Cyber Diplomacy and National Sovereignty in AUKUS Alliance: Balancing Regional Strategic Interests with Collective Cyber Security Goals

Kezzoute Mhammed*

Founder and director of the Moroccan Center for Cyber Studies and Technology Security and part-time professor at Mohammed First University, Oujda, Morocco.

Abstract: We must closely study the balance of interests within the AUKUS alliance, and the role of cyber diplomacy in this game of interests and power. Knowing that the alliance is constrained to address the challenges and issues of global instability, it primarily aims to strengthen the members' capabilities in cybersecurity and cyber defense. At this point, the desired balance among the members raises several questions and concerns. Regulatory frameworks, national interests, geopolitical and strategic issues, hegemony, and U.S. dominance all seem to be obstacles to the harmony and coherence of the alliance in achieving its objectives. In our study, we examine how the members manage these difficulties to eliminate obstacles to decision-making and deep cooperation. We also hope to understand how these states manage to maintain their sovereignties while contributing coherently and effectively to the alliance's collective cybersecurity strategy. Respect for national interests and the avoidance of establishing a hegemonic paradigm, etc., will be the main questions to examine in this work with a view to serving as a model for strengthening global cybersecurity and cyber governance.

Keywords: Aukus alliance, Cyberdiplomacy, Cybersovereignty, Cyberspace, Geopolitics, Indo-pacific.

INTRODUCTION

The AUKUS agreement between Australia, the United Kingdom, and the United States is a step towards building an alliance to manage the collective geopolitical goals and ambitions of these countries in the Indo-Pacific region. The alliance also aims to address, primarily, the complex cyber threats (Wilkins, 2022) emerging in the Indo-Pacific region, particularly with China, highlighting the importance and necessity of a specific competition strategy and unified planning to stabilize the region and achieve the objectives (AUKUS Forum, 2024).

However, the reconciliation between defense and cybersecurity interests within the alliance seems somewhat unbalanced according to known notions of national sovereignty, while the fight against geopolitical and cyber threats requires a balance between the principles of collaboration and the concepts of cyber sovereignty (Shen, 2016). To this end, the AUKUS alliance seeks to maintain the formulation of a framework for cooperation in cyber diplomacy and a specific cyber strategy aimed at strengthening the foundations of diplomatic ties between the members and the institutionalization of collaboration in cybersecurity.

According to Bell and Mbaziira (2023), the alliance aims to provide a specific framework in cybersecurity, beyond the known international commitments in this field, and to inaugurate a new stage of cyber trust, based on the principles of liberalism and to overcome the slowness of international efforts in cybersecurity. Sharing technological potentials among members to strengthen cybersecurity among its states and secure shared infrastructures and common devices, the alliance seeks to offer deep operational trust among its members (Radanliev, 2024). In accordance with its announcements, the alliance aims for a common technological integration to strengthen the unity of Western cyber defense in the region against potential rivals and competitors (AUKUS forum, 2024).

It should be added that the unfavorable geopolitical context in the Indo-Pacific interacts negatively with the objectives set by the alliance, imposing other realities that influence the operational process of the alliance. This indicates that the context of the operational implementation of the alliance must take into account diplomatic changes and strategic transformations in the region, where cross-border measures applied by Indo-Pacific states change the game and certainly involve rivalries, geopolitical confrontations, and diplomatic tensions with the states of this region (Kennedy & Sariguna, 2023). However, the obligation to reconcile the imperatives of national interests with the requirements of a common and collaborative cybersecurity stipulates the existence of robust governance mechanisms and instruments, associated with adaptive policies and regular practices to reconcile concerns, sovereign interests, and the objectives of AUKUS (Centre for Advanced Cybersecurity Research and Engineering, 2020).

*Address correspondence to this author at the Founder and director of the Moroccan Center for Cyber Studies and Technology Security, Professor at Mohammed I University, Oujda, Morocco.; E-mail: m.kezzoute@ump.ac.ma

In this article, based on the inductive method, we examine the interactions between the principles of digital sovereignty and the collective cybersecurity mechanisms established within the alliance. We critique the traditional framework of international alliances in the field of cybersecurity, particularly in the areas of cybersecurity and digital sovereignty, while proposing recommendations to harmonize national interests with the ambitions and objectives of the alliance. We also examine the geopolitical applications at the level of cyber diplomacy, incorporating a forward-looking vision of the challenges that may arise during the implementation of this strategy. We believe that our analysis will help improve the functioning of the alliance and the respect for the fundamental principles of international security, including by contributing to the reduction of tensions and malicious intentions in the region.

The Grande Lines and the Ambitions of our Research

According to Markowski (2024), the context of the alliance represents an advancement in cyber warfare by engaging members to cooperate and share experiences in intelligence, technical expertise, and best practices in defense and security outside of known conventional frameworks. The author also attests that the main objective of this group is to protect the interests of the alliance's states in an unfavorable geopolitical context in the Indo-Pacific, to keep the members' profiles away from security turbulence in the region, and to ensure cyber resilience.

In this regard, the alliance seeks to develop its capabilities in surveillance technologies and cyber threat detection, to secure the alliance's vital infrastructures, and to strengthen cooperation in the field of cyber intelligence (Dolan, 2024). This will facilitate, according to the same author, responses to cyber threats through intelligence sharing and collective maneuvers in this field, although it raises multiple questions regarding the sovereignty measures of member states, the alliance will offer members an exceptional potential to strengthen national cybersecurity capabilities.

In this section, Wyatt (2024) notes that cooperation within AUKUS has indeed improved the cybersecurity and cyber defense mechanisms and instruments of the members in response to the growing emergence of informational and technological influence from rivals in the Indo-Pacific. However, the author puts forward certain hypotheses highlighting the complete misalignment of the United Kingdom and Australia with the geopolitical ambitions of the United States in the region, where a form of hegemony exists and is also well defended by the detractors of this alliance. This means that statements regarding the privilege of American defense at the expense of the allies' sovereignty principles can potentially constitute a limiting reality for the existence of a cybersecurity policy independent of issues of hegemony and American supremacy in the alliance's strategy.

At the operational level, the partnership for data and intelligence sharing among alliance members, in order to serve the strategic cybersecurity objectives of the alliance, can introduce a lack of thorough control over certain sensitive information, or a misinterpretation or sharing of collected data or an analyzed situation, or even a poor execution of a trilateral decision, due to the presence of massive amounts of security information (Dows, 2022). And according to the same author, this probable situation of disorganization can distort data governance processes and disfigure collaborations and other related processes such as filtering, analysis, and interpretation.

Indeed, the alliance not only imposes challenges but also offers us a specific paradigm of international cooperation in the field of cybersecurity and cyber governance, highlighting the imbalance between the needs for cybersecurity and cyber defense and the functioning of global governance in the face of the internal interests of nations (Kezzoute, 2024). In terms of stakes, this could impose a new dynamic in the global governance of cyberspace, strengthening the influence of the West and the neoliberal paradigm, as well as their protocols and arrangements for cyber cooperation, to the detriment of the well-known traditional or classical balances, widely used in the international system to establish norms recognized by international law.

This means that the states of the alliance, although they are members of global commitments to combat cyber threats and instability in cyberspace, are dedicating more efforts to succeed in this new regional experiment. However, by prioritizing the successful implementation of the alliance at the expense of international commitments, one reinforces the detractors' hypothesis against international governance of cyberspace and collective commitments in cybersecurity.

