EXTENDED ABSTRACT

Cybersecurity and the international regulatory framework

From the fragility of soft law to the necessary and problematic adoption of a binding conventional instrument on a global scale.

Manuel Saldanha Póvoas da Costa Cabral

Cybersecurity is emerging as one of the most urgent and intricate challenges facing contemporary society. Growing global interconnectedness, dependence on digital technology and the rapid evolution of cyber threats present collective challenges whose solution or even mitigation does not seem to be achievable in the short term.

The World Economic Forum (WEF), based on a survey of leaders of various organizations, ranks "widespread cybercrime and insecurity in cyberspace" eighth among the most severe risks facing the world in both the short and long term.

Nevertheless, it is not easy to define a concept as broad and multifaceted as cybersecurity, or security in cyberspace.

Cyberspace must be understood as a Global Common. A domain or space shared by various states, but which is not the property of any one of them in particular, but rather a domain of common responsibility.

This cyberspace is a multifaceted terrain, which can be divided into five layers[1]: physical, network / IP, transport, applications, and the content and transactions layer.

The security of cyberspace therefore presupposes action at various levels, which, being interconnected, require different skills and an understanding of each of them.

The International Telecommunication Union (ITU)[2], the United Nations Specialized Agency for Information and Communication Technologies, defines cybersecurity as:

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.
Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- *Availability*
- *Integrity, which may include authenticity and non-repudiation*
- *Confidentiality"*

In addition to this definition, it is important to note that cybersecurity encompasses several areas of action. In this regard, Lino Santos and others[3] identify three areas of action, namely: simple protection (in which cyber-attacks are seen as threats to the availability, integrity and confidentiality of information and other assets); criminal prosecution (cyber-attacks are seen as criminally relevant acts) or defense of the state (cyber-attacks are seen as an act of war, putting the existence of the state at risk).

[1] Drake, W. J., Vinton, C. G., & Kleinwächter, W. (2016, January). Internet fragmentation: An overview. World Economic Forum

[2] Recommendation ITU-T X.1205 (adopted in the scope of Study Group 17 of the ITU Standardisation Sector, ITU-T SG17, April 2008), available at https://www.itu.int/rec/T-REC-X.1205-200804-I.

[3] Santos, L., Bravo, R., & Nunes, P. V. (2012). Proteção do ciberespaço: Visão analítica.

In view of these areas of action, the paper addresses the area of "State Defense", although from a broader perspective than that which seems to result from the proposal made by the authors cited. In fact, it seems that this area of action, as described, is fundamentally associated with the military dimension of State Defense. In the broader approach proposed, cyber-attacks do not necessarily have to be seen as acts of war in order to jeopardize fundamental pillars of the state, namely its political or social organization, such as:

- political or social organization, for example when campaigns are orchestrated to falsify or manipulate public opinion on a large scale via digital platforms, which could affect electoral results.
- economic organization in a country, for example, as a result of cyber-attacks, regardless of whether the perpetrators are public or private agents, which paralyze or significantly condition a certain critical infrastructure.

It is this broader understanding of the "Defense of the State" domain that we will consider in the development of this work. It should be noted, however, that the other domains cannot be ignored, given that the distinction between them is not always feasible. In particular, the distinction between "state defense" and "criminal prosecution" seems particularly demanding.

For a better understanding of this article, it is also important to clarify some legal concepts, such as international law and its sources, in particular what is meant by international convention and soft law.

Maria Luísa Duarte gives us a definition of Public International Law as being the "set of general rules and principles defined within the framework of the global legal order that aim to regulate the existence and functioning of the international community"[4].

With regard to the sources of international law, there is a consensus on the relevance of the contribution of Article 38(1) of the Statute of the International Court of Justice (ICJ)[5], which identifies a number of sources of law. Among them the Statute refers to international conventions or international treaties.

Maria Luísa Duarte's definition of soft law[6] is also relevant and useful for us. The author includes soft law among the non-typified sources of international law, considering that this concept is elastic and versatile. It is "quasi-law, soft law, normativity that is not entirely binding, as opposed to hard law". It is a source of law that breaks with a "dualist model of sources, inspired by the normative will of States, of express (treaties) or tacit (custom) consent".

Examples of soft law include resolutions of the deliberative bodies of an international organization (for example, resolutions of the United Nations General Assembly), political agreements, guidelines, codes of conduct, declarations of principles, etc.

Despite the difficulties in understanding the concept and its scope, cybersecurity is a relevant topic and there are many organizations, forums and working groups, both governmental and non-governmental, that discuss the issue with the aim of developing non-binding norms in which some principles are established with the purpose to contribute to the defense of states in the context of cyberspace.

