African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Le cyberespace comme vecteur de redéfinition de la puissance : Perspectives marocaines en Afrique"

Cyberspace as a vector for redefining power : Moroccan Perspectives in Africa.

Auteur 1 : SAAID Zahra.

SAAID Zahra, Affiliation institutionnelle : Université Mohammed V, faculté des sciences juridiques, économiques et sociales-Agdal- Rabat- Maroc.
Laboratoire Droit Public et Sciences Politiques.
https://orcid.org/0009-0005-6600-114X

Déclaration de divulgation : L'auteur n'a pas connaissance de quelconque financement qui pourrait affecter l'objectivité de cette étude.

Conflit d'intérêts : L'auteur ne signale aucun conflit d'intérêts.

Pour citer cet article : SAAID Zahra (2025). « Le cyberespace comme vecteur de redéfinition de la puissance : Perspectives marocaines en Afrique », African Scientific Journal « Volume 03, Num 33 » pp: 0397 – 0420.

DOI : 10.5281/zenodo.17780921

AFRICAN SCIENTIFIC JOURNAL
MANAGEMENT AND ECONOMIC DEVELOPMENT

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Résumé

Un nouvel espace de projection de puissance, de rivalité et de coopération émerge : Le cyberespace.

Son intégration dans les relations internationales soulève des enjeux géopolitiques et théoriques majeurs. Dans cet article, nous présenterons une analyse croisée de ce nouveau champ de bataille, à travers les principales théories des relations internationales, à savoir le réalisme, le libéralisme et le constructivisme, tout en révélant comment ce dernier contribue à redéfinir l'équilibre des forces sur la scène mondiale, en adoptant une approche analytique et qualitative, fondée sur une méthode documentaire et une recherche théorique, cette méthodologie permet de croiser le cadre théorique avec la réalité empirique.

Nous nous intéressons également à une dimension géopolitique qui met en évidence l'émergence de la diplomatie numérique comme levier d'influence. À titre d'illustration, le cas du Maroc est mobilisé comme nouvelle puissance émergente dans ce domaine sur le continent africain. À travers cet article, nous espérons démontrer la manière dont la diplomatie marocaine mobilise le cyberespace comme levier de puissance émergent, ainsi que la place de l'Afrique dans les recompositions engendrées par les transformations profondes de la sécurité internationale.

Mots clés :

Cyberespace, Cybersécurité, Théories des relations internationales, Théorie des gains relatifs.

Abstract

Cyberspace is emerging as a new domain for power projection, rivalry, and cooperation. Its integration into international relations presents significant geopolitical and theoretical challenges. This article offers an intersectional analysis of this new battlefield through the primary theories of international relations: realism, liberalism, and constructivism. It further explores how cyber capabilities have redefined the global balance of power.

Utilizing an analytical and qualitative approach grounded in documentary research and theory, our methodology connects theoretical frameworks with empirical reality. We also examine the geopolitical rise of digital diplomacy as a tool of influence, using Morocco as a case study of an emerging cyber power on the African continent. Ultimately, this article aims to demonstrate how Moroccan diplomacy leverages cyberspace to project power, and to assess Africa's role amidst the geopolitical shifts caused by the deep transformation of international security.

Keywords: Cyberspace, Cybersecurity, International relations theories, Relative gains theory.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

INTRODUCTION

Dans un monde de plus en plus interconnecté où l'interconnexion des réseaux redéfinit les frontières traditionnelles et les rapports de force internationaux. L'émergence du cyberespace a façonné et transformé la politique étrangère. Il constitue désormais un pilier structurant, dessinant des frontières virtuelles où les nations ne se préoccupent plus uniquement des frontières physiques.Par conséquent, les infrastructures numériques sont devenues une priorité et un atout stratégique dont la protection est essentielle pour préserver la stabilité économique, les relations diplomatiques et la sécurité nationale. Considérer le cyberespace comme un élément *sine qua non* de la politique nationale et internationale d'un État n'est plus un choix, mais un impératif

Le Maroc, puissance régionale émergente et acteur incontournable sur la scène internationale, a reconnu l'importance stratégique de l'intégration du cyberespace dans ses politiques de défense, économiques et diplomatiques. Face à la réalité des dangers que peut générer le numérique et à la montée des cybermenaces, que ce soit sur ses infrastructures vitales ou sur la perception du Maroc comme un État stable, souverain et émergent, le Royaume a adopté une Stratégie nationale de cybersécurité visant à protéger ses infrastructures critiques, à assurer sa souveraineté numérique et à renforcer son positionnement géopolitique en Afrique et au-delà.