However, the framework of the alliance can serve as a catalyst to encourage international efforts and advance discussions on cybersecurity and global

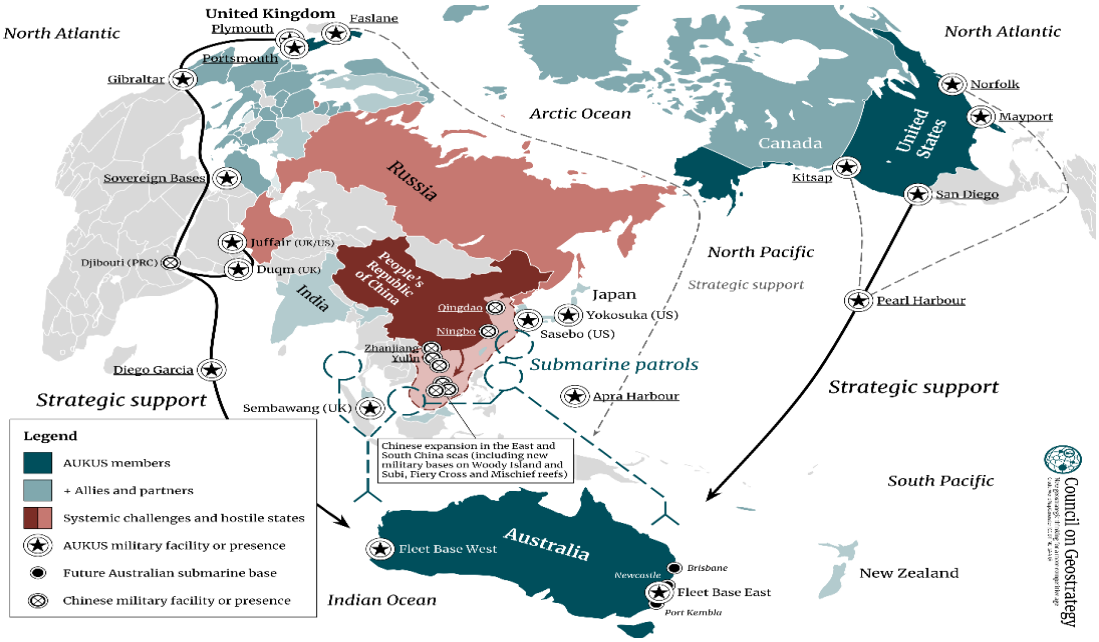

Figure 1: This map demonstrates The geopolitics of AUKUS and the power competition in the Indo-Pacific region realized by the Council on Geostrategy[1].

cyberspace governance. This could hypothetically serve as a model and alternative to global cooperation frameworks in the field of cyberspace, where the exclusive nature of AUKUS, although it brings benefits, can extend its effects throughout the entire region, intensifying geopolitical and strategic rivalries and multiplying obstacles to various regional international dialogues (Markowski, 2024).

The AUKUS Alliance, the Context of Urgency, and the Theoretical Framework

Although its historical process is too short, AUKUS marks the advent of a new era of security and defense alliances and international cooperation, aiming to defend the interests of its founding member states and to protect multiple ambitions and interests against politically and strategically motivated cyber threats (AUKUS, 2024). Called the Five Eyes Initiative, Godovanyuk (2022) shows that the alliance aims to consolidate an in-depth sharing of intelligence in the field of security and to strengthen defensive cooperation among members, beyond known frameworks, in technological and cyber collaboration at the level of international organizations in order to balance China's operational game hindering Western interests in the Indo-Pacific region.

The alliance involves three powers, with Australia's confrontation against regional threats developing due to Chinese and Indian hegemony in the region and minimizing Australia's ambition to acquire technological innovations monopolized by a few global powers (AUKUS, 2024). The United Kingdom, due to the post-Brexit situation, sees the AUKUS alliance as a solid opportunity to make a significant return to the international political stage and to reaffirm its power in the Indo-Pacific region (Godovanyuk, 2022). Whereas for the United States, it will become clear that the alliance aims to alter the balance of power in the region and redefine the geopolitical situation in the Indo-Pacific to China's strategic and geopolitical disadvantage. For these reasons, AUKUS constitutes a genuine framework of cooperation and partnership to develop collective strategies that encompass multiple objectives and ambitions in the Indo-Pacific region (Overview of AUKUS – The quasi-Indo-Pacific alliance, 2024).

The alliance, in terms of regional influence and global repercussions, is considered in specialized writings as an initiative aimed at altering the balance of power, due to the security potentials it has offered to its members, while simultaneously raising concerns among certain states in the region (Li, 2022). From these concerns, the opposing states in the region have expressed their rejection of this alliance, due to its alteration of the regional security balance and existing political and strategic orientations. Alongside these

[1]Source of the Map : https://www.geostrategy.org.uk/research/the-geopolitics-of-aukus/

claims, AUKUS has also raised global concerns due to its fueling of interstate competition among international powers and the way these powers interpret these changes in regional spheres of influence and hegemony (Karp & Maass, 2024).

At the heart of these changes and fears, deep cybersecurity plays the most important role in the AUKUS strategy, as within the alliance, the consolidation of intelligence collaboration frameworks, deterrence, detection, and response is defined as the cornerstone of this strategy (AUKUS Forum, 2024). This importance is due to the convergence of the intentions of instigators in the cyber territories of the Indo-Pacific, exploiting the vulnerabilities of international, regional, and national frameworks, and thus, with the help of state intelligence agencies, refining cyberattacks against the vital assets of the region's states (Indo-Pacific Defense Forum, 2024).

In addition to its implications, the AUKUS alliance will have economic dimensions, not deeply discussed in this study, where the joint development of technologies among member states encourages research and innovation, including shaping their companies' access to colossal investments in these areas, thus creating unprecedented economic and employment opportunities (Markowski *et al.*, 2024). In the same vein, the amplification of the defense budgets of the member will have a favorable effect on value creation and revenue stimulation, as well as on the development of national defense industries and companies. However, experts warn us about the possibilities of invoking a new arms race that the international system and the countries of the Indo-Pacific region no longer need (Rooney *et al.*, 2021).

Theoretical Paradigms for Understanding the Dynamics, Implications, and Potential Future Trajectories of AUKUS

Digital diplomacy, as a concept, is often used to describe a situation where diplomatic efforts extend into cyberspace in the form of alliances, agreements, conventions, treaties, etc. However, the concept reinforces its innovations by neglecting certain traditional norms of international law and classical diplomacy, giving rise to new dimensions of negotiation navigating complex dynamics, establishing cyber norms and specific digital frameworks (Delerue *et al.*, 2020). This transformation in diplomacy has been fueled by the fluid nature of cyberspace, where traditional diplomacy is no longer relevant given the rapid changes in cyberspace (Desforges, 2014). Because using the vision of traditional inter-state diplomacy to respond to what cyberspace imposes on international relations increases the potential for disagreement between states in situations of rivalry or tension, to the detriment of maintaining stability and trust (Barrinha, 2024).

Cyber sovereignty at this moment, as a principle of interoperability in cyberspace, challenges the notion of sovereignty as we know it, given that the infrastructure constituting the global web escapes the constraints of borders and the material requirements of geographical controls and surveillance, making digital sovereignty an element to be rethought and re-discussed. Because in international law, sovereignty defines the existence of a political power and a will to control and regulate a defined territory, we note that with the existence of cyber technologies, these principles will become obsolete, rigid, and will require new reformulations and reinterpretations (Moynihan, 2020). AUKUS offers its members the opportunity to go beyond the traditional requirements of international law and especially conventional diplomacy, by establishing a specific order of cooperation. However, the alliance raises questions about the balance between security and defense requirements and the respect for national sovereignty principles, to which the treaty-signing countries are exposed to revisions regarding their interpretations (AUKUS Forum, 2024).

The deep cooperation that this paradigm proposes, particularly in sensitive areas such as cybersecurity and defense technologies, intelligence, affects the ability of members to independently control their sensitive information as well as the flow of information within their cyber territories (Moynihan, 2020). In addition to the other international commitments of these states within the framework of global initiatives, this, due to the interoperability of agreements and the weakness of national cybersecurity frameworks and cyber strategies in these countries, further reduces independent action in cyberspace and weakens the control of national territories in cyberspace according to the same author.

The analytical potentials of neorealism in the field of international relations will help us understand the dynamics of power competition in the Indo-Pacific region (Arslan, 2022). Proven by Chinese interpretations related to this alliance, surely perceived in terms of interstate competition, as an attempt at encirclement and strategic and geopolitical weakening, particularly directed against China's technological and cyber capabilities and its geopolitical ambitions in the region (Li, 2022). This determines the existence of a

real local and interstate power game between regional and global powers in this region, further fueling rivalries and leading to new power dynamics and geopolitical competitions that are already burdensome for the region (Russian International Affairs Council, 2024).

The relations within and around the alliance can be interpreted from other perspectives, when suspicions regarding China's ambitions in the region are not the only ones, as the objectives of the members are also active and in a mode of internal competition. That is to say, within the alliance itself, we can demonstrate the presence of competition among the members, where issues related to deep collaboration impose a clear burden on the full implementation of the alliance since its signing. The concession of certain rights and the abundance of certain freedoms to act individually and independently in certain areas, while prioritizing the overall cause of the alliance, inevitably provoke political competition and internal diplomatic disengagement (Chernenko, 2018). However, despite this internal competition, the liberal nature of the alliance and its member states encourages the deepening of cooperation and intensive collaboration to the detriment of the isolated strengthening of individual national cybersecurity policies (Buckland *et al.*, 2015).

According of Hosh and Issa (2024), which attest to the hegemonic nature of the alliance, the authors also testify that these three powers are not aligned in many areas of comparison, from the economy to global geopolitics. They argue that the superpower at the head of the alliance stimulates international problems that distance the members and divide Western consent around these international issues. Thomann (2020) sees that this situation stimulates the emergence of forms of competition arising from disagreements and the mismanagement of international issues, disrupting the functioning of the alliance which maneuvers to establish common behaviors and feelings of trust that underpin collective action against new cyber threats. In the following paragraphs, we will dedicate more space to examining the decisions and practices, particularly political ones, within the alliance in order to analyze the manifestation of the theoretical frameworks we have used to shed light on the controversy.

This may involve analyzing a well-known event within the alliance to closely examine the coordinated response of member states and how they are trying to overcome challenges and imbalances for better collective collaboration. Following this analysis, we are putting more effort into addressing our investigations on how this alliance will contribute to encouraging the development of solutions and international standards in cybersecurity and cybergovernance.

METHODOLOGY

We base our study on relevant documentary research related to AUKUS, including agreements, reports, and national strategies, particularly in the field of cybersecurity. We also commit to conducting a comparative analysis between the members' visions and their approaches to addressing and responding to issues related to cyber threats, in order to measure the convergence or divergence among the actors involved in the study and how the members harmonize their efforts to protect vital infrastructures within the alliance. The discourse also constitutes a factor of analysis, particularly the statements of decision-makers or politicians and strategists from these countries. This specific approach that we have adopted to achieve our research objectives also contributes to the emergence of a new vision and evaluation never undertaken or realized before on the exploration of the impacts of the AUKUS alliance on the national requirements for cybersecurity and cyber defense of the member states in a geopolitical and strategic context of ongoing competition and rivalry.

THE ANALYSIS

The formulation of the AUKUS alliance has imposed a context of power competition on China in the Indo-Pacific region, including technological and military regional rivalries. The fact that China is already demonstrating multiple ambitions for the Indo-Pacific region due to its global Belt and Road Initiative, which will have worldwide repercussions and impact the region targeted by AUKUS, justifies, according to the founders of the alliance, the existence of behaviors aimed at limiting Chinese ambitions in the region (Imannurdin *et al.*, 2024). This means at first glance that the cornerstone of the alliance's existence is purely geopolitical and strategic, aiming to strengthen the capabilities of the allies in the face of Chinese ambitions, which seeks to extend regional hegemony, particularly technological.

The members of the alliance are not only seeking to consolidate their strategic presence, but also envision deepening cooperation among themselves and with their environment as part of this strategy. Intelligence and cybersecurity, as well as the transfer of advanced technologies, and global and regional security issues are at the forefront of the diplomatic concerns of the members, including encouraging neighboring countries and regional actors to support the existence of AUKUS,

away from political claims. Yet, the alliance, as a grouping seeking to impose a new reality in the Indo-Pacific region, is often criticized for defending Western interests at the expense of the interests of the states in the region (Sumandianta, 2023).

In addition to the above, among the reasons justifying the existence of the alliance, there is the slowness of international law mechanisms, which, according to the decision-makers of the alliance member states, are not yet capable of deterring cyberattacks against their advanced cyber infrastructures. That is why the member states are committed to strengthening their collective defense and cybersecurity capabilities within the alliance and establishing specific and collective standards to fill the gaps in international law procedures related to cyberspace. What is ultimately seen is a strengthening of the positioning of member states at the international level in cyberspace, as well as a limitation of the hegemony of the Chinese model in both cyberspace and the real world (Cheng, 2022). In addition to the previous arguments, the existence of the alliance, according to Dolan (2024), also demonstrates that it is no longer just an alliance against China, as the promotion of new standards of collaboration and organization, the procedures for cooperation and sharing of technological knowledge and security innovations, as well as the consolidation of feelings of responsibility among the members, constitute a strategic choice within the alliance.

As a pact uniting states to address challenges and achieve interests, AUKUS also seeks to establish its own decision-making and governance process. The fact that the alliance is still new compared to others in the field of international security and defense makes its initial state still evolving and under discussion, and open to proposals among the members. But given that the final framework of the alliance is still under discussion years after its creation, it should be noted that the decision-making process takes into account the cooperative, partnership-focused nature and the liberalism of the members, and is attentive to global and regional geopolitical changes, where considering the opinions, orientations, positions, and considerations of each member state of the trilateral alliance before making a decision is an obligation.

Indeed, the distinct capabilities of the members in various fields weigh on the decision-making processes, in which the United States, thanks to their technological and cyber capabilities, probably influence the relations within the alliance and define the work and cooperation agenda of the allies as a global leader and partner in security and defense (Leonova, 2022). Sumadinata (2023) confirms the idea, explaining how the United States, due to their positions including in the cyber domain and their wealth of technological expertise and operational intelligence, enrich and affect the behaviors of all other AUKUS members by the way they discuss international issues, despite the confirmation of the democratic and liberal nature of the studied alliance.

