REDE
DE PESQUISA
EM GOVERNANÇA
DA INTERNET

Anais do Encontro Anual da Rede de Pesquisa em Governança da Internet

Maio de 2024

VII ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET - REDE 2024

FICHA TÉCNICA

ANAIS DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET-VOL. 7, ISSN 2675-1690

Editores

Diego Vicentin
Hemanuel Jhosé Alves Veras
Maria Vitoria Pereira de Jesus

Autores

Andressa de Bittencourt Siqueira
Ane Carine Meurer
Diná Santana Santos
Elen Nas
Elizabeth Machado Veloso
Henrique S. Xavier
Isabelle Brito Bezerra Mendes
Jeiel de Santana Barbosa
João Araújo Monteiro Neto
Josiane Ribeiro
Kauã Arruda Wioppiold
Lucas Zanotto
Luis Henrique de Menezes Acioly
Luísa Carli de Lacerda
Matheus Fernandes da Silva
Pedro Odebrecht Khauaja
Sérgio Braga
Tatiana Nascimento Heim
Yago Rabelo Daltiba

COMITÊ ORGANIZADOR

Núcleo de Coordenação da Rede de Pesquisa em Governança da Internet

Alexandre Arns Gonzales
Carolina Batista Israel
Diego Vicentin
Fernanda R. Rosa
Hemanuel Jhosé Alves Veras
Kimberly de Aguiar Anastácio
Maria Vitoria Pereira de Jesus
Nathan Paschoalini Ribeiro Batista
Rodolfo Avelino

Comitê Científico

Alexandre Arns Gonzales
Ana Paula Camelo
Carolina Batista Israel
Daniela Araújo
Diego Vicentin
Fernanda R. Rosa
Flávio Rech Wagner
Gills Vilar-Lopes
Jean Ferreira dos Santos
Leonardo Ribeiro da Cruz
Maria Mónica Arroyo
Martha Mourão Kanashiro
Rafael Evangelista
Raquel Gatto
Rodolfo Avelino
Sergio Marcos de Ávila Negri
Rodrigo Firmino

Moderadores

Daniela Araújo
Diego Vicentin
Hemanuel Jhosé Alves Veras
Laura Conde Tresca

Debatedores

Diná Santana Santos
Elen Nas
Elizabeth Machado Veloso
Henrique S. Xavier
Jeiel de Santana Barbosa
Josiane Ribeiro
Kauã Arruda Wioppiold
Lucas Zanotto
Luísa Carli de Lacerda
Matheus Fernandes da Silva
Pedro Odebrecht Khauaja
Sérgio Braga
Tatiana Nascimento Heim
Yago Rabelo Daltiba

O VII Encontro da Rede de Pesquisa em Governança da Internet e a publicação dos Anais resultantes deste encontro receberam apoio de: Comitê Gestor da Internet no Brasil - CGI.br, Internet Society - Capítulo Brasil e do Programa de Pós-graduação em Ciências Sociais da Universidade Estadual de Campinas (Unicamp), através de recursos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES)

Internet Society Capítulo Brasil

CAPES

cgi.br

NAVIGATING FRAGMENTATION: COHERENCE IN INTERNATIONAL CYBERSECURITY NORMS

Tatiana Nascimento Heim

SUMÁRIO

NAVIGATING FRAGMENTATION: COHERENCE IN INTERNATIONAL CYBERSECURITY NORMS

Tatiana Nascimento Heim[1]

RESUMO

A presente era enfrenta diversas ameaças à segurança, nomeadamente, ciber-ataques e violações da privacidade dos dados. Em resposta a esses desafios, a cibersegurança tornou-se fundamental na proteção de sociedades dependentes da internet. Além disso, a internet possui um caráter transnacional e as ameaças ao seu funcionamento não podem ser reguladas ou tratadas por países individualmente. A regulamentação internacional pode fornecer ferramentas para regular a cibersegurança. No entanto, existem pontos de vista contrastantes sobre o funcionamento da internet e as instituições possuem interesses distintos dentro do ciberespaço, que gera uma fragmentação de instrumentos internacionais. Dessa forma, utilizando uma abordagem exploratória-descritiva, este estudo examina a coerência entre instrumentos internacionais que abordam a construção de capacidade, o fortalecimento da confiança e a cultura de cibersegurança. Isso, porque as instituições internacionais entendem que esses três aspectos são pilares fundamentais para um ciberespaço resiliente e seguro. O estudo concentra-se em instrumentos de instituições internacionais selecionadas. A análise verifica uma coerência geral, especialmente em iniciativas de construção de capacidade e cultura de cibersegurança. No entanto, surgem conflitos quando se trata das interações entre Estados, em relação à aplicação das normas. Portanto, para assegurar uma maior coerência, as instituições internacionais devem priorizar medidas preventivas, que considerem os diferentes entendimentos sobre cibersegurança.

PALAVRAS-CHAVE

Cibersegurança; Fragmentação; Coerência; Normas Internacionais

ABSTRACT

The present era faces diverse security threats, notably, cyber-attacks and breaches of data privacy. In response to these challenges, cybersecurity has become fundamental in safeguarding internet-dependent societies. Furthermore, the internet has a transnational character, and threats to its functioning cannot be regulated or addressed

[1] Doutora (PHD) pela Universidade de Twente, na Holanda. Vínculo institucional atual: Pontifícia Universidade Católica do Paraná. E-mail: tatiana.heim@gmail.com

by individual countries. International regulation can provide tools to regulate cybersecurity. However, there are contrasting viewpoints on how the internet operates and institutions have distinct interests within cyberspace, leading to a fragmentation of international instruments. Thus, employing an exploratory-descriptive approach, this study examines the coherence among international norms addressing capacity-building, confidence-building, and cybersecurity culture. This is because international institutions understand that these three aspects are fundamental pillars for a resilient and secure cyberspace. The study focuses on norms from selected international institutions. The analysis reveals a general coherence, especially in capacity-building and cybersecurity culture initiatives. However, conflicts arise when it comes to interactions between states, regarding the application of these norms. Therefore, to ensure greater coherence, international institutions should prioritize preventive measures that take into account the different understandings of cybersecurity.

KEYWORDS
Cybersecurity; Fragmentation; Coherence; International Norms

INTRODUCTION

The present era is characterized by an increasing diversity of security threats (PERNICE, 2017). Many states and individuals face cyber-attacks, breaches of data privacy, and other cyber threats. In response to these challenges, cybersecurity has emerged as a crucial defence mechanism in a society that is heavily reliant on the internet for everyday activities (TABANSKY, 2015). The internet is transnational in character and threats to its functioning cannot be regulated or dealt with by single states. Moreover, it is further complicated by the intricate governance and regulatory processes operating within a multi-level framework (global, EU and national). This framework involves diverse actors across different levels, each bearing responsibility for numerous interconnected rules, standards, and principles.

International law – and in a broader sense international regulation – can provide tools for answering questions related to opportunities to regulate the international cyber field, because cyber norms have become the main regulatory vehicle for stability and safety in cyberspace (FINNENMORE, 2016). However, there are contrasting viewpoints regarding the operation of the internet and institutions that possess distinct interests within cyberspace. This results in a patchwork of different norms (softer and harder legal rules) which is disorganised and fragmented (TROPINA, 2015). Despite this complexity, cyber norms have emerged as the primary regulatory mechanism for ensuring stability and safety in cyberspace (FINNEMORE, 2016). The current regulatory landscape reveals that cybersecurity norms are formulated by a variety of actors, including

international organizations like the United Nations, through the Group of Experts process (HENRIKSEN, 2019), as well as private entities, such as Microsoft (HUREL, 2018).

In other words, the international norms are fragmented, because of to the proliferation of international rules and instruments and the multiplication of international institutions, from formal international organisations to more informal standard-setting bodies (PROST *et al*. 2006; KOSKENNIEMI, 2014; HAFNER, 2003; PAUWELYN, 2003). Even though fragmentation is not bad *per se*, it may create conflicts between different instruments that can lead to disharmonised case-law, forum-shopping and or even loss of legal certainty. Furthermore, the lack of a clear understanding of the content of the instruments relating to cybersecurity creates regulatory uncertainty which delays the development of effective regulatory solutions.

In this fragmented and disorganized context, this study aims to analyze if there is coherence among the international norms that address capacity-building, confidence-building, and cybersecurity culture. This topic was chosen, because international institutions place significant emphasis on fostering capacity-building, confidence-building and cultivating a cybersecurity culture as the fundamental pillars of a resilient and secure cyberspace. The article is divided into three sections. The first part of this paper will present the methodology. The second part of this paper will analyze the cyber instruments selected. Finally, the last section will present the conclusions of the article.

METHODOLOGY

Using an exploratory-descriptive approach, this study concentrates on norms from international institutions. The exploratory research aims to generate generalizations about the group, process, activity, or situation under study, when little scientific knowledge exists (STEBBINS, 2001). The descriptive methodology attempts to describe the world in a scientific manner that goes beyond listing attributes, but also assigns facts into classes and categories (TOSHKOV, 2016). International institutions are defined as relatively stable sets of related norms and rules that pertain to the international system, its actors (including states and non-state entities), and their activities (DUFFIELD, 2007).

The selection of data started by first selecting the institutions and second, the cybersecurity instruments. The study selected institutions cited in academic publications, conducting a literature review using Google Scholar on June 22, 2020, with the

keywords, in the title, internet AND “global governance”, global cybersecurity, internet AND “international organizations, cybersecurity AND “global governance”, cybersecurity AND international organizations resulted in 369 unique articles initially retrieved. Out of the 369 articles initially retrieved, 111 were found in the search results, but were not accessible (only citations were available). Additionally, 197 articles were not relevant to the research as they did not mention any organization related to cybersecurity governance within the text. Resulted in 61 academic papers that were utilized in the selection of international institutions.

The next step involved scouring the 61 documents to identify the institutions mentioned in the articles. All organizations referenced in the analysis were included, resulting in the selection of 38 international institutions. Once the institutions were identified, the subsequent step involved locating cyber instruments on their websites. Specifically, cyber instruments available in English, in force or undergoing the process of entering into force, the preferred formats were .pdf, .doc, or .docx.

To streamline the search process, the study leveraged the search limitations available on some organization websites. Typically, these limitations encompass two categories: constraints based on the type of document and restrictions related to research topics. In total, the research uncovered 5969 documents. Institutions that presented at least one document meeting the specified criteria were included in the analysis. The final stage involves the selection of cybersecurity norms. To accomplish this, we follow a three-step process. Firstly, we determine whether the primary focus is on cybersecurity or cyber threats. Secondly, we locate documents produced by the organization. And thirdly, we identify elements within these documents that indicative of cyber norms.

The term norms encompass both binding and non-binding, legislative and non-legislative measures. This distinction, in international law, is traditionally framed as a distinction between hard and soft law. The term 'hard law' denotes a hard obligation and/or a hard enforcement. For example, in situations where rules are submitted to judicial control (TERPAN, 2015). In this category of law there is an obligation and rights of involved parties (TRACHTMAN, 2004) and a violation could trigger a legal consequence (PRONTO, 2015). Soft enforcement could be compliance without direct coercion (TERPAN, 2015) or an expectation that it will be respected (GRUCHALLA, 1984). Regarding the soft obligations, we focus on soft law that has an international nature, originates from international institutions (THURER, 2000) or agreements between

state representatives (GRUCHALLA, 1984). Regarding the content, soft law should be relatively formal, has an institutional character (ABBOTT, 2012) and resembles a legal instrument. Therefore, the format of the document is important and the words are typically similar to those found in hard law (TERPAN, 2015). In other words, we used the term 'instrument' to a written formal or legal document (THE LAW DICTIONARY, 2022). The term 'Norms' are more specific and form the building blocks of legal instruments. They aim to guide or influence the behaviour of states, institutions and private actors. The table 1 show the result of the selection:

Table 1: Instruments selected

Institution	Instruments selected
African Union	African Union Convention On Cyber Security and Personal Data Protection
ITU	ITU Resolution 50 (2012)
ITU	ITU Resolution 50 (2016)
ITU	ITU Resolution 130 (2018)
ITU	ITU Resolution 130 (2014)
ITU	ITU Resolution nº 174 (2014)
ITU	ITU Resolution nº 181
United Nations	UNGA Resolution nº 54/49
United Nations	UNGA Resolution nº 55/28
United Nations	UNGA Resolution nº 56/19
United Nations	UNGA Resolution nº 56/121
United Nations	UNGA Resolution nº 57/53
United Nations	UNGA Resolution nº 57/239
United Nations	UNGA Resolution nº 58/32
United Nations	UNGA Resolution nº 58/199
United Nations	UNGA Resolution nº 59/61
United Nations	UNGA Resolution nº 60/45
United Nations	UNGA Resolution nº 61/54
United Nations	UNGA Resolution nº 62/17
United Nations	UNGA Resolution nº 63/37
United Nations	UNGA Resolution nº 64/211
United Nations	UNGA Resolution nº 64/25
United Nations	UNGA Resolution nº 65/41
United Nations	UNGA Resolution nº 66/24
United Nations	UNGA Resolution nº 67/27
United Nations	UNGA Resolution nº 68/243
United Nations	UNGA Resolution nº 69/28
United Nations	UNGA Resolution nº 70/237
United Nations	UNGA Resolution nº 71/28

United Nations	UNGA Resolution nº 73/27
United Nations	UNGA Resolution nº 73/266
United Nations	UNGA Resolution nº 74/28
United Nations	UNGA Resolution nº 65/41
Organisation for Economic Co-operation and Development (OECD)	Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document.
Shanghai Cooperation Organization (SCO)	Agreement on Cooperation in Ensuring International Information Security
European Union	EU Directive 2016/1148
European Union	Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 2013
Tech Accord	Tech Accord
Organization for Security and Co-operation in Europe (OSCE)	OSCE Decision 1106
Organization for Security and Co-operation in Europe (OSCE)	OSCE Decision 1202
European Union	EU Directive on Security of Network and Information Systems
Organization for American States	OAS Declaration Strengthening Cyber-Security in the Americas

Source: own elaboration

The next section of the study will use these instruments as the foundation for the analysis and present the findings from the examination of the selected cybersecurity instruments.

COHERENCE IN FRAGMENTATED LANDSCAPE

The analysis reveals both fragmentation and coherence among the selected cybersecurity governance instruments. As outlined in the introduction, this research is premised on the assumption of a fragmentation of actors and norms within the cybersecurity governance domain. However, we do not frame this fragmentation as inherently positive or negative, but rather as the consequence of the expansion of multiple normative communities (BERMAN, 2007) or semi-autonomous spheres of normative control (FALK, 2001).

In this context, we anticipate encountering differences and conflicts between the instruments, as we recognize the singularities of national legal frameworks and do not subscribe to the notion of universal values (LEGRAND, 2021). Coherence is generally understood in a broader sense, requiring that the norms ‘make sense’ in conjunction (BAXTER, 1980; BELLIDO, 2004; DEL TORTO HUERTA, 2006). Coherence demon-

strates the quality of the process and involves several factors (GEBHARD, 2017). Furthermore, it is a matter of degree and refers to positive connections (WESSEL, 2000) or mutual reinforcement (GOMAR, 2014). It would be erroneous to comprehend coherence solely in terms of 'unity' and 'consensus', as it is a value that necessitates different variables to be achieved over time (D'ASPREMONT, 2012), such as consistency, comprehensiveness and completeness (BERTEA, 2005).

At the national level, a coherence of norms must obey the hierarchy of legal instruments (for example *lex specialis derogat lex generalis*) (KOSKENNIEMI, 2014). However, at the international level, in the context of global governance of cybersecurity, where there are soft, rather than hard laws, the traditional legal ways of solving conflicts of norms and achieving coherence are difficult to apply. International scholars have developed criteria for coherence between legal norms. For example, according to McCormick norms are coherent when they share common values and principles. The author emphasises that the objectives of the norms should be formulated in clear terms and harmonised, the strategies and mechanism should be attuned to the objectives and the outcome should correspond with intentions and objectives (MACCORMICK, 1984). The interpreter of the norms has an important role to achieve a coherent set of norms and must try and apply alternatives of interpretation to prevent a normative collision (AMARAL, 2009). Moreover, from a public policy perspective, the policy output should be in line with the policy processes that are the institutional arrangements, policies objectives and the behavioural changes (GOMAR, 2014). In this study, coherence is understood as a situation in which all the components fit together (BERTEA, 2005), in the sense that the instruments and organisations are linked together in a systematic manner. In that sense, even if there is normative inconsistency, there can be coherence in a set of norms.

In the case of the selected cyber instruments, there is fragmentation arising from the existence of various institutions at different levels, sometimes with conflicting interests, which establish different instruments to achieve the common goal of cybersecurity. Notably, there is also coherence, because the selected cyber instruments complement and reinforce each other, as they share the overarching objective of enhancing capacity-building, confidence-building, and cybersecurity culture. It is important to note that the selected instruments do not provide specific details on how these measures should be implemented, as their primary aim is to create awareness and provide a sense of

direction, rather than establishing strict rights and obligations. Additionally, these instruments target a diverse audience with varying levels of technological development.

The next section will present the main results found in three aspects that frequently appear in the cybersecurity instruments: Capacity-building, confidence-building and cybersecurity culture.

CAPACITY- BUILDING

The first capacity analysed in the instruments is called capacity-building and is more closely related to the idea of sharing knowledge and skills. This objective of improving capacity for cybersecurity is found in various instruments. The idea of promoting capacity is similar among the instruments. Nonetheless, a possible criticism is the vagueness and ambiguity within these instruments can lead to a semblance of coherence.

The literature describes cybersecurity capacity-building as efforts to provide support and assistance that empower individuals, communities and governments to mitigate the risks associated with accessing and using information and communication technologies (HOMBURGER, 2019). Collett offers a comparable definition, characterizing capacity-building as a form of international cooperation that arose in the mid-2000s to share the knowledge and skills necessary for safeguarding the digital realm (COLLETT, 2021).

The analysis will begin by examining the Cybersecurity Tech Accord. The Cybersecurity Tech Accord, a private sector initiative, so far, the Cybersecurity Tech Accord is supported by more than 100 companies, including Dell and Cisco, advocates for promoting capacity-building measures among tech companies (CYBERSECURITY TECH ACCORD, 2018). However, the principles of the accord are brief and vague, leaving room for different interpretations. In addition, the lack of a clear governance mechanism and the voluntary nature of the norm can generate a selective implementation of the principles. This allows tech companies to establish norms in a semi-regulated environment, enabling them to be perceived as change-makers without genuine commitment (GORWA, 2018). On the other hand, despite the vague principles, the accord provides specific guidance for other organizations, such as the OECD's work on Digital Security (CYBERSECURITY TECH ACCORD COMMENTS, 2018)

In addition, since 2007, big tech companies, such as Microsoft, consolidate themselves as political international players with a quasi-diplomatic (HUREL, 2018).

One of the goals of the instruments established is the division of responsibility of cyber-attacks with the public sector. Even though it is possible to question if these divisions are responsible for securing their system to the point it is profitable (CARR, 2016; BURES, 2017). Tech companies are important actors for intensity initiatives to improve self-protection and development of products that use data within the concept of privacy by design (PERNICE, 2017).

International organizations have also been actively involved in the establishment of cyber norms that focus on capacity-building efforts. The European Union, a supranational organization, has played a significant role in the development of various cyber instruments. For instance, the General Data Protection Regulation (GDPR) is widely regarded as a global data regulation framework (KOMAITIS; SHERMAN, 2021) and the EU's cyber diplomacy toolbox, among other initiatives, has introduced the first cyber sanctions against perpetrators of cyberattacks (EUROPEAN UNION, 2023).

Regarding capacity-building, the European Union defines it as a relevant form to respond, effectively, to the challenges of security of networks and information (EUROPEAN UNION, 2016). In addition, capacity-building is also a fundamental pillar within the EU's international cyber policy. This viewpoint is further reinforced by the "Cybersecurity Strategy of the European Union," which underscores the significance of capacity-building initiatives in aiding third countries. The recommended actions to improve national and regional capacity-building are related to the prevention, deterrence and response to cyberthreats. The instrument recommends, among other things, the coordination of CERTs, the development of cybersecurity certification and investment in a specialised workforce (EUROPEAN UNION, 2013).

It can be argued that enhancing capacity within the European Union is considered a crucial step towards improving European Union digital sovereignty. By developing and strengthening its internal capabilities, the EU aims to address concerns related to the socio-economic influence of non-EU companies within the Union, thereby fostering greater control and independence over its digital landscape (KOMAITIS; SHERMAN, 2021). This objective is further supported by Europe's focus on strengthening European tech companies and enforcing national regulations (CHEN, 2022). Carver (2023) explains that, since 2020, there has been a shift from emphasizing 'cyber' capacity building to 'digital' capacity building, indicating a repackaging of capacity-building goals within the framework of European digital sovereignty.

CONFIDENCE-BUILDING

Another common element across the various instruments adopted by different institutions is the need to promote confidence-building measures (CBMs). Confidence-building measures can be characterized as components of international policy that work to diminish threats, improve trust and make relationships between states more predictable (BASELEY-WALKER, 2011). The term confidence-building has a great importance at the international level, because it is the basis for enhancing cooperation and coordination between different international actors. Without a minimum level of trust between the stakeholders in an interdependent system, it would not be possible to fight cyberthreats. It comes as no surprise that the greater divergences originate from the development of confidence-building measures.

The main institutions which have established international instruments about confidence-building measures are the United Nations Group of Governmental Experts (UN GGE). The United Nations Group of Governmental Experts (GGE) was established by Resolution A/RES/58/32 of the United Nations with the objective of promoting responsible State behavior in cyberspace (UNITED NATIONS, 2022). The GGE operates on an annual basis and its membership is determined based on a fair geographic distribution, ensuring diverse representation. GGE was established in 2004, constituted of 15 members, which include persons with different backgrounds, such as diplomatic, academic and cybersecurity (UNGA, 2010). In 2019, the number of participants increased to 25 members of the United Nations that were selected, considering equitable geographic distribution (UNGA, 2018). Decision-making within the group is achieved through consensus (UNGA, 2016).

The UN GGE was able to produce different recommendations to further improve confidence-building, such as establishing points of contact, consultative mechanisms, cooperation between incident response teams and information exchange, among others. However, these recommendations did not provide detailed guidance on how states should implement the proposed confidence-building measures (HITCHENS, 2019).

The development of confidence-building instruments continued through the subsequent third and fourth rounds of the UN GGE, which concluded that international law, including the United Nations Charter, applies to cyberspace. Additionally, the UN GGE determined that principles of state sovereignty and relevant international norms and principles apply to state behavior in the cyber domain (UNGA, 2013). However, the

success of the UN GGE in advancing confidence-building measures came to an end with the failure of the 2016-2017 GGE process, which was unable to reach consensus on the application of specific areas of international law, such as the law of armed conflict, self-defense and countermeasures, to state conduct in cyberspace (UNGA, 2013).

Divergences between Western and Non-Western countries in their perceptions of cyber threats, particularly regarding the application of international law in cyberspace are expected to persist. Non-Western countries like those in the Shanghai Cooperation Organisation view harmful information as a cyber threat due to concerns about regime stability and sovereign control (LEWIS, 2011). This clashes with Western principles of free speech and democracy (CLAESSEN, 2020). These differences can strain geopolitical relations and hinder cooperation (MEYER, 2020). Bridging these gaps and promoting dialogue is important for developing shared norms in cyberspace.

Another organisation that is responsible for creating confidence-building measures is the Organisation for Security and Co-operation in Europe (OSCE). The organisation aims to build trust between Euro-Atlantic and Eurasian countries in three main dimensions: Military matters, economic and environmental issues and Human Rights and fundamental freedoms. The OSCE has 57 member states, comprising countries from the Euro- Atlantic and Eurasian regions (OSCE, 2022). According to Hichens (2019), fifty-two of the fifty-seven OSCE member states have implemented at least one confidence-building measure at a national level. The success in implementation can be explained by the focus of the organisation on practical measure and the private sector and non-governmental organisations working together (HITCHENS, 2019)

At last, the Paris Call for Trust and Security in Cyberspace, launched by French President Emmanuel Macron, represents a multistakeholder initiative that aims to enhance trust, security and stability within the cyber domain. This endeavor involves the participation of diverse entities, including national governments, companies and civil society organizations. The instrument encourages various stakeholders to combat cyber threats and protect critical infrastructure and citizens. The instrument is based on nine principles to secure cyberspace and enhance cooperation between public and private actors (PARIS CALL, 2018). In the year 2020, the Paris Call initiative established six working groups tasked with driving the implementation of the instrument's guiding principles (PARIS CALL, 2018). While the specifics of the online consultative processes undertaken by these groups remain opaque, the Kaspery website does provide access

to the questions posed and responses generated through these collaborative efforts (KAPERSKY, 2020).

Notwithstanding these implementation measures, the Paris Call continues to grapple with challenges in achieving truly global reach and participation. The African and Asian regions remain underrepresented and several key nation-states, including the United States, India, China, and the Russian Federation, have yet to become signatories to the initiative. Scholars, such as Amazouz, have posited that the limited engagement from African countries may be attributable to the absence of a robust cybersecurity culture and awareness among both end-users and policymakers within these contexts (AMAZOUZ, 2019). An additional factor contributing to this gap in participation may be the Paris Call's alignment with the Budapest Convention on Cybercrime, which has engendered resistance from certain stakeholders (LÉTÉ, 2021).

Consequently, sustained efforts are required to promote the participation of a more diverse array of countries and institutions in the Paris Call. Expanding the breadth of engagement and buy-in from various stakeholders holds the potential to enhance the effectiveness of the cyber norms and principles espoused by the initiative, thereby strengthening global cybersecurity resilience.

CYBERSECURITY CULTURE

Another aspect that emerges in cyber policy instruments is the integration of capacity-building measures with confidence-building efforts - the creation of a culture of cybersecurity. The African Union Convention on Cybersecurity defines cybersecurity culture as a new mindset and behavior when utilizing information systems. It emphasizes the need for different stakeholders, such as governments, enterprises and civil society, to develop a culture of cybersecurity. This can be accomplished through the establishment and implementation of cybersecurity plans, fostering cybersecurity culture in enterprises, involving civil society and creating national sensitization programs for various user groups (AFRICAN UNION, 2014).

The United Nations General Assembly's Second Committee has established two key instruments aimed at cultivating a global culture of cybersecurity that holistically integrates political and economic considerations. The Resolution A/RES/57/239 created the foundational document "Creation of a Global Culture of Cybersecurity", which delineates nine mutually reinforcing elements as the basis for this culture: Awareness,

Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment (UNGA, 2003). Building upon this initial resolution, Resolution A/RES/64/211 further expanded the scope to explicitly include the protection of critical infrastructure (UNGA, 2010).

At the regional level, the Organisation of American States (OAS) was the first multilateral body to adopt a comprehensive Cyber Security strategy in 2004, titled “The Comprehensive Inter-American Cyber Security Strategy”. This instrument aims to assist member states in cultivating a culture of cybersecurity through the development of preventive measures to anticipate, address and respond to cyber threats; the criminalization of attacks; the protection of critical infrastructure and; the security of networked systems. To achieve these objectives, the strategy emphasizes the importance of all participants being cognizant of their respective roles and responsibilities (OAS, 2004).

Additional measures promoted by the OAS strategy include supporting users and operators in securing their computers and networks, as well as responding to and recovering from incidents. Furthermore, the strategy underscores the need to foster partnerships with the goal of enhancing education and awareness. Finally, the instrument encourages member states to adopt technical standards, best practices and legislative frameworks addressing cybercrime (OAS, 2004).

CONCLUSION

The identified international instruments show a convergence on the importance of capacity-building, confidence-building and cybersecurity culture to enhance global cybersecurity measures. While a clear and universally accepted definition of these terms remains elusive, there is a broad consensus on their fundamental role in strengthening international cybersecurity cooperation. These umbrella concepts are used by various international institutions as platforms to promote enhanced cooperation in cyberspace. However, the implementation of these norms faces challenges, as some organizations have limited global reach. Additionally, the proliferation of different cyber norms established by various entities underscores the importance of the issue, but also raises concerns about potential conflicts and inconsistencies.

When the focus shifts to state-to-state interactions, conflicts surrounding the application of cyber norms become more evident. A key distinction lies in the emphasis on confidence-building measures regarding the application of international law in cy-

berspace, which arises from mistrust among nations and concerns about the potential misuse of cyberspace for unilateral military actions. This suggests that the broader and less well-defined an instrument is, the more controversy it tends to generate. As confidence-building instruments become more specific, issues and disagreements are more likely to arise.

Consequently, conflicts between legal norms are expected to persist, highlighting the need to prioritize preventive measures in areas where greater convergence can be achieved. This divergence could also encourage like-minded states to come together, while providing an opportunity for international actors to better understand different geopolitical interests and potentially find common ground. Overall, the analysis of international instruments reveals both progress and challenges in the global effort to enhance cybersecurity. Continued dialogue, transparency and a focus on areas of consensus will be crucial in addressing the complex and evolving landscape of cyber norms and regulations.

REFERENCES

ABBOTT, Kenneth W.; MARCHANT, Gary E.; CORLEY, Elizabeth A. Soft Law Oversight Mechanisms for Nanotechnology. **Jurimetrics Journal**, v. 52, p. 279–312, 2012.

AMARAL JÚNIOR, Alberto do. El" diálogo" de las fuentes: fragmentación y coherencia en el derecho internacional contemporáneo. **Academia: revista sobre enseñanza del derecho de Buenos Aires, v.** 7, n. 13, p. 71-102, 2009.

BERTEA, Stefano. Looking for coherence within the European community. **European Law Journal**, v. 11, n. 2, p. 154-172, 2005.

CARVER, Julia. More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. **Journal of European Public Policy**, p. 1-37, 2023.

CARR, Madeline M.; ERSKINE, Toni. Beyond "quasi-norms": The challenges and potential of engaging with norms in cyberspace. **NATO Cooperative Cyber Defence Centre of Excellence**, 2016, p. 87-109.

CHEN, Xuechen.; YANG, Yifan. Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance. **The International Spectator**, 2022, p. 1-18.

CLAESSEN, Eva. Reshaping the internet–the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU. **Journal of Cyber Policy**, v. 5, p. 140-157, 2020.

COLLETT, Robert. Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. **Journal of Cyber Policy**, v. 1, n. 1, p. 1-20, 2021.

D'ASPREMONT, Jean. The systemic integration of international law by domestic courts: domestic judges as architects of the consistency of the international legal order. **The Practice of International and National Courts and the (De-) Fragmentation of International Law***,* 2012.

DUFFIELD, John. What Are International Institutions?. **International Studies Review**, p. 1-22, 2007.

EUROPEAN UNION. EU imposes first ever cyber sanctions to protect itself from cyber--attacks. **European Union External Action**. Disponível em: https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en . Acesso: 22 maio 2023.

EUROPEAN UNION. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Disponível em: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. Acesso: 22 maio 2023.

FINNEMORE, Martha; HOLLIS, Duncan B. Constructing norms for global cybersecurity. **American Journal of International Law**. v. 110, n. 3, p. 425-479, 2016.

GENERAL ASSEMBLY OF THE UNITED NATIONS (UNGA). Report nº 65/201 of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2010.

GENERAL ASSEMBLY OF THE UNITED NATIONS (UNGA). Report A/68/98, Report of the Group of Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, 24 June 2013. Disponível em: https://www.un.org/ga/search/viewm_doc.asp?symbol=A/68/98. Acesso: 22 maio 2023.

GENERAL ASSEMBLY OF THE UNITED NATIONS (UNGA). Resolution 57/239 - Creation of a global culture of cybersecurity, 31 January 2003.

GENERAL ASSEMBLY OF THE UNITED NATIONS (UNGA). Resolution 73/27 of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2018.

GENERAL ASSEMBLY OF THE UNITED NATIONS (UNGA).Resolutions 64/211 - Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 17 March 2010.

GEBHARD, Carmen. The problem of coherence in the EU's international relations. **International relations and the European Union**, p. 123-142, 2017.

GOMAR, Jose. Octavio. V.; STRINGER, Lindsay. C., & PAAVOLA, Jouni. Regime complexes and national policy coherence: Experiences in the biodiversity cluster. **Global Governance**, v. 20, n.1, p. 119-145, 2014. Disponível em: https://brill.com/view/journals/gg/20/1/article-p119_8.xml. Acesso: 22 maio 2023.

GORWA, Robert; PEEZ, Anton. Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, **Policy Advocacy, and Microsoft's Cybersecurity Tech Accord**, 2018.

GRUCHALLA-WESIERSKI, Tadenz. A Framework for Understanding Soft Law. **McGill Law Journal**, 30, 37, 1984.

HAFNER, Gerhard. Pros and cons ensuing from fragmentation of international law. **Mich. J. Int'l L**. v. 25, p. 849, 2003

HENRIKSEN, Anders. The end of the road for the UN GGE process: The future regulation of cyberspace. **Journal of Cybersecurity**. v. 5, n. 1, 2019.

HOMBURGER, Zine. The necessity and pitfall of cybersecurity capacity building for norm development in cyberspace. **Global Society**, v. 33, n. 2, p. 224-242, 2019.

HUREL, Louise Marie; LOBATO, Luisa Cruz. Unpacking cyber norms: private companies as norm entrepreneurs. **Journal of Cyber Policy**. v. 3, n. 1, p. 61-76, 2018.

KAPERSKY. Working together to ensure trust in and the security of cyberspace: our contribution to the Paris Call consultation. Disponível em: https://www.kaspersky.com/about/policy-blog/supporting-paris-call. Acesso: 16 de February de 2020.

KOMAITIS, Konstantinos; SHERMAN, Justin. US and EU tech strategy aren't as aligned as you think. **Brookings Tech Stream**. v. 11, 2021.

KOSKENNIEMI, Matti. Fragmentation of international law: difficulties arising from the diversification and expansion of international law: report of the study group of the International Law Commission. **Erik Castrén Institute of International Law and Human Rights**, 2014.

LEGRAND, Pierre. The Guile and the Guise: Apropos of Comparative Law as We Know It. **Asian Journal of Comparative Law,** v. 16, n.1, p. 155-181, 2021.

LÉTÉ, Bruno. The Paris Call and Activating Global Cyber Norms. **German Marshall Fund of the United States**, 2021. Disponível em: https://www.jstor.org/stable/10ceee-4d-15c4-3423-8cf9-7974a5b348dd. Acesso em: 22 de maio 2023.

LEWIS, James. Confidence-building and international agreement in cybersecurity. **Disarmament Forum**. Vol. 4, 2011

MACCORMICK, Neil. Coherence in legal justification. **Theory of Legal Science**. Dordrecht: Springer, 1984.

MEYER, Paul. Confidence-building measures in cyberspace: New applications for an old concept. Routledge Handbook of International Cybersecurity. **Routledge**, p. 286-296, 2020.

ORGANISATION FOR SECURITY AND CO-OPERATION IN EUROPE. **What is the OSCE?** Disponível em: https://www.osce.org/whatistheosce/factsheet. Acesso: 22 maio 2023.

ORGANIZATION OF AMERICAN STATES (OAS). AG/RES. 2004 (XXXIV-O/04) - A Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating A Culture Of Cybersecurity, 2004.

PARIS CALL. Paris Call: For trust and security in cyberspace. 12 de November de 2018.Disponível em: <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital--diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november--2018-for-trust-and-security-in>. Acesso em: 2022 de April de 2022.

PAUWELYN, Joost. Bridging fragmentation and unity: International law as a universe of inter-connected islands. **Mich. J. Int'l L**. v. 25, p. 903, 2003,.

PERNICE, Ingolf. Cybersecurity Governance: Making Cyberspace a Safer Place. **HIIG Discussion Paper Series**. n. 2017-05, 20 Jul. 2017. Disponível em: https://ssrn.com/abstract=3012136 Acesso: 22 maio 2023.

PRONTO, Arnold. N. Understanding the hard/soft distinction in international law. **Vanderbilt Journal of Transnational Law**, v. 48, p. 941, 2015.

PROST, Mario; CLARK, Paul Kingsley. Unity, diversity and the fragmentation of international law: how much does the multiplication of international organizations really matter? **Chinese Journal of International Law**. v. 5, n. 2, p. 341-370, 2006. Disponível em: https://academic.oup.com/chinesejil/article-abstract/5/2/341/295618?login=false. Acesso: 22 maio 2023.

SCHERMERS, Henry G.; BLOKKER, Niels M. **International Institutional Law: Unity within Diversity**. Brill, 2018.

STEBBINS, Robert A. **Exploratory research in the social sciences**. Sage, 2001.

TABANSKY, Lior. **Cybersecurity in Israel**. Nova Iorque: Springer, 2015.

TERPAN, Fabien. Soft Law in the European Union—The Changing Nature of EU Law. **European Law Journal**, v. 21, n.1, p. 68-96, 2015.

THE LAW DICTIONARY. Disponível em: https://thelawdictionary.org/instrument/. Acesso: 20 janeiro de 2022.

THURER, Daniel. Soft law. In: Encyclopedia of Public International Law. vol. 4, p. 452-460, 2000.

TOSHKOV, Dimiter. **Research design in political science**. Bloomsbury Publishing, 2016.

TRACHTMAN, Joel P. Conflict of Norms in Public International Law: How WTO Law Relates to Other Rules of International Law. **American Journal of International Law,** 2004, p.855-861.

TROPINA, Tatiana; CALLANAN, Cormac. **Self-and co-regulation in cybercrime, cybersecurity and national security**. Heidelberg: Springer, 2015.

WESSEL, Ramses A. The inside looking out: consistency and delimitation in EU external relations. **Common Market Law Review.** v. 37, n. 5, 2000. Disponível em:https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/37.5/276760. Acesso: 22 maio 2023.