Envisagé à travers le prisme des relations internationales, le cyberespace a un rôle croissant comme instrument de puissance et de compétition stratégique. C'est dans cette optique que l'on peut s'interroger sur la mobilisation numérique réalisée par le Maroc afin de consolider et affirmer son rôle sur la scène africaine et internationale. Le sujet examiné est celui du cyberespace comme un levier de recomposition des formes de puissance et de reconfiguration des rapports de force, au prisme de l'engagement marocain sur le continent.

L'ambition centrale de cette contribution est de mettre en lumière en quoi l'intégration du cyberespace et de la cybersécurité dans les politiques de défense, économiques et diplomatique du Royaume favorise la consolidation de sa souveraineté numérique et à renforcer son ancrage géopolitique en Afrique sur la scène internationale. Plus spécifiquement, il s'agit d'analyser comment le Maroc mobilise le numérique pour affirmer son statut de puissance émergente, tout en faisant face aux vulnérabilités liées aux interdépendances technologiques.

méthodologiquement, cet article adopte une approche qualitative de type étude de cas, focalisée sur le Royaume du Maroc en tant qu'acteur émergent du cyberespace africain. Un tel choix s'explique par le constat que les politiques africaines du numérique demeurent difficilement quantifiables et en grande partie en devenir, qui se prêtent davantage à une analyse approfondie des discours, des dispositifs juridiques et des stratégies étatiques qu'à un traitement statistique.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

D'un point de vue épistémologique, l'étude se place dans une posture à la fois analytique et compréhensive, soucieuse des représentations, des narrations de la puissance et des usages politiques du cyberespace. Le raisonnement mobilise à la fois une démarche inductive et déductive : il s'agit de partir des pratiques et instruments concrets de la politique numérique marocaine pour les mettre en dialogue avec les principaux cadres théoriques des relations internationales et de la cyber-géopolitique.

Cet article se propose d'analyser cette problématique centrale en explorant trois dimensions fondamentales : la lecture du cyberespace à travers le prisme des relations internationales, les perspectives de la stratégie numérique marocaine, et l'importance cruciale de la sécurisation des infrastructures vitales dans la consolidation de la cyber-souveraineté. Chaque dimension vise à éclairer la manière dont le cyberespace reconfigure les rapports de force, contribue au renforcement de la compétitivité technologique des États et, surtout, comment le cyberespace devient un vecteur d'affirmation géopolitique pour le Maroc.

Partant de là, la structure de l'article repose sur trois séquences complémentaires. Le premier temps consiste en une relecture du cyberespace au prisme des principales théories des relations internationales, afin de rendre compte des transformations des rapports de puissance dans cet espace immatériel. Le second temps est centré sur la dimension cyber géopolitique et à la contribution de la cybersécurité à la redéfinition du pouvoir étatique. Le troisième temps examine le cas marocain, en analysant la stratégie numérique et de cybersécurité du Royaume, les cybermenaces qui le visent et les réponses stratégiques mises en œuvre dans son environnement africain.

Penser le cyberespace à travers une lecture croisée des enjeux contemporains

Dans un monde en mutation rapide et parfois chaotique, le numérique et le cyberespace ont transformé les relations internationales. Nous assistons à une redistribution des cartes, où les rapports de force prennent de nouvelles formes, où les États sont contraints de s'adapter à un monde en constante évolution. Joseph Nye confirme que « *Cyberspace will not replace geographical space and will not abolish state sovereignty, but like the town markets in feudal times, it will coexist with them and greatly complicate what it means to be a sovereign state or a powerful country.* »[1]. Par ce passage Joseph Nye (2004) affirme que l'existence d'un nouvel espace ne signifie pas la suppression de l'ordre Westphalien,dont le socle est la souveraineté territoriale, mais introduire plutôt un espace où le pouvoir ne se limite plus aux seuls États ni à la géographie, il redessine la définition de puissance dans le monde contemporain. Les grandes

[1] **Joseph Nye** (2004). *Power in the Global Information Age: From Realism to Globalization*. Routledge. p (88)

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

théories des relations internationales ont été supplantées au cours du XXe siècle par des reformulations critiques et des idées novatrices, rendant difficile leur transposabilité au cyberespace du XXIe siècle. Dans les lignes qui suivent, nous illustrerons brièvement trois perspectives distinctes sur ces grandes théories des relations internationales.