Meanwhile, for different reasons, it will become evident that the influence of the United States within the alliance is very real due to their positioning in the global power game. This concludes that we are indeed faced with a management and governance system, although it is democratic and specific, which emphasizes the liberal and democratic aspect to promote cooperation and collaboration within the alliance. But, it is based on the varied priorities and capabilities of the members. This confirms why the United Kingdom and Australia bring specific perspectives supported by their geopolitical visions and positions, while trying to escape the influence and hegemony of the United States in this negotiation context (Department of Defence, 2021).

Aligned with our analysis, Poshedin (2022) confirms that the members emphasize interactive and intelligent cooperation in the field of intelligence and the sharing of essential information in order to operationalize cooperation and cybersecurity processes in the region. He adds that this operation reinforces the views that have examined the alliance's past, the mechanisms of cyber defense, and ensures the establishment of robust deterrent measures against cyber threats attempting to weaken the alliance's cyber capabilities in the Indo-Pacific region. However, Imannurdin *et al.* (2024) emphasize that this type of cooperation will introduce complexities related to the legal and regulatory frameworks governing this activity within the alliance, as well as the security requirements for sensitive information, adding more obstacles to full cooperation in the field of intelligence and to the decision-making process within the alliance.

In addition to the above, internal complexities cause undesirable disruptions and impact the functioning of the alliance, affecting the decision-making processes within the alliance. It is also added that the issue of intellectual property and the protection of industrial and technological secrets may be given little consideration, as collaboration on critical technological issues, including cyberwarfare tools and the massive flow of information and data, as well as the fight against

decision-making bureaucracy and the cooperative management of vital digital infrastructures, can introduce disruptions regarding the respect of specific rights to the detriment of filling security and defense gaps (World Economic Forum, 2024).

This means that the fact that AUKUS members have essentially come together to combat violations and to strengthen their capabilities to counter cyber threats against the alliance's assets can lead to disruptions in the overall system of trust and accountability governing the alliance (Korwa & Wambrauw, 2023). And confirms that the importance of having specific instruments to defend the alliance's vital assets and infrastructure, as well as defense secrets, is crucial (Halvorsen, 2024).

In this aspect, the alliance seeks to find a balance between its security and legal requirements, and the need for cooperation among allies to maintain the geopolitical and strategic preeminence of the alliance in its operational environment. However, we have found that the principles of sovereignty regarding certain issues are indeed in conflict with the general principles of the alliance, as the states do not wish to fully relinquish their powers in favor of a common decision-making body that is still in the process of being established and is in disagreement in terms of status, rights, obligations, and competencies, even though their political systems are based on the ideas of federalism and libertarian principles.

And moreover, intelligence and cybersecurity are emerging as the main areas where members insist on not handing over management to external contractors or partners with limited experience in the field of cybersecurity, or who do not adhere to their political commitments (Leonova, 2022). Moreover, during the creation of the AUKUS alliance, the negotiations focused on potential disputes between internal rules and the impositions of the alliance. And although the complexity between the objectives of collective cybersecurity and national requirements and interests existed during the negotiation process among the alliance members, the United Kingdom and Australia demanded injunctions with their external interests under various pretexts. This did not actually limit the debate during these preliminary stages; on the contrary, disputes over several issues persist within the alliance and reinforce the need for its presence (Setiabudi Sumadinata, 2023).

The field of intelligence is the most decisive and reflects the degree of incompatibility between national interests and the strategic orientations of the alliance. Negotiations around defense protocols are likely to continue generating debates on compatibility with the alliance's sharing recommendations, thus illustrating the need to rethink the situation and reconcile conflicts. In this regard, the United States and Australia have conducted negotiations separate from the alliance, aiming to discuss the conditions for sharing sensitive information and to align cyber strategies without compromising national security (Poshedin, 2022). These efforts represent an attempt to strengthen trust and balance within the alliance, and to align the objectives and interests of the members while simultaneously aiming to reshape its image, presenting the alliance as an element of the United States' overall strategy, and the member states as agents implementing this anti-China strategy in the region (Kennedy & Sariguna, 2023).

Among the favorable points of the alliance in the field of cyber governance, there is the potential to influence global efforts to strengthen cyber governance and cybersecurity, avoiding the development of fragmented cyber institutionalization, heavily influenced by the geopolitical and strategic interests of states (Korwa & Wambrauw, 2023). The fact that this type of framework encourages states with technological and economic potential, as well as the willingness to participate in this pragmatic new cyber diplomacy framework, to surely engage in these initiatives, while ignoring international norms to individually stabilize cyberspace. Could favorably encourage the international community to rethink the situation and strengthen current efforts, consolidate the role of existing common international instruments and mechanisms, and also encourage the establishment of collective and cooperative frameworks and approaches, in order to prevent fragmentation and division of international efforts (Imannurdin *et al.*, 2024).

Although the initiative demonstrates that countries unable to participate in these bilateral and trilateral initiatives cannot protect their interests as well as they could by participating in these powerful initiatives, which, on the other hand, divide international efforts in digital governance and threaten the international vision of cyberspace. AUKUS has also raised concerns in the Indo-Pacific region, where the states directly involved in its creation have denounced its establishment within ASEAN, claiming that this alliance will trigger a new technological arms race and constitute a new American project of destabilization and hegemony (Nindya & Abbiya, 2022).

These detractors denounce the alliance due to its influence on power dynamics in the region, as the alliance will contribute to the emergence of new rivalries by forcing the states in the region to revise their national cybersecurity policies and support them with more offensive and aggressive frameworks. In fact, AUKUS will not only lead to more power struggles, militarization, and the collapse of international cybersecurity efforts, but it will also encourage countries in the region to work harder within regional and international organizations to protect their cyber territories in accordance with international cybersecurity standards (Dowse, 2024).

How Does the AUKUS Alliance Interpret the Domain of Cyberwarfare?

AUKUS is considered a step forward in strengthening cybersecurity and cyber defense and an important step in repositioning its allies in cyber governance. One of the main objectives of AUKUS is the improvement of the nuclear-powered submarine technologies of its members and the strengthening of the cyber defense and cybersecurity capabilities of its allies by expanding their skills towards broader geopolitical dimensions related to cybersecurity. However, cyber diplomacy within the alliance continues to play essential collaborative roles, helping to overcome complex situations exacerbated by cyber threats in the Indo-Pacific region. We wish to expand the analysis and approach we have used to effectively manage the issues arising from the interaction between diplomacy and technology used to resolve disagreements while respecting national principles.

However, the situation in the Indo-Pacific region is still complicated, as the intelligence agencies of certain states are known for encouraging criminals to carry out cyberattacks against the most important targets of the alliance states or even against other countries. Moreover, the advanced methods that states use for economic cyber-espionage aim to minimize the technological development gap between advanced states and rivals in the Indo-Pacific region. Position China as a leader in these areas of stealing sensitive data and industrial and technological secrets. These activities heighten fears towards China, as it no longer targets only economic or commercial entities; rather, a significant number of attacks likely target the military and security infrastructures of Western countries (Murphy & Nagy, 2024). Moreover, the region is already facing a series of professional cyberattacks that do not all originate from China, with North Korea, Russia, and a number of other criminal groups, etc., flooding the region and targeting the interests of AUKUS countries, strengthening the will and logic of the targeted countries to engage in initiatives accelerating the need for regional protection frameworks in cybersecurity and cyber governance (Radanliev, 2024).

The AUKUS states were supposed to establish a regional cooperation system to overcome the perilous situation in the region, prevent the spread of cyber threats, and reduce the effects of geopolitical rivalries threatening the assets of the alliance members. This requires new ideas on how to establish rules for information sharing and collaboration, particularly in the field of intelligence, where member states can work more closely with external international security agencies like INTERPOL and EUROPOL, for example, and not just see what they can do alone in order to avoid confirming what non-adversaries of AUKUS assert within the international community (Sendjaja *et al.*, 2024).

When members develop new rules and procedures to share and achieve their objectives, they can also examine what other international organizations have done in the field of cybersecurity and cyber defense, such as NATO's efforts to stabilize cyberspace (Oancea, 2022). In this way, we can agree that countries wishing to learn from the experiences of international organizations in the field of cybersecurity and cyber defense, which they deem necessary to improve the alliance's capacity to respond to and manage crises, as well as to strengthen trust and streamline operations among its members, will succeed in achieving their objectives.

AUKUS, in other ways, can also strengthen these skills in cybersecurity resilience by bringing together discussions on digital governance in its region and with ASEAN countries, particularly India. By focusing on states outside the alliance, this can help make the members' cyber defense capabilities more effective and the interoperability frameworks more efficient. This will not only improve the alliance's image within the international community but also strengthen the trust between its members and, eventually, its future partners in the measures it takes to protect itself against cyber threats. AUKUS should pave the way for the development of more relevant international standards in the field of cybersecurity and strengthen its presence within the UN, and not be an alternative to major international organizations or mere extensions of existing institutions (Zinovieva, 2022).

Indeed, the improvement of cybersecurity and cyber defense within AUKUS primarily involves understanding and taking into account the geopolitical issues and all the strategic challenges of the region, as well as integrating a broader vision that respects the alliance's objectives and the regional stability and security requirements in the Indo-Pacific. The alliance must not only avoid pushing the states in the region into an arms race by making them distrustful of each other, but it must also respect the digital sovereignty of its members and states outside the region. These states must feel in control of their own cyber territories and digital infrastructures and not fear the objectives and ambitions of the alliance. In this regard, it should eliminate and avoid unilateral practices that can alter and degrade its image with the international community, by engaging in intrusion and espionage practices or cyber infiltration or any other practice that disrespects the national sovereignty of other states or involves anyone in the global cyberspace (Kaloudis, 2024).

On the other hand, harmonization with the states of the region, particularly the ASEAN community, promotes accountability and integration, giving the impression that AUKUS is an alliance of law and stabilization rather than a hegemonic and geopolitical domination force. Communication and dialogue, particularly in the Indo-Pacific region, will strengthen – although this is a utopian assertion – not only the image of AUKUS as an alliance seeking to help its members overcome the situation of gaps and voids that criminals exploit for their security and stability. But also, to avoid escalation and undesirable rivalries by sending messages of pacification, balance, and cooperation (Tsvetkova *et al.*, 2022).

Alongside the technological innovations that the alliance offers to the international community, innovations in the field of cyber norms aimed at international cyber cooperation and the promotion of cyber governance remain at the forefront of these adopted novelties. And it is in this case that the frameworks invented by the alliance states can in the future help other states around the world overcome their problems in cyberspace by establishing similar frameworks to address the challenges of international law and the strategic issues that hinder the good governance of cyberspace and the existence of a coexistence ecosystem, ensuring equality of members before the law and accountability.

Towards a more open strategic policy and cyber governance

In this chapter, we attempt to present guidelines for the implementation of recommendations, taking into account the geopolitical and strategic impositions surrounding the alliance and how the members can collaborate and address cyber threats in the future, considering all these territorial requirements and impositions. At this stage, we confirm the intersection between sovereignty and cyber diplomacy, where sovereignty, as an essential legal element in the constitution of a state (The State, Subject and Actor of Public International Law, 2026), poses several problems, where national legal principles come into conflict with the novelties of digital technology, generating multiple issues and questions of territories and sovereignty. This contradiction is often manifested within AUKUS, preventing member states from maintaining full oversight over their digital infrastructures without compromising the processes of openness and common cybersecurity (Krasikov Lipkina, 2020).

We illustrate an example addressed in the attempts to reconcile sovereignty with the diplomatic and security obligations of the alliance. In this regard, Australia has implemented an innovative plan operating under the alliance's competencies, named CESAR –Cyber Enhanced Situation Awareness and Response–, which illustrates the efforts to balance cybersecurity obligations with the principles of national sovereignty and common security, as well as the determination of Australian decision-makers to defend their principles in an environment of technological supremacy and imbalance (Department on Home Affairs, 2020). This program aims to strengthen Australia's position at the national level and within the alliance, distancing it from the hegemonic appeasements of other alliance member states. Such procedures reflect the willingness of member states to introduce policies aimed at strengthening the capabilities of states within the alliance without violating their mutual commitments and the objectives of the alliance, particularly regarding the sharing of sensitive intelligence and collaboration against cyberattacks (Gov-Au, 2025).

Similar initiatives in the United Kingdom are numerous, such as the NCSC, National Cyber Security Centre, the Security Operations Centre SOC, governmental, and the Cyber Essentials initiative (Gov-UK, 2025), while in the United States, the instruments operating in this field are now multiple, including the SAIR Situational Awareness and Incident Response, complemented by the CESER agency (Office of Cybersecurity, Energy Security, and Emergency Response) and the CISA, Cybersecurity and Infrastructure Security Agency, which crown cyber

policies (Gov-USA, 2025). These initiatives, alongside several other organizations and institutions in these states, can serve as case studies in diplomacy and cybersecurity for other states and regions of the world, regardless of their position, and to leverage the innovation and creativity of these experiences to move away from voices advocating for concentration and firmness towards more open and cooperative visions.

Far from the direct issues of sovereignty, we have also noticed that the socio-technical context of the alliance plays an influential role when the geopolitical and strategic issues of the Indo-Pacific play an important role in determining each study or analysis of interstate interactions and also influence the responses and management of causes as well as the way in which the states of the region react to phenomena. It is due to China's genuine rise in power in the region that we argue the alliance is actually a response to curb its ambitions and not merely a process of cooperation against cybercrime.

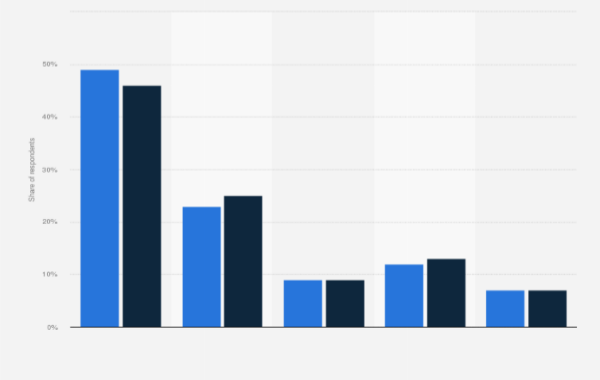

Figure 2: The Survey realized in 2023, demonstrates how Australians perceive their integration into the AUKUS alliance as a solution to consolidate national security and defense[2].

And it is in this context, alongside the promises of granting technological potential, that the United States and the United Kingdom promised Australia the provision of sophisticated nuclear submarines and committed to guaranteeing advanced cyber defense technologies in the future, strengthening Australia's cyber deterrence capabilities against China (Cheng, 2022). The acquisition of these submarines is not just a deterrent act to limit Chinese influence and hegemony in the region, but also involves the cybersecurity of military communications traversing cyberspace and specifically the networks of submarines among the alliance's member states, aiming to encircle China's maritime strategy in the Indo-Pacific (Babbage, 2024).