Once this conceptual framework has been established, the following sections will describe the multiple forums in which cybersecurity is debated, from the perspective of state defense, and in which norms on cybersecurity are created. In this context, global forums will be analyzed, with a focus on the United

[4] Duarte, M. L. (2014). Direito internacional público e ordem jurídica global do século XXI. Coimbra Editora. P.27

[5] Statute of the International Court Of Justice, available at https://www.icj-cij.org/statute
Article 38

1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
   a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
   b) international custom, as evidence of a general practice accepted as law;
   c) the general principles of law recognized by civilized nations;
   d) subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

[6] Duarte, M. L. (2014). Supra n.º 4. P 156 e ss

Nations (UN) system. As for regional forums, the focus will be on the organizations in which Portugal is a Member. Special attention will be paid to the European Union (EU), within which there is extensive legislative activity on cybersecurity, although other organizations will also be studied.

Finally, the national context will also be addressed.

Cybersecurity and the United Nations

Within the complex United Nations system, the issue of cybersecurity has been debated at various levels.

UN General Assembly

Within the UN General Assembly, cybersecurity issues have essentially been debated within the First Committee (Committee on Disarmament and International Security) and the Third Committee (Social, Humanitarian and Cultural Committee), although the Second Committee (Economic and Financial Committee) also works on cybersecurity.

Within the First Committee in particular, two expert groups have been set up which have been key platforms for the discussion and drafting of soft-law, namely:

- Groups of Government Experts (UN GGEs);
- and the Open-Ended Working Group (UN OEWG).

The norms that have emerged from these Groups relate to the question of the applicability of existing international law to cyberspace and how international law can be applied in cyberspace. Another set of relevant norms relates to the responsible behavior of States in cyberspace and matters of international cooperation to strengthen cybersecurity.

More recently, the work of the UN OEWG has evolved into more operational issues, such as the creation of a list of relevant contacts in each Member State, to strengthen international collaboration.

UN Secretary-General

In addition to coordinating the United Nations System, the Secretary-General plays an important role in identifying challenges and threats, inspiring and influencing future actions by the UN system and its member states.

UN Security Council

The UN Security Council has not been particularly active in cybersecurity discussions. The Security Council has, however, organized Arria-formula meetings, which are informal and confidential meetings that allow Security Council members to have a frank and private exchange of views. At the invitation of one or more members of the Security Council, renowned experts in the area under discussion have taken part in these meetings. The model also allows for the participation of non-governmental entities.

International Telecommunication Union (ITU)

The ITU, created in 1865, is the oldest international governmental organization and the world's largest telecommunications organization, and has been a specialized agency of the United Nations since 1947.

The ITU's work in the field of cybersecurity is supported by the World Summit on the Information Society (WSIS - see "UN Forums on Internet Governance and the Information Society" below), which designated the ITU as facilitator of action line C5 "Strengthening trust and security in the use of ICTs".

Since then, the ITU's mandate on cybersecurity has been discussed at the Union's main Conferences and Assemblies, such as Plenipotentiary Conferences.

United Nations Educational, Scientific and Cultural Organization (UNESCO)

UNESCO is the UN's specialized agency that aims to contribute to peace and security by promoting international cooperation in the fields of education, science, culture, communication and information.

One of the aspects of UNESCO's work in the digital field is the action called "Internet for Trust - towards Guidelines for Regulating Digital Platforms"[7]. The guidelines that UNESCO intends to develop aim to safeguard freedom of expression, access to information and other human rights in the governance of digital platforms. At the same time, they address harmful content that can, according to UNESCO, be legitimately restricted under international human rights law and norms.

UN Forums on Internet Governance and the Information Society

It was 2003 when the first phase of the World Summit on Information Society (WSIS), organized by the United Nations, took place in Geneva. The second phase of the WSIS took place in 2005 in Tunis, Tunisia.

From this Summit came important conclusions that still shape the current understanding of the Information Society and Internet Governance, as well as what is known as *multistakeholderism*[8]. The WSIS resulted in two relevant multistakeholder events, which are held annually to discuss Internet Governance and Information Society issues: the Internet Governance Forum (IGF) and the WSIS Forum.

At this point, it should also be noted that in September 2021, UN Secretary-General António Guterres released his report Our Common Agenda, as part of the celebration of the 75th anniversary of the United Nations. The Common Agenda proposes a redefinition of the Organization's priorities and commitments, including the Global Digital Compact, which should outline "shared principles for an open, free and secure digital future for all". The security of cyberspace will therefore be a central theme of the Global Digital Compact.

The UN has therefore been dealing with cybersecurity since the early days of the Internet's popularization (1998 marks the beginning of such endeavour) and since then, the work, which began in the First Committee of the UN General Assembly, has been deepened and metastasized by countless UN bodies, agencies, committees, forums and working groups.

To such an extent that the process has become somewhat chaotic and difficult to follow, implying that only the richest nations (and even those with some difficulties) or the wealthiest technology companies have the resources to follow the cybersecurity debate at the UN in a comprehensively manner.

Even so, the UN is a global platform and is unique in the way it provides a forum for dialog between member states of all stripes. In a matter such as cybersecurity, the need for this global dialog seems all too evident, given the interdependence in cyberspace.

[7] More on "Internet for trust- towards Guidelines for Regulating Digital Plataforms" at https://www.unesco.org/en/internet-trust?hub=71542

[8] The concepts of Internet Governance and multistakeholderism are defined in the Tunis Agenda that emerged from the WSIS. Article 34 "A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet". Available at https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html .

It should be noted that the UN's activity in the field of cybersecurity has been restricted to the production of non-binding norms, which has its limitations, which will be discussed below.

Cybersecurity in the regional and national context

Having analyzed the global discussions taking place within the UN, it is now important to focus on the main developments in the organizations of which Portugal is a member.

In our analysis, priority is given to the EU, whose legislative output on cybersecurity has been pioneering and also quite prolific, such is the diversity of initiatives that contribute to strengthening security in the digital world. Other institutions analyzed, although in less detail, will be the Organization for Economic Cooperation and Development (OECD), the Council of Europe and the NATO Cooperative Cyber Defence Centre of Excellence and the Community of Portuguese Speaking Countries (CPLP).

Given its relevance, the paper addresses the state of the art in terms of cybersecurity regulation in Brazil and its organizational model. Finally, reference will be made to the organizational model in Portugal.

European Union

At this point it is important to note, first of all, that cybersecurity is not included among the Union's internal policies and actions, as listed in the Treaty on the Functioning of the European Union (TFEU)[9]. This means that all actions taken by the EU in this area had to be justified, in the first instance, in the light of competences already attributed to the Union[10]. In this case, in particular, the EU justifies its intervention with arguments fundamentally of an economic nature and of its competences, in particular within the framework of the construction of the internal market[11].

Among the recent EU initiatives to strengthen cybersecurity, the "EU Cybersecurity Strategy for the Digital Decade"[12] of December 2020 stands out, comprising three main vectors:

- "Resilience, technological sovereignty and leadership";
- "Building the operational capacity to prevent, deter and respond";
- "Promoting a global and open cyberspace".

It is also important to highlight Directive (EU) 2022/2555, of December 14, 2022, on measures to ensure a high common level of cybersecurity across the Union - the NIS2 Directive[13], which extends the scope of application of cybersecurity rules in order to "ensure comprehensive coverage of sectors and services of vital importance for key economic and social activities in the internal market".

In addition to this piece of legislation, it is important to point out other legislative initiatives in related but extremely important areas, such as: privacy, security and data governance; the resilience of critical

[9] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, available at https://eur-lex.europa.eu/legal-content/En/TXT/HTML/?uri=CELEX:12012E/TXT

[10] Odermatt, J. (2018). The European Union as a cybersecurity actor. In *Research Handbook on the EU's Common Foreign and Security Policy* (pp. 354-373). Edward Elgar Publishing.

[11] The legal basis for protecting the functioning of the internal market is found in various articles of the Treaty on the Functioning of the European Union, in particular Articles 4(2)(a), 26, 27, 114 and 115. The principle of the internal market is contained in the Treaty Establishing the European Economic Community, the Treaty of Rome, signed in 1957, and was intended to eliminate trade barriers between Member States with the aim of increasing economic prosperity and helping to bring people closer to the Union.

[12] "The EU's Cybersecurity Strategy for the Digital Decade" available at https://digital-strategy.ec.europa.eu/pt/node/435

[13] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive), available at https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022L2555&from=PT

entities; the electronic communications regulation; the digital services regulation (DSA - Digital Services Act and DMA - Digital Markets Act), and finally, artificial intelligence.

In our opinion, the EU's intervention in cybersecurity has come a long way and has been a pioneering effort to protect the interests of its member states, citizens and companies in the search for a safer digital environment, with the guiding principle being respect for fundamental values, respect for human rights, including those enshrined in the EU Charter of Fundamental Rights and Freedoms[14].

It is concluded, however, that the legislative tangle is complex and difficult to apply, and the relationship between the various pieces of legislation is not obvious. This could have unintended implications, including related to the competitiveness and innovation in Europe. However, it seems fair to say that the efforts made so far indicate a desire to make cyberspace a safer domain in which users' fundamental rights are guaranteed, which is a relevant and positive aspect.

NATO Cooperative Cyber Defence Centre of Excellence and the Tallinn Manual

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE[15]) was founded in 2008 on the initiative of Estonia, together with six other states (Germany, Italy, Latvia, Lithuania, Slovakia and Spain), with the aim of providing training and research in support of the North Atlantic Treaty Organization (NATO) mission. The Center has been developing the Tallinn Manual, which is an analysis of how international law applies to cyberspace.

Council of Europe and the Budapest Convention

The Budapest Convention, or Convention on Cybercrime[16] (hereinafter referred to as the Convention or Treaty), is an international treaty signed in 2001. The Convention was the first legal framework to institutionalize international cooperation in the fight against cybercrime and is still a reference today, being the most relevant agreement with regard to cybercrime. The Budapest Convention falls within the the scope of criminal prosecution that was mentioned before.

Organization for Economic Cooperation and Development

The Organization for Economic Cooperation and Development (OECD) is an international organization that promotes economic growth, trade and social welfare among its member countries.

In general terms, the OECD's work on digital security can be systematized into three vectors:

- A vector for producing recommendations / guidelines for strengthening digital security;
- A vector for producing a general policy framework;
- Finally, a training vector.

Cybersecurity in the CPLP and Brazil

The activities of the CPLP, especially within the framework of ARCTEL-CPLP, and Brazil, as a particularly important member state, are also relevant to the discussion of cybersecurity.

[14] Odermatt, J. (2018). The European Union as a cybersecurity actor. In *Research Handbook on the EU's Common Foreign and Security Policy* (pp. 354-373). Edward Elgar Publishing.
[15] CCDCOE History available at https://ccdcoe.org/about-us/
[16] The Budapest Convention was approved by Resolution of the Portuguese Parliament no. 88/2009, of 15/09 and ratified by Decree of the President of the Republic no. 91/2009, of 15/09 (available at https://rm.coe.int/16802fa428)

Cybersecurity in Portugal

It is important to bear in mind that the policies and legal framework in the field of cybersecurity are, to a large extent, a consequence of EU policy and law.

Cybersecurity in non-governmental forums

The level of threats in cyberspace is so significant that the process of creating a regulatory framework to facilitate the response to such threats is not limited to a governmental and multilateral organization such as the United Nations.

Other actors have sought to create discussion platforms for the development of norms that contribute to a more reliable and secure use of communication and information technologies.

Ruhl[17] identifies three other ways of creating norms for cyberspace, in addition to the multilateral way: the private way, the industry way and finally the multistakeholder way.

Ruhl defines each of these routes and identifies some of the processes that fall within them.

The private route, according to the author, involves experts of various backgrounds who may be associated with states or other actors which participate purely individually. The Global Commission on Internet Governance (also known as the Bildt Commission), the Global Commission on the Stability of Cyberspace or Carnegie's Cyber Policy Initiative are examples of this type of route.

The path promoted by industry includes processes such as the Digital Geneva Convention, led by Microsoft and the Tech Accord authored by 34 technology companies or the Charter of Trust by Siemens.

The multistakeholder route involves several players, such as governments, the private sector, academia and civil society. These players, working collaboratively and on an equal footing, can also initiate processes to create norms for cyberspace. Among the processes identified are the IGF, NETMundial[18] and Paris Call.

From this analysis, it is concluded the global panorama in which cybersecurity and the norms applicable to it are discussed is complex and labyrinthine. However, these characteristics coincide with the description of International Law itself brought to us by Maria Luísa Duarte. According to Maria Luísa Duarte International Law is based on a plurality of Sources with an uncertain relationship between them; by the dispersion between norms; and by the fragmentation of International Law in the form of different specific regimes.

In addition, the so-called soft law plays an important role in the way cybersecurity is regulated at both a global and regional level.

On the need for an international cybersecurity convention

Given this context, the question arises as to whether non-mandatory norms will be sufficient to strengthen security in cyberspace. Or differently stated: To what extent the adoption of a binding conventional instrument on a global scale would strengthen the security in cyberspace?

[17] Ruhl, C., Hollis, D., Hoffman, W., & Maurer, T. (2020). *Cyberspace and geopolitics: Assessing global cybersecurity norm processes at a crossroads*. Carnegie Endowment for International Peace.

[18] Ruhl places the Internet Governance Forum in the context of multistakeholder processes. In reality, it is a process in which various actors participate collaboratively

Statistical evidence (both in terms of the vulnerabilities identified and the economic impact) and paradigmatic examples demonstrate the limitations of the adequacy of current international law for cyberspace and highlight the shortcomings and even inconsistencies of the processes for creating non-binding rules.

The paper concludes that a global and binding legal framework for cyberspace would be necessary to strengthen cybersecurity in the field of state defense. It is argued that the ideal model for creating such a framework would be the negotiation of an International Convention for Cybersecurity, negotiated within the UN.

A binding, global legal framework of this nature could address some of the following issues:

- Defense of fundamental rights in cyberspace, such as the right to privacy, freedom of expression and information;
- Cooperation mechanisms;
- Guidance to states on the need to adopt national cybersecurity strategies;
- Importance of protecting critical infrastructures;
- Importance of capacity building;
- Conflict resolution mechanisms.

On the feasibility of an international cybersecurity convention

The second fundamental question to be answered is whether the creation of such a global and binding legal framework for cyberspace would be feasible at the present time.

To answer this question, a diagnosis is made comprising several dimensions:

- Geopolitical;
- Institutional, in which an assessment of multilateralism is presented, in particular the United Nations Organization;
- The future of cyberspace and competition for technological supremacy;
- And finally, the different understandings and ambiguities that the issue of cybersecurity raises.

In geopolitical terms, the world is facing an Era of instability, distrust, (in)security and self-centeredness. The paper calls it the Egopolar Era.

From an institutional point of view, which stems from geopolitics, we assess the state of multilateralism, in particular the United Nations Organization.

The UN is under fire given the constraints resulting from the Global Order described; from its dispersion in terms of the issues it deals with, under an institutional framework that is unsuited to reality; and from a problem of representativeness that results from the unequal involvement of some regions or groups of countries in the UN system.

With regard to the future of cyberspace and the competition for technological supremacy, there are substantially opposing visions of what cyberspace should be.

In essence, from a global point of view, there are two models of Internet Governance:

- A model based on the multistakeholder concept, in which Internet Governance is conducted by governments, the private sector, civil society, academia and other actors, on equal terms.
- A model of intergovernmental Internet Governance in which governments took control, to the detriment of other actors.

Although committed to the multistakeholder model, the EU has been on a pioneering path towards regulating cyberspace and its actors.

In addition to these different visions of cyberspace, there is an important dispute going on over the technological supremacy at a global level, with the US and China as the main players.

With regard to the differences that the issue of cybersecurity raises, there is a great deal of vagueness and ambiguity when it comes to the concept of cybersecurity. Little clarity about what this concept means and what threats it comprises is also problematic. On the other hand, there are still doubts as to how international law applies to cyberspace.

From the assessment of these dimensions, the conclusion we draw is that agreeing on a global and binding legal framework, in particular the drafting of an International Convention for cybersecurity, is not currently a feasible exercise.

A digital world without an international cybersecurity convention and conclusions

In the context of growing cyber threats and given the unfeasibility of an agreement for a global and binding legal framework, a set of recommendations is presented and reflections on some paths that can be taken and that can contribute to strengthening cybersecurity, particularly in the field of state defense.

Bearing in mind that one of the obstacles in reaching an understanding in the process of creating norms in the field of cybersecurity is related to the breadth and ambiguity of this concept, it is proposed that the issue is approached in a more granular way, seeking to clearly identify which layers of cyberspace are being dealt with, which areas of cybersecurity the negotiations fall within, and which concrete problems are intended to be solved.

In addition, there is a need to implement the existing non-binding norms that have emerged from the existing processes. The construction and constant updating of a comprehensive systemic vision, i.e. a mapping of all existing processes and the relationships between them, is also seen as valuable.

The text also addresses the role that the EU can play. The EU is seen as a leading actor in the construction of a regulatory framework for cybersecurity and cyberspace in general, and could play an even more influential role, in our opinion, if the model that has been built is inspiring for other regions.

For its part, the CPLP could be used as a successful (and perhaps less politicized) platform for sharing information, training and solutions to specific and specific problems in the field of cybersecurity, thus providing a practical example of cooperation between different continents and hemispheres, which is as rare as it is valuable today.

By taking on the role of honest broker and bridge-builder between divergent visions, Portugal can bring added value and strengthen its capacity to influence, even in an area as critical and complex as the subject of this dissertation.

Finally, and despite all the efforts that can be made in the near future, we cannot neglect the risk of having to deal with a cyberspace that tends to be more politically fragmented and far from the ideal of openness and unity that was once envisioned or dreamed of.

It is even considered that this scenario of political fragmentation of the Internet is increasingly plausible, and it is necessary to better understand and study the implications from a technical, economic, social and, above all, geopolitical point of view that such fragmentation may entail.