *The New York Times*, 11 October 2012, available at: https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

[139] KLAAS, B. "We're sleepwalking toward a cyber 9/11", *op. cit.*

[140] Regarding this event, *Cfr*. ALDER, S. "Change Healthcare Cyberattack Affected 100 Million Individuals", *The HIPAA Journal*, 24 October 2024, available at: https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/.

ATKINSON, Jr., W. H. "A Review of the Trump Administration's National Cyber Strategy: Need for Renewal and Rethinking of the Public-Private Partnership in U.S. National Security Policy", *Institute of World Politics*, 22 October 2020, available at: https://www.iwp.edu/active-measures/2020/10/22/a-review-of-the-trump-administrations-national-cyber-strategy-need-for-renewal-and-rethinking-of-the-public-private-partnership-in-u-s-national-security-policy/#_ftn42.

BAEZNER, M. and ROBIN, P. "The Use of Cybertools in an Internationalized Civil War Context: Cyber Activities in the Syrian Conflict", *Center for Security Studies (CSS),* 2017.

BELLINGER III, J. B. "The Trump Administration's Approach to International Law and Courts: Are We Seeing a Turn for the Worse?", *Case Western Reserve Journal*, Vol. 51, Issue 1, 2019.

BULLIMER, E. and SHANKER, T. "Panetta Warns of Dire Threat of Cyberattack on U.S.", *The New York Times*, 11 October 2012, available at: https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

CORN, G. "Tallin Manual 2.0 – Advancing the Conversation", *Just Security*, 15 February 2017, available at: https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.

DELERUE, F. *Cyber operations and International Law*, Cambridge University Press, 2020, 513 p.

EGAN, B. J. "Remarks on International Law and Stability in Cyberspace", *US Department of State*, 10 November 2016, available at: https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.

FIDLER, D. P. "President Trump's Legacy on Cyberspace Policy", *Council on Foreign Relations*, 2 December 2020, available at: https://www.cfr.org/blog/president-trumps-legacy-cyberspace-policy.

HAGGARD, S. and LINDSAY, J, R. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace", *East-West Center*, Asia Pacific Issues, No. 117, May 2015.

HAMIN, M. *et. al*. "How Will the US Counter Cyber Threats? Our Experts Mark Up the National Cybersecurity Strategy", *Atlantic Council*, 3 March 2023, available at: https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/the-us-national-cybersecurity-strategy-mark-up/.

HEALEY, J. "What the White House Should Do Next for Cyber Regulation", *Dark Reading*, 7 October 2024, available at: https://www.darkreading.com/vulnerabilities-threats/what-white-house-next-cyber-regulation.

- "Twenty-Five Years of White House Cyber Policies", *Lawfare*, 2 June 2023, available at: https://www.lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies.
- "A One-Page Cyber Strategy", 9 November 2020, available at: https://www.sipa.columbia.edu/sites/default/files/2023-03/One-Page%20Cyber%20Strategy_9Nov2020.pdf.

KLAAS, B. "We're sleepwalking toward a cyber 9/11", *The Washington Post*, 14 September 2021, available at: https://www.washingtonpost.com/opinions/2021/09/14/were-sleepwalking-toward-cyber-911/.

KOENDERS, B. "Foreword", in Schmitt, M. N. (eds.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, pp. xxv-xxvii.

KOH, H. H. "The Trump Administration and International Law", *Washburn Law Journal*, Vol. 56, 2017.

- "International Law and Cyberspace", *US Department of State*, USCYBERCOM Inter-Agency Legal Conference, 18 September 2012, available at: https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.

LEMOS, R. "Trump 2.0 May Mean Fewer Cybersecurity Regs, Shift in Threats", *Dark Reading*, 15 November 2024, available at: https://www.darkreading.com/cloud-security/trump-20-mean-cybersecurity-regs-shift-threats.

LEWIS, J. A. "Risk, Resilience, and Retaliation. American Perspectives on International Cybersecurity" in *Routledge Handbook of International Cybersecurity*, Tikk, E. and Kerttunen, M. (eds.), Routledge, 2020, pp. 252-259.

- "U.S. International Strategy for Cybersecurity", *Testimony before the Senate Foreign Relations Committee: Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*, Center for Strategic and International Studies (CSIS), 14 May 2015.

MCCULLAGH, D. "Senate Ratifies Controversial Cybercrime Treaty", *CNET*, 7 August 2006, available at: https://www.cnet.com/tech/tech-industry/senate-ratifies-controversial-cybercrime-treaty/.

NAKASHIMA, E. “Obama to name Howard Schmidt as cybersecurity coordinator”, *The Washington Post*, 22 December 2009, available at: https://www.washingtonpost.com/wp-dyn/content/article/2009/12/21/AR2009122103055.html.

NEY, JR., P. C. “DOD General Counsel Remarks at U.S. Cyber Command Legal Conference”, 2 March 2020, available at: https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, “The National Intelligence Strategy of the United States of America. Transformation Through Integration and Innovation”, October 2005, 20 p.

PAGLIERY, J. “Iran hacked an American casino, U.S. says”, *CNN Business*, 27 February 2015, available at: https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html.

SABIN, S. “How Trump Could Change Cybersecurity”, *AXIOS*, 3 September 2024, available at: https://www.axios.com/2024/09/03/donald-trump-2024-cybersecurity-agenda.

- “Trump, Biden, Harris targeted in Iran phishing campaign, Google finds”, *AXIOS*, 14 August 2024, available at: https://www.axios.com/2024/08/14/google-biden-harris-trump-iran-cyberattacks.

SANGER, D. E. “Obama Order Sped Up Wave of Cyberattacks Against Iran”, *The New York Times*, 1 June 2012, available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

SCHMITT, M. N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, 598 p.

SNYDER, O. “The U.S. Cyber Security and International Law”, *Embry-Riddle Aeronautical University*, 15 December 2022, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4501857.

STEGON, D. “DoD Releases First Cyberspace Strategy”, *Fedscoop*, 14 July 2011, available at: https://fedscoop.com/dod-releases-first-cyberspace-strategy/.

THE WHITE HOUSE, “2024 Report on the Cybersecurity Posture of the United States”, May 2024, 29 p.

- “National Cybersecurity Strategy”, March 2023, 35 p.

- "National Intelligence Strategy of the United States of America", 2019.
- "President Trump Unveils America's First Cybersecurity Strategy in 15 Years", 20 September 2018, available at: https://trumpwhitehouse.archives.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.
- "National Security Strategy of the United States of America", December 2017, 58 p.
- "International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World", May 2011, 25 p.
- "National Security Strategy", May 2010, 52 p.
- "The National Strategy to Secure Cyberspace", February 2003, 60 p.

US DEPARTMENT OF DEFENSE, "2023 Cyber Strategy of the Department of Defense. Summary", September 2023.

- "Department of Defense Strategy for Operating in Cyberspace", July 2011, 13 p.

US DEPARTMENT OF HOMELAND SECURITY, "Trump Administration Launches First Cybersecurity Principles for Space Technologies", 4 September 2020, available at: https://www.dhs.gov/archive/news/2020/09/04/trump-administration-launches-first-cybersecurity-principles-space-technologies.

US GOVERNMENT ACCOUNTABILITY OFFICE, "The U.S. Now Has a National Cybersecurity Strategy, but Is It as Strong as It Could Be?", 21 March 2024, available at: https://www.gao.gov/blog/u.s.-now-has-national-cybersecurity-strategy-it-strong-it-could-be.

WEAVER, J. M. *The U.S. Cybersecurity and Intelligence Analysis Challenges*, Palgrave Macmillan, 2022, 142 p.

WEINBERGER, S. "Is This the Start of Cyberwarfare?", *Nature*, Vol. 474, 9 June 2011.

WHYTE, C. "How the US DOD Cyber Strategy changes national cyber defense", *CSO*, 19 October 2023, available at: https://www.csoonline.com/article/655937/how-the-us-dod-cyber-strategy-changes-national-cyber-defense.html.

Final conclusions

Cesáreo GUTIÉRREZ ESPADA
Emeritus Professor of Public International Law and International Relations
University of Murcia

1. Regarding the position of the European Union with regard to the application of international law in cyberspace, the issue that heads the analysis of this book, there are four, in my opinion, relevant conclusions:

A) The Union has been very clear about the applicability of current international law to cyberspace. Both the Declaration of November 2024 and a number of documents from the institutions confirm the position of the Union and its Member States in this respect.

The institutions of the Union have also confirmed the application of international law to cyberspace in specific areas; for example, the principles of sovereignty, non-intervention, the use of force, due diligence and countermeasures.

It is important to note the evolution in the European Union with respect to the principle of due diligence, which at present and for some years now is considered by the EU to be more forcefully binding.

It is also worth noting (although the common position expressed in the November 2024 Declaration does not mention this) the recognition by various EU bodies and institutions of the possible adoption of collective countermeasures, especially in response to the violation of obligations *erga omnes.*

B) There has been significant convergence in the position of Member States on the application of international law to cyberspace, which has paved the way for the development of a common Union position in this area, adopted, as already mentioned, in November 2024.

C) The primary law of the Union, and in particular the clauses of mutual solidarity and defence, can be interpreted, and this has been done by the European institutions, in the sense that they are applicable as a response to cyber-attacks of the necessary severity.

Likewise, secondary legislation has been equipped in recent years with instruments specifically designed to respond to cyberattacks, namely a regime of restrictive measures against those responsible for them, and the possibility of adopting collective anti-coercion measures that could, we believe, also be applied in the cyber sphere in the future.

D) Both the positions expressed by the institutions of the Union and the content of the legal acts adopted by them (for example, with regard to the definition of cyberattack or the obligatory nature of the principle of due diligence) can contribute to the progressive development of international law.

This would be consistent with Article 3 TEU, paragraph 5 (a text whose omission in the November 2024 Declaration is regrettable) and with the case law of the European Courts, thus contributing very positively to the establishment of global rules governing the conduct of States and other actors in this field, for the benefit of global security and peace but also the fundamental rights and freedoms of all human beings.

2. The official documents that States formally adopt in which they specify their position on cyberspace and the activities that take place in it have become an ideal way to find out in detail which international law regulations are applied and, more importantly, how they will be enforced. It is true that some of these texts are formulated in too general a way, especially in areas where there are still discussions, but for the moment they are the best way to take the pulse of the States. Let us not forget, moreover, that knowing how they think and what they consider to be a legal obligation is important in determining the *opinio iuris* on a subject that is still, at least to a large extent, in the shadows.

Spain, as a middle power among the fifteen most developed economies, should have its own Position on International Law in Cyberspace. One might think that there is no urgency, since the European Union has adopted a Common Position on this new domain (November 2024), but beyond the fact that one may not agree with everything it contains, a position of its own would be a unique opportunity for our government to clarify certain aspects that are still in doubt or, even better, and since we are talking about hypotheses, to take a step forward in other respects on which some states have not yet made a definitive statement.

In accordance with what is stated in chapter 2 of this book, some elements that would not go amiss would be an express mention of sovereignty as a norm, opting for flexible interpretations of the principle of non-intervention that allow for those operations of interference or manipulation that are of such concern to today's society (in the European Union, precisely, as this is being written, the scandal of the elections in Romania and the influence exerted on voters through social networks is still reverberating) or due diligence as an obligation, to demand responsible behaviour from other states but also to be consistent with what is happening in its own.

Our country should also make it clear that behaviour in cyberspace generates responsibility for states and that countermeasures or the state of necessity can be perfectly legitimate responses. And, why not, Spain could expressly pronounce itself on the so-called collective countermeasures that some states (few at the moment, yes) are already explicitly accepting in their respective strategies.

Resorting to the formula that each problem will be determined in the last instance and on a case-by-case basis is always a good option for our State to have a certain freedom of action. In an area such as cyberspace, moreover, where changes are rapid, it seems the appropriate option if we want to avoid official positions that quickly become outdated.

And I would like to finish, if the reader will allow me, by suggesting what is covered in chapter 2: that Spain should not be shy about committing itself, in general terms, to the protection of human beings in cyberspace:

- Defending the basic norms and principles of international humanitarian law is not, as some states claim, to militarise it, but to recognise a reality that recent armed conflicts have already shown.

And the same could be said of human rights: the temptations to restrict certain fundamental freedoms in cyberspace are many, but precisely for that reason the guarantees offered must be especially careful or cyberspace will irretrievably lose the essence of what it once was: that free environment that allowed human beings to escape from the limitations of the analogue world.

Controls will be necessary, of course, and they are already being put in place (the European Union's lengthy regulations in this regard or even the United Nations

Convention on Cybercrime are two good examples), but the necessary balance between freedom and abuse must always be sought.

3. Following the research carried out in chapter 3 of this book, it is fair to say that the overall cybersecurity strategy of both African and Latin American states has been able (and can) contribute positively to clarifying and deepening the legal regime applicable to cyberspace. Thus, the African Common Position on the applicability of international law to cyberspace represents the *opinio iuris* of 28.5% of the votes of the United Nations General Assembly and the 2022 report of the Inter-American Juridical Committee, for its part, reflects the position of 18% of those same votes.

In general terms, it could be said that there has been an evolution of interest in the cyber maturity of the States involved, although it is also true that there is still room for improvement. The 2024 *Global Cybersecurity Index* reveals that 39% of African states have already developed national cybersecurity strategies, as have 26% of Latin American and Caribbean states. The data clearly contrasts, however, with that which can be obtained in the European Union, given that in it 76% of its member states today have cybersecurity strategies.

In any case, African, Latin American and Caribbean states have an unwavering commitment to their cybersecurity, although this is only unequally realised:

- The African Union is committed to the adoption of legally binding standards for its member states (see the Malabo Convention, for example)

- The Organisation of American States, on the other hand, follows the path of non-binding acts and the creation of contact networks to advance cybersecurity that, if I may say so, could be described as ‘dialoguing’.

In both regions, however, there is probably an excessive focus on national cybercrime legislation, to the detriment of the technical aspects and good practices of real cybersecurity:

- In Africa, the focus is on control of the online space and surveillance, rather than on securing systems.

- In Latin America and the Caribbean the emphasis is on the creation of technical response teams and on capacity building in line with the financial resources available.

It is also worth noting that in both regions, all kinds of cyber-skills training activities are being developed through international cooperation, with the aim of presenting a united front against the global threat of cybercrime. All these efforts do not prevent the geopolitics of certain states (such as China, Russia, Israel or the United Arab Emirates) to extend or consolidate their power from being present in these areas of the world.

However, despite the progress made, a fundamental issue remains unresolved. For cybersecurity to make a significant contribution to 'international peace and security', more attention should be paid to regional approaches and their shortcomings. The scant consideration of a perspective of this nature is not a legal problem, but a political one; other regions and large states (the 'technological giants') refuse to advance in the international regulation of the Internet for purely strategic interests or take advantage of local loopholes to extend their influence and thus generate the dependence of others.

4. The so-called *information space*, as cyberspace is known in Asia, is posing many challenges for international law and for the different states and other actors. On the one hand, because of the peculiarities of this new domain; but, on the other hand, also because of the positions that states have been adopting.

China and Russia have not remained on the sidelines of the challenges, but neither have they remained on the sidelines of the threats that this *space of information poses* to their national and international interests. Hence the development of their official positions in the *Information Security Strategy of the Russian Federation* of 2021 and, in the case of the Chinese government, in the *Strategy of Cooperation in Cyberspace* of 2017.

Both strategies have allowed the two governments to verify the existence of common sections that have generated a common alliance:

- A *strategic,* alliance that is committed to developing hegemonic policies through binding legal instruments that take into account the special characteristics of the new domain.

- Also for a global governance of the Internet, which prevents it from being controlled by a few states.

And, finally, for the application of the principles of sovereignty and due diligence.

However, the duration of this strategic alliance will depend on the stability it offers to the policies of both states. But neither Beijing nor Moscow will hesitate to reverse their alliance on this issue if the wind does not blow in their favour.

5. In the international community, cyber strategies have been adopted mainly at the national level and, therefore, the actions and interests of each state have been prioritised. The result? Uncertainty; the uncertainty generated by different interpretations of the rules to be applied, especially in a scenario of competition between the great powers, in which, in any case, the United States of America plays a decisive role.

And what kind of role is that? To date, the United States has always considered international law to be applicable to cyberspace and, therefore, that its conduct as a state in this area should be consistent with the rules of international law. Thus, its positions on various issues have reiterated the US commitment to the application of international law principles such as the prohibition of the use of force, the right to self-defence or the principle of non-intervention *in and in cyberspace*, and, simultaneously, it has introduced concepts such as non-binding agreements or the principle of due diligence, in order to progressively adapt to the evolution of its interests and needs.

The US national strategy for cyberspace has undergone certain changes over the years. While Democratic administrations emphasised the importance of regulations, Republican administrations have traditionally favoured market-centred approaches, which translated into high expectations for the private sector.

One of the main problems identified is that national strategies do not include an adequate mechanism for measuring their performance and there is no analysis comparing the resources invested with the results obtained. To this end, and with the aim of improving security, it has been proposed to create a cyber-regulation strategy office. This office would be in charge of drafting the strategy, but also of developing an adequate implementation plan and of monitoring its fulfilment.

Despite all the strategies considered at the national level and the eventual international cooperation of the United States with partners and allies, the key question could still be when the next cyberattack will take place. The lack of international standards and the cyber strategies adopted in the United States raise doubts as to whether a 'cyber 9/11' will ever occur.

It is more than likely that the second Trump administration will be less willing to regulate the issue than the previous Biden administration. However, some kind of cybersecurity plan will be necessary, given the possible cyber threats and the unstable international context. While the focus in the coming years will most likely be on national rather than international security, the new Trump administration may consider agreements with others necessary, particularly cooperation with the European Union.

However, if we remember the unexpected decisions that Mr Trump made in his first term in the White House, neither the global strategy nor the specific policies that the Republican administration will adopt on cyberspace today seem easy to predict.