Not only the Australian decision-makers are influenced by the proposals of Western allies, which the masses also believe, that the AUKUS treaty will provide the nation with unprecedented defensive and security potentials as shown in the graph above. In the same vein, the alliance is strongly supported at the national level, giving the United Kingdom the opportunity to benefit from its imperial legacy and return to the international political stage, thereby restoring its hegemonic power in this region of the world over which it lost control in previous decades, while escaping American influence and imposing the concept of an open alliance (Suparman, 2024).

To further measure the benefits of the alliance, it will become apparent that the emergence of new collaborative orientations based on a liberal openness, particularly with neighboring parties such as Japan and India, constitutes a step forward in consolidating open and broad cooperation with partners and rivals, and in consolidating the alliance's presence in its operational environment (John, 2024). This underscores the importance of listening to ongoing issues and attempting to balance them according to the requirements of AUKUS and the region, while avoiding potential tensions with China and its allies in the Indo-Pacific. These arrangements for the AUKUS states and also for the states of the entire region constitute diplomatic innovations to be followed in order to find solutions to the tensions with China due to AUKUS. However, diplomatic engagement motivated by the challenges and interactions of the environment and context, and which seeks to find balanced solutions, is very important to avoid regional escalations and tensions, by alleviating anxiety and improving trust and stability (Ro'is, 2022).

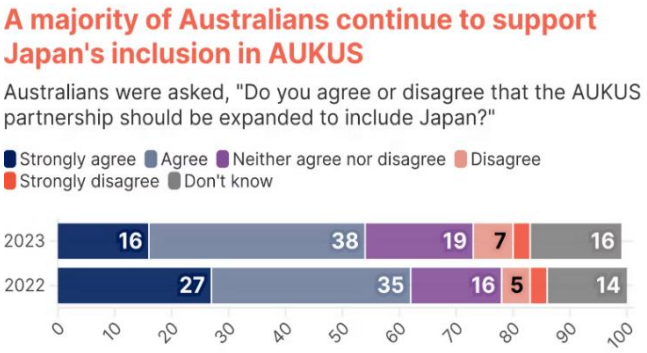

Figure 3: The Figure realized by the United States studies Center, demonstrates how the majority of Australian really support the integration of Japan to the AUKUS alliance[3].

[2] Source of the Survey : https://www.statista.com/statistics/1451801/australia-perception-of-aukus-alliance/

[3]Source of the Figure: https://www.ussc.edu.au/by-the-numbers-or-most-australians-agree-with-expanding-aukus-to-include-japan

The popularity of AUKUS in the diplomatic and Indo-Pacific environment is increasing, with the general opinion studied showing that the acceptance of the alliance's expansion towards new actors in the region is progressing. This demonstrates that the alliance constitutes an opportunity for the populations of the allies to benefit from in order to stabilize the region and develop cyber efforts. This is due to the opportunities offered by the alliance to produce good practices in cyber diplomacy and security and defense cooperation, and the establishment of trust and assurance of communication and openness in a tense region (Yulyanti, 2023).

In the same vein, Zinovieva and Shitkov (2023) confirm that the alliance can be used to merge interests in the region and encourage influential states in the Indo-Pacific to integrate into this approach with the aim of balancing the game in the region. The integration of Indonesia, Malaysia, India, as well as influential countries in this initiative, will strengthen the alliance's capabilities in the areas of collaboration against cyber threats and global security issues and challenges in the region, and will also minimize fears among the Indo-Pacific states.

In this legacy of AUKUS, we anticipate that this environment will encourage the development of stability and accountability standards in cyberspace and strengthen trust and belief in international norms and institutions, fortifying their capacities to maintain order and stability in this regional space. AUKUS will help the international community draw lessons and provide the necessary responses in terms of reforms of essential legal frameworks for good conduct and governance in cyberspace.

CONCLUSION

In terms of results, in our article, we explored two main objectives: the first is the examination of cooperation in the field of cybersecurity and the study of the progression of collaboration in the face of the multiple obstacles listed by the study, in which the principles of sovereignty play a major role. The alliance teaches us several lessons on the progress in cooperation and collaboration in the field of intelligence and the sharing of sensitive information related to security and defense. It also serves as a concrete example of the level of collaboration in regional security and the efforts to limit bureaucracy and control the debate around the concepts of national autonomy that the member states have achieved. As a result, the member states have somehow managed to control the debate and find a balance between their principles and the operational requirements of the AUKUS alliance, with these interactions taking place in one of the most geopolitically sensitive regions in the world.

Alongside internal concerns related to cyber governance and the challenges of managing inter-state sovereignty within the alliance, it will become evident that members are facing several other issues. The states in the region express their distrust regarding the hidden objectives of the alliance and the undeclared ambitions, which include the destabilization of the region and the reconfiguration of interests in this geographical area according to the Western vision. It is within this analytical framework that we have observed that the states in the region, particularly those that are not members of the alliance, have repeatedly expressed their distrust and, indeed, their rejection of this initiative, undermining their traditional influences in the Indo-Pacific. Although the member states of the alliance try to attribute a non-aggressive nature to the alliance with slogans of technological cooperation, the non-member states, the rivals in the region, criticize this initiative and prefer to depict it as a Western hegemonic status. However, the alliance has offered its members multiple advantages by redefining the balances in the region and opening new perspectives for negotiations and strategic cooperation with all the states of the Indo-Pacific.

In addition to the advantages that the alliance can offer to experts and professionals to enhance their expertise in cooperation frameworks and the precise study of the issues and challenges surrounding alliances and diplomatic pacts. AUKUS can also serve as an example and implication for cyber governance and cybersecurity for other regions wishing to engage in a similar process or improve their positioning in these processes at the global level. Because the collaboration model that the alliance proposes to its members seems structured and well illustrates that this collective initiative can respond to the evolution of complex cyber threats. These practices and implications could inspire decision-makers at the international level to redefine their confrontations and reconsider competition in order to stabilize their confronted regions and promote the existence of a stable and secure cyberspace.

However, the blind exportation of this experience without taking into account the specificities of the geographical regions confronted at the global level seems a bit adventurous. For within the alliance, we are faced with a clan of global powers that will indirectly

impose a new pace of competition in the region, alongside their principles of consolidating cybersecurity and cyber defense. This can, in some cases, hinder the ability of states wishing to import this experience to overcome divisions and address regional challenges and issues, pushing them to promote rivalries and confrontation instead of reducing them. Conversely, to leverage the governance lessons drawn from this experience, we recommend, in principle, the necessity of always finding a balance between the strategic interests of the confronted States and the need to consolidate trust and consensus among the actors of the international community.

We finally recommend that efforts continue to be made to strengthen digital diplomacy, support transparency and trust within the alliance and among member countries. Openness and accountability among alliance members and the Indo-Pacific community can reduce fears and strengthen trust if countries in the region are regularly included in consultation and discussion processes, especially with detractors. Because if the states of the South Asian region see themselves as partners in this process and not as competitors, it will give a boost of hope to AUKUS's efforts to stabilize the region according to the principles of geopolitical balance.

Indeed, to succeed in the alliance, it is necessary that the respect for sovereignty among the alliance members in cyberspace be institutionalized and organized. This should be achieved by respecting the rights of the members and their equality before the law as a fundamental principle organizing the alliance. This will change the pessimistic image and encourage states around the world to engage in similar initiatives to consolidate trust and sincerity in cyberspace, and will also help member states remain flexible in times of peril and vigilant in the face of the global geopolitical context. This openness and continuous collaboration between the alliance members as well as with their environment will strengthen the alliance's overall vision in cyberspace and the way they must approach professional cyber threats in the digital space, particularly those funded and organized by state services of incitement and strategic sabotage.

In addition to the above, we assert that the alliance's engagement in international initiatives and discussion forums, particularly at the regional level, will not only help the alliance achieve its objectives but will also similarly increase its global influence on the development of standards and frameworks in the field of global cyberspace governance. However, this will encourage the international community to take similar initiatives to strengthen the presence of cybersecurity frameworks and standards among the world's states and also to reinforce the paradigms of cyber defence and regional and global stability.

Finally, the future of the alliance, as we see it, will depend on its potential not only for cooperation, but also on the financial and technological integration of innovative cybersecurity techniques to develop the cybersecurity of its members and implement mechanisms of trust and accountability, which are also essential. It is equally essential to encourage the alliance's presence in similar initiatives to clarify its objectives and ambitions, often accused of hegemony and supremacy, and also to give rise to a resilient, inclusive, cooperative, and stable regional order.

REFERENCES

[1] Arslan, A. S. & Department of Political Science and International Relations, Marmara University, Istanbul, Turkey. (2022). Neorealist Analysis of Security Dilemma in Cyberspace; A Quantitative Study. Department of Political Science and International Relations, Marmara University, Istanbul, Turkey. journal-article. Retrieved from https://preprints.apsanet.org/engage/apigateway/apsa/assets/orp/resource/item/6426247691074bccd08f c239/original/neorealist-analysis-of-security-dilemma-in-cyberspace-a-quantitative-study.pdf

[2] AUKUS Forum, (2024). Advanced Cyber Capabilities: A Pillar of the AUKUS Partnership. Retrieved from https://aukusforum.com/aukus-news/f/advanced-cyber-capabilities-a-pillar-of-the-aukus-partnership

[3] Babbage, R. (2024, July 29). Deterrence and alliance power: Why the AUKUS submarines matter and how they can be delivered. Lowy Institute. https://www.lowyinstitute.org/publications/deterrence-alliance-power-why-aukus-submarines-matter-how-they-can-be-delivered

[4] Barrinha, A. (2024). Cyber-diplomacy: The Emergence of a Transient Field. The Hague Journal of Diplomacy, 19(3), 439-466. https://doi.org/10.1163/1871191x-bja10183

[5] Bell, N., & Mbaziira, A. (2023). Exploring a Diplomatic System of Cooperation in the Cyber Space through a Proposed Cyber Diplomacy Cooperation Framework. International Conference on Cybersecurity and Cybercrime, 10, 7–11. https://doi.org/10.19107/CYBERCON.2023.01

[6] Buckland, B. S., Schreier, F., & Winkler, T. H. (n.d.). DCAF HORIZON 2015 WORKING PAPER 7. Retrieved from https://www.dcaf.ch/sites/default/files/ publications/documents/CyberPaper_3.6.pdf

[7] Cheng, M. (2022). AUKUS: The Changing Dynamic and Its Regional Implications. European Journal of Development Studies, 2(1), 1–7. https://doi.org/10.24018/ejdevelop.2022.2.1.63

[8] Chernenko, E. (2018, February 9). Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms. Council on Foreign Relations. Retrieved from https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

[9] Delerue, F., Douzet, F., & Géry, A. (2020). Droit international et normes pour le cyberespace : ambiguïtés et instrumentalisation géopolitique. Études Internationales, 51(2), 287–312. Retrieved from

https://www.erudit.org/fr/revues/ei/2020-v51-n2-ei06608/1084460ar.pdf

[10] Desforges, A. (2014). Les représentations du cyberespace : un outil géopolitique. Hérodote, n° 152-153(1), 67-81. https://doi.org/10.3917/her.152.0067.

[11] Dolan, Ch. (2024). Perspective Chapter: AUKUS Pillar 2 – Technology, Interoperability, and Advanced Capabilities in the Evolving Trilateral Security Partnership. Book Chapter: National Security in the Digital and Information Age. http://dx.doi.org/10.5772/intechopen.1005189

[12] Dowse, A., (2024, February 8). Opportunities and Challenges of AUKUS | GJIA. Georgetown Journal of International Affairs. https://gjia.georgetown.edu/2024/02/07/opportunities-and-challenges-of-aukus/

[13] World Economic Forum (2024, September 10). Geopolitical rivalries are costly for global businesses. https://www.weforum.org/stories/2024/05/business-geopolitics-rivalries-private-sector-geoeconomis/

[14] Godovanyuk, K.. The Factor of Australia in British Foreign Policy. Journal of European Studies, 92(1), 308-314. http://dx.doi.org/10.1134/S1019331622100070

[15] Halvorsen, T., & Halvorsen, T. (2024, October 30). How technology and information sharing can help AUKUS protect the Indo-Pacific. IBM Blog. https://www.ibm.com/blog/how-technology-and-information-sharing-can-help-aukus-protect-the-indo-pacific/

[16] Hosh, M., & Issa, N. (2024). The Institutionalisation of Security Norms in the Context of Cyber Alignments: The Transatlantic Alignment in the Cyber Domain. Central European Journal of International and Security Studies, 18(2), 35–70. https://doi.org/10.51870/iluj7632

[17] Imannurdin, N. Y., Sudiarso, N. A., & Sianturi, N. D. (2024). The Impact Of The Aukus Alliance On China's Influence In The Indo-Pacific Region. International Journal of Humanities Education and Social Sciences (IJHESS), 3(5). https://doi.org/10.55227/ijhess.v3i5.976

[18] John, J. V. (2024). Navigating Indo-Pacific Dynamics: The Four Phases of India-Japan Strategic Partnership - Centre for Public Policy Research (CPPR). Retrieved from https://www.cppr.in/articles/india-japan-indo-pacific-strategic-partnership

[19] Kadlecová, L. (2024). Cyber Sovereignty: The Future of Governance in Cyberspace. Stanford University Press.

[20] Kaloudis, M. (2024). Digital Sovereignty as a Weapon of Diplomacy in Cyber Warfare in Democracies. In IntechOpen eBooks. https://doi.org/10.5772/intechopen.1005231

[21] Karp, R., & Maass, R. W. (2024). Alliances and Partnerships in a Complex and Challenging Security Environment. (Nato allied command transformation & Old Dominion University). sact nato hq. Retrieved from https://www.act.nato.int/wp-content/uploads/2024/06/NATO-AC24-Compendium.pdf

[22] Korwa, J. R., & Wambrauw, M. S. F. (2023). A Constructivist Analysis of the Establishment of the AUKUS Security Pact and its Implications for Regional Stability in the Indo-Pacific. Jurnal Hubungan Internasional, 16(1), 19–35. https://doi.org/10.20473/jhi.v16i1.36888

[23] Krasikov, D. V., & Lipkina, N. N. (2020). Sovereignty in Cyberspace: A Scholarly and Practical Discussion. Conference: XIV European-Asian Congress "the Value of Law." https://doi.org/10.2991/assehr.k.201205.028

[24] Leonova, O. (2022). The Impact of the Strategic Partnership AUKUS on the Geopolitical Situation in the Indo-Pacific Region. International Organisations Research Journal, 17(3), 194–211. https://doi.org/10.17323/1996-7845-2022-08

[25] Markowski, S., Wylie, R., & Chand, S. (2024). The AUKUS agreement: a new form of the plurilateral defence alliance? A view from downunder. Defense and Security Analysis, 1–20. https://doi.org/10.1080/14751798.2024.2385704

[26] Moynihan, H. (2020, December 17). The Application of Sovereignty in Cyberspace [Chapter 2]. In The Application of International Law to State Cyberattacks (pp. 5-11). Chatham House. https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace

[27] Murphy, T., & Nagy, S. (2024). Middle Power Cyber Security Cooperation in the Indo-Pacific: An Analysis Through the Lens of Neo-Middle Power Diplomacy. The Journal of Intelligence Conflict and Warfare, 7(1), 1–24. https://doi.org/10.21810/jicw.v7i1.6454

[28] Nindya, A. P., & Abiyya, R. A. (2022). The Influence of AUKUS to Indo-Pacific Regional Stability and Indonesia's Stance. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 13(1), 67–84. https://doi.org/10.22212/jp.v13i1.2917

[29] Oancea, V. (2022). Establishing Effective Cyber Diplomacy and Deterrence Capabilities between International Partners. Proceedings of the International Conference on Cybersecurity and Cybercrime. 9(n), 113-116. https://www.academia.edu/9750 1257/E/stablishing/Effective/Cyber/Diplomacyand/Deterrence/Capabilitiesbetween/Internationa/Partners

[30] Poshedin, O. (2022). A New Enhanced Trilateral Security Partnership between Australia, the United Kingdom, and the USA (AUKUS): Reasons for Creation, Consequences for International Security. Problems of World History, 19, 123–142. https://doi.org/10.46869/10.46869/2707-6776-2022-19-8

[31] Kennedy, J. & Sariguna, P. (2023). Analysis of the Indo-Pacific Outlook and Impact of the AUKUS Triatral Pact. International Journal for Research Publication and Seminars, 14(5), 197–213. https://doi.org/10.36676/jrps.v14.i5.1443

[32] Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology, 1–51. https://doi.org/10.1080/23742917.2024.2312671

[33] Rooney, B., Johnson, G., Priebe, M., & RAND Corporation. (n.d.). How Does Defense Spending Affect Economic Growth? Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RRA700/RRA739-2/RAND_RRA7392.pdf#:~:text=URL%3A%20https%3A%2F%2Fwww.rand.org%2Fcontent%2Fdam%2Frand%2Fpubs%2Fresearch_reports%2FRRA700%2FRRA739

[34] Russian International Affairs Council: The Strategic Impact of Expanding AUKUS in the Indo-Pacific. (n.d.). Retrieved from https://russiancouncil.ru/en/blogs/sufian-ullah/the-strategic-impact-of-expanding-aukus-in-the-indopacific/

[35] Ro'is, N. (2022). Cyber Sovereignty Gotong Royong, Indonesia'a Way of Dealing with the Challenges of Global Cyber Sovereignty. Pancasila and Law Review, 3(1), 15–30. https://doi.org/10.25041/plr.v3i1.2573

[36] Sendjaja, T., Irwandi, N., Prastiawan, E., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks. International Journal of Science and Society, 6(1), 1008–1019. https://doi.org/10.54783/ijsoc.v6i1.1098

[37] Schmitt, M. N. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

[38] Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. Chinese Political Science Review, 1(1), 81–93. https://doi.org/10.1007/s41111-016-0002-6

[39] Shi, X.. Beyond AUKUS: the emerging grand maritime alliance. International Affairs, 98, 441–459. https://doi.org/10.1093/ia/iiac014

[40] Sumadinata, W. S. (2023). Analysis of the AUKUS Agreement on Security in the South China Sea Region. Neo Journal of Economy and Social Humanities, 1(4), 265–271.

https://doi.org/10.56403/nejesh.v1i4.72

[41] Suparman, (S). Analysis of British Foreign Policy Forming the Australia, United Kingdom, and United States (AUKUS) Security Alliance in 2021. Asian Journal of Engineering, Social and Health, 3(3):548-555, https://doi.org/10.46799/ajesh.v3i3.260

[42] *L'État, sujet et acteur du droit international public*. (2026, February 8). Droits Africains Et Droit International. https://droitsafricainsonline.com/home/themes/introduction-au-droit-international-public/les-sujets-du-droit-international-public/letat-sujet-du-droit-international-public/

[43] The Indo-Pacific Defense Forum. (2024, November 12). Securing the Digital Future. Retrieved from https://ipdefenseforum.com/2024/11/securing-the-digital-future/

[44] Thomann, P. E., AUKUS, un triumvirat anglo-saxon dans l'Indo-Pacifique pour conserver l'hégémonie mondiale : quelle riposte géopolitique pour la France ? Non-alignement et Pivot vers la Russie – Eurocontinent. (2020). Retrieved from https://www.eurocontinent.eu /aukus-un-triumvirat-anglo-saxon-dans-lindo-pacifique-pour-conserver-lhegemonie-mondiale-quelle-riposte-geopolitique-pour-la-france/

[45] Tsvetkova, N., Sytnik, A., & Grishanina, T. (2022). Digital diplomacy and digital international relations: Challenges and new advantages. Vestnik of Saint Petersburg University International Relations, 15(2), 174–196. https://doi.org/10.21638/spbu06.2022.204

[46] U.S. Department of Defense. (2021). AUKUS: The Trilateral Security Partnership Between Australia, U.K. and U.S. https://www.defense.gov/Spotlights/AUKUS/

[47] White House. (2021). Remarks by President Biden on the AUKUS Partnership. https://www.whitehouse.gov

[48] Wilkins, T. Is AUKUS really an 'Alliance'?. Institute of South Asian Studies. https://www.isas.nus.edu.sg/papers/is-aukus-really-an-alliance/#_ftnref2

[49] Wyatt, A., Ryseff, J., Yoshiara, E., Boudreaux, B., Black, M., Black, J., & RAND Corporation. (2024). Towards AUKUS Collaboration on Responsible Military Artificial Intelligence: Co-Design and Co-Development of AI Among the United States, the UK and Australia. Research Report. RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3000/RRA3079-1/RAND_RRA3079-1.pdf

[50] Yulyanti, R. T. (2023). Strategy of indonesia maritime defense in the middle of Asia Pacific conflict potential implication of aukus vs people's republic of china. Jurnal Pertahanan & Bela Negara, 12, 175–192. https://doi.org/10.33172/jpbn.v12i2.1542

[51] Zinovieva, E. S. (2022). Cyber Diplomacy under Increased Competition Between the Great Powers. MGIMO Review of International Relations, 17(4), 27–47. https://doi.org/10.24833/2071-8160-2022-olf5

[52] Zinovieva, E., & Shitkov, S. (2023). Sovereignty as Practice in Digital Age. In Digital International Relations (pp. 75–90). https://doi.org/10.1007/978-981-99-3467-6_5

Received on 20-04-2026 Accepted on 03-06-2026 Published on 29-06-2026

https://doi.org/10.65879/3070-5789.2026.02.04