1.1. Une relecture des grandes théories à l'ère numérique

Dans le domaine des relations internationales, le réalisme a constitué un cadre théorique majeur. Il postule que les États sont les acteurs principaux, agissant en tant qu'entités souveraines au sein d'un système international anarchique, dépourvu d'autorité centralisée. Dans ce cadre, ils agissent rationnellement pour maximiser leurs intérêts, en quête de puissance et de sécurité. En ce sens, Hans J. Morgenthau (1948) soutient que les États sont motivés par la quête de puissance dans un système international anarchique[2].

À l'issue de la Seconde Guerre mondiale le réalisme a constitué une doctrine centrale, qui accorde la primauté aux intérêts nationaux et aux rapports de force où dominent les enjeux de puissance, de richesse et de sécurité, constituant ainsi une grille de lecture qui apparaît partiellement inadaptée au contexte du cyberespace et aux dynamiques propres à ce dernier, de la cybersécurité aux conflits potentiels. En effet, de par sa nature l'accès au cyberespace est par essence déterritorialisé[3]. Dans ce contexte, les relations internationales peinent encore à cerner clairement ce que recouvre la cybersécurité, de même que la portée du concept «force» dans le cyberespace. Suivant cette logique, dans un monde en constante mutation, l'ordre mondial est en recomposition, marqué par des tensions géopolitiques et des rivalités de puissance sans fin et une militarisation progressive du cyberespace constituant un vecteur central de confrontation et un nouveau champ d'affrontement stratégique[4], à l'instar de l'air et de l'espace extra-atmosphérique dans lesquels les États renforcent leurs propres dispositifs de sécurité s'efforcent de restreindre les capacités défensives ou offensives de leurs adversaires.

Dans « Countdown to Zero Day », (Kim Zetter, 2014), affirme que l'attaque du virus Stuxnet marque un tournant historique, un moment charnière dans l'histoire des relations internationales contemporaines, en exploitant un logiciel malveillant conçu pour causer des dommages

[2] **Morgenthau, Hans J.** (1948). *Politics Among Nations: The Struggle for Power and Peace*. New York: Alfred A. Knopf.

[3] **Choucri, Nazli** (2012), *Cyberpolitics in International Relations*. MIT Press.p 14

[4] The 2001 Department of Defense Quadrennial Defense Review Report listed four "Key Military–Technical Trends." The third was "Emergence of new arenas of military competition. (p.7)

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

physiques réels, ciblant les centrifugeuses nucléaires iraniennes[5]. Cette opération attribuée aux États-Unis et à Israël, illustre comment la technologie numérique peut être utilisée comme arme de guerre asymétrique pour affaiblir un rival. En outre, elle prouve que le cyberespace peut être utilisé pour atteindre des objectifs géopolitiques sans franchir le seuil d'une guerre ouverte.

Il ressort de cette analyse que la sécurisation et le contrôle des infrastructures numériques constituent un élément essentiel du pouvoir étatique. Dans une perspective réaliste, le cyberespace devient le prolongement du territoire stratégique où la cyber souveraineté se traduit par la capacité d'un État à protéger ses infrastructures numériques, à limiter sa dépendance technologique vis-à-vis des acteurs étrangers et à sécuriser ses données. Cette logique s'est manifestée clairement dans les stratégies étatiques de cybersouveraineté qui se traduisent par l'interdiction ou l'exclusion d'entreprises étrangères dans des secteurs stratégiques, comme les restrictions imposées par les États-Unis à Huawei[6], illustrant ainsi une volonté de préserver l'autonomie technologique nationale face aux États concurrents.

À rebours de la lecture conflictuelle et anarchique des relations internationales propre au réalisme, la seconde perspective est le libéralisme[7] (Choucri NAZLI, 2012), une logique étatique de régulation des interactions politiques, davantage axée sur la coordination, la coopération et les mécanismes visant à normaliser le comportement international des États, par le biais de mécanismes formels et informels. Ainsi, chaque État reconnaît qu'une coordination durable exige une convergence de normes qui ne peut être obtenue qu'en institutionnalisant les exigences de gestion des interactions dans le cyberespace.

Nous faisons ici référence à l'institutionnalisme, une tradition issue des prémices du libéralisme, qui se focalise sur la mise en place de mécanismes formels et informels destinés à routiniser le comportement international des États, tout en s'appuyant sur la coordination et la collaboration. Bien qu'animés par leurs intérêts nationaux, les États peuvent coopérer dans le cyber domaine à condition de s'accorder en amont sur un ensemble de règles partagées. Ainsi, cette approche peut paraître idéaliste mais la réalité témoigne d'une interdépendance complexe et croissante entre les acteurs étatiques, créant ainsi une incitation à la coopération car les vulnérabilités sont souvent partagées. Ce concept d'interdépendance complexe est développé par Keohane et Nye

[5] Zetter, Kim (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing Group.

[6] *The Hacked World Order* d'Adam Segal (2016), p 140-141

[7] *Choucri, N. (2012). Cyberpolitics in international relations. MIT press.*

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

dans *Power and Interdependance* (1977), précisant que les États sont liés par plusieurs canaux — sociaux, technologiques et économiques — et que la force militaire n'est plus le seul moyen d'influence[8].

Dans ce sens, Keohane insiste dans son ouvrage *After Hegemony* (1984)[9] sur le fait que les institutions internationales ont un rôle clé dans la réduction des incertitudes, et ce, même en l'absence d'une puissance hégémonique bienveillante qui surveille le respect des normes et des exigences de la transparence ; Keohane défend également la rationalité des États dans la coopération au sein des institutions, non pas par esprit idéaliste, mais plutôt par un intérêt bien compris, voire pragmatique.

À cet égard, afin d'assurer une gestion collective du cyberespace et d'éviter qu'il ne devienne un terrain de conflit entre États, l'ONU a proposé un Pacte numérique mondial, proposé dans le rapport « Notre Programme commun »[10]. Le pacte appelle à une utilisation éthique et équitable des technologies, afin que l'intelligence artificielle profite à toute l'humanité et non à une poignée de nations ou d'acteurs privés[11], garantissant ainsi une continuité de l'approche institutionnelle libérale. Cet accord encourage les collaborations visant à renforcer les capacités technologiques des pays en développement.

Par ailleurs, le pacte met l'accent sur la coopération entre États en veillant à réduire les asymétries de pouvoir, à renforcer la coopération technique, et à encourager l'investissement dans les infrastructures numériques dans les pays en développement. Ce volet s'inscrit pleinement dans une logique de justice distributive globale, défendue par *la théorie des capabilités* développée par Amartya Sen[12]. Cette théorie justifie une forme de redistribution internationale basée sur l'expansion des libertés réelles. De ce fait, si les pays en développement sont inclus dans la gouvernance numérique, cela participe à la réalisation d'une justice mondiale.

---

[8] Robert O. Keohane et Joseph S. Nye, Power and Interdependence: World Politics in Transition, Boston, Little, Brown and Company, 1977, pp. 24–25.

[9] Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy*, Princeton, Princeton University Press, 1984, p. 67.

[10] Nations Unies, Le Pacte numérique mondial proposé vise à tracer les grandes lignes de la coopération numérique pour un avenir inclusif et sûr, https://www.un.org/fr/summit-of-the-future/global-digital-compact (consulté le 23 juillet 2025).

[11] United Nations. (2024). *Global Digital Compact: Zero Draft*. Office of the Secretary-General's Envoy on Technology

[12] Amartya Sen, *Development as Freedom*, Oxford University Press, 1999.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

La coopération internationale dans le cyberespace constitue le socle d'un environnement numérique sûr, pacifique et stable, assurant ainsi la préservation d'un intérêt commun, à savoir la sécurité du cyberespace. Dans cette perspective, la stabilité de ce dernier est un bien public mondial, et l'adoption de la Convention de Budapest sur la cybercriminalité en *2001*[13]marque un tournant majeur dans sa préservation, en constituant le premier traité international en son genre qui vise à contribuer à la lutte contre les crimes qui ne peuvent être commis qu'au moyen de technologies,en s'appuyant sur l'harmonisation des législations nationales favorisant ainsi la coopération judiciaire et policière, afin d'avoir un cadre procédural coopératif essentiel pour la répression et la prévention des actes malveillants. Ce dispositif est la pierre angulaire d'un ordre cybernétique fondé sur le droit.

Assurer un cadre normatif multilatéral applicable au cyberespace constitue une avancée majeure dans la concrétisation d'une stabilité stratégique et juridique des relations internationale, ce qui est intimement lié à l'ancrage national des normes internationales, telles que consacrées par le droit coutumier et codifiés par l'article 2§7 de la Charte des Nations Unies. Ce dont attestent également les résolutions de l'Assemblée générale des Nations Unies ou les rapports du Groupe d'experts gouvernementaux (GGE), qui n'acquièrent pas de portée opérationnelle que si les États traduisent ces engagements dans leurs ordres juridiques internes. Cette affirmation se trouve confirmée par un ouvrage de Cybil Portal (2021) «Putting Cyber Norms in Practice[14]», qui porte sur les orientations et les exemples pratiques de mise en œuvre des normes volontaires du GGE au niveau interne des États.

Dans ce contexte, le Maroc représente un cas d'appropriation nationale des enjeux du cyberespace, et amorce la mise en place d'une stratégie numérique souveraine axée sur la cybersécurité et la transformation technologique. La première est placée dans les mains de la Direction générale de la Sécurité des Systemes d'Informations (DGSSI), tandis que la seconde se traduit par un espace de dialogue sud-sud et nord-sud sur les enjeux numériques, couronné par l'organisation de GITEX Africa. Le cas marocain illustre ainsi l'alignement des pratiques internes avec les principes globaux, ce qui renforce sa légitimité normative et aide à produire des effets tangibles dans la gouvernance du cyberespace. Toutefois, un rapport d'INTERPOL

[13] Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. ETS No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[14] Cybil Portal, *Putting Cyber Norms in Practice: Possible Ways to Implement the UN GGE Norms and Capacities Required*, 2021, p. 5. Disponible en ligne : https://cybilportal.org/wp-content/uploads/2021/11/Putting-Cyber-Norms-in-Practice.pdf (consulté le 23 juillet).

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

(2023) sur les cybermenaces en Afrique[15] souligne la croissance exponentielle des cyberattaques ciblant le secteur bancaire national. Dès lors, la prise de conscience par le Maroc de la nécessité d'une approche coopérative trouve sa résonance particulière dans la création du GITEX AFRICA à Marrakech en 2024, traduisant ainsi une volonté de consolider sa propre résilience et de faire du Maroc un pont numérique entre l'Afrique, l 'Europe et l'Asie.

Cependant, l'ensemble des dynamiques de coopération dans le cyberespace en termes d'intérêts rationnels et de régulation institutionnelle -telles que défendues par l'approche libérale-, ne suffit pas à saisir pleinement les dimensions qui influencent le comportement des États, que ce soit au niveau identitaire, normatif ou symbolique. Il serait judicieux d'inviter une troisième perspective théorique qui écarte les deux lectures matérialistes précédentes, afin de poser les jalons pour une structuration de la politique internationale fondée sur les représentations intersubjectives et les valeurs partagées. Nous faisons ici référence au constructivisme, selon lequel les actions des États ne sont pas simplement motivées par la quête de puissance matérielle, mais par la manière dont ils souhaitent être perçus et intégrés à l'ordre international. C'est précisément ce qu'illustre Alexander Wendt dans un passage de Social Theory of International Politics[16] (1999) où il affirme que : *«c'est à travers des normes et des interactions partagées que se construisent les identités et les intérêts des États ; ce sont les représentations intersubjectives qui comptent».*

Le cyberespace est un terrain particulièrement fécond pour l'application de l'approche constructiviste, au point de le considérer comme une construction sociale, façonnée par des interactions et des normes, comme le souligne Auffret (2016), qui décrit le cyberespace comme un catalyseur d'anarchie non pas tant par l'absence d'autorité centrale que par l'absence de consensus. Aujourd'hui, la gouvernance du cyberespace est structurée par une pluralité de conceptions idéologiques. Trois grandes visions concurrentes s'en détachent : La première incarne une voie médiane entre la protection des droits fondamentaux et la sécurité des données, la seconde prône une logique et un marché multipartite, tandis que la dernière se focalise sur le contrôle étatique et la cybersouveraineté absolue.

Dans ce paysage, la position européenne veille à garantir la durabilité d'un Internet ouvert par l'instauration d'une réglementation, tout en assurant un encadrement juridique et une ouverture technologique. Cette conviction est portée par la Commission Européenne, qui proclame un

[15] *INTERPOL. (2023). African Cyberthreat Assessment Report 2022 (p. 31). African Cybercrime Operations Desk*

[16] Alexander Wendt, Social Theory of International Politics, p. 334

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

internet ouvert et surtout régulé[17]. En ce sens, le président Emmanuel Macron (2017) souligne dans son discours : *« Ce que je souhaite pour l'Europe, ce n'est pas simplement de réussir cette transition numérique, mais de construire un cadre équitable pour celle-ci. »*[18].La volonté d'établir un cadre juridique ambitieux traduit la volonté européenne de ne pas subir les risques et les menaces cybernétiques dans une logique géopolitique, mais s'efforce plutôt de proposer une feuille de route pour la bonne gouvernance du cyberespace, tout en garantissant un équilibre triptyque entre responsabilité, souveraineté et innovation.

En contraste avec l'approche européenne, les États-Unis s'inscrivent dans une logique libérale fondée sur un modèle multi-acteurs (multistakeholderism), reflétant ainsi une flexibilité institutionnelle qui confère un rôle pivot aux entreprises privées dans la régulation d'Internet, mais aussi aux milieux académiques et à la société civile sans qu'elle ne soit monopolisée par les seuls acteurs étatiques[19]. C'est dans ce sillage que s'inscrit la domination des GAFAM (Google, Apple, Facebook, Amazon, Microsoft).Claire Landais, ancienne Secrétaire générale de la Défense et de la Sécurité nationale, a affirmé que *« Les nouvelles technologies ont progressivement permis à des acteurs privés de rivaliser avec les États, en assumant des fonctions faisant historiquement et sans conteste jusqu'alors l'objet de monopoles régaliens »*[20].

Cependant, les États-Unis conservent un rôle central et une forte présence grâce à son pouvoir législatif et à son pouvoir judiciaire. Cette position n'implique pas le retrait de l'État au profit du marché. En réalité les GAFAM existent parce qu'un État, source de droit, garantit leur existence – même si leurs intérêts ne sont pas toujours convergents, les intérêts des deux restent intrinsèquement liés– ce qui rappelle une citation célèbre prononcée par le PDG de General Motors, Charles Wilson, lors de sa nomination au poste de secrétaire à la Défense : *« ce qui est*

[17] European Commission. (2020). *Shaping Europe's Digital Future*. Publications Office of the European Union

[18] Macron, E. (2017, 26 septembre). *Initiative pour l'Europe : Discours pour une Europe souveraine, unie, démocratique*. Élysée. https://www.elysee.fr/emmanuel-macron/2017/09/26/initiative-pour-l-europe-discours-d-emmanuel-macron-pour-une-europe-souveraine-unie-democratique

[19] Musiani, F. (2019). *Gouverner l'Internet : Entre logiques de pouvoir et gouvernance distribuée*. In **M. Badie, D. Vidal & A. Froment (Eds.)**, *Vers une diplomatie des interconnexions ?* (pp. 141–152). HAL-SHS. https://shs.hal.science/halshs-02320725/document

[20] *Le devoir de souveraineté numérique – Tome II : comptes rendus*, rapport d'information n° 19 007-2 de la Commission d'enquête du Sénat sur « Les enjeux de la souveraineté numérique » (2019), consulté le 24 Juillet 2025.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

bon pour General Motors est bon pour les États-Unis et tout ce qui est bon pour les États-Unis est bon pour General Motors »[21].

La logique demeure globalement la même, inchangée en ce qui concerne les GAFAM. Si une certaine autonomie fonctionnelle de ces derniers est observable, les États-Unis disposent encore des leviers nécessaires pour orienter leurs comportements. Ainsi, la loi Cloud Act témoigne de la prétention souveraine que possèdent les États-Unis pour accéder aux données stockées à l'étranger par les GAFAM; cette forme d'extraterritorialité juridique confirme la domination normative de l'État sur ces entreprises, y compris dans leur dimension transfrontalière.

À rebours de cette logique de souveraineté normative dissimulée derrière le discours d'un Internet libre, la Chine incarne une idéologie numérique antagoniste, là où Washington valorise une gouvernance distribuée dans le cyberespace, Pékin revendique un cyberespace strictement contrôlé par l'État, en le considérant comme un prolongement naturel du territoire national et non pas un bien commun mondial. Ce modèle est fondé sur une conception souverainiste, centralisée et sécuritaire. Cette posture s'accompagne d'un droit fondamental consistant en ce que chaque Etat dispose d'un droit de contrôle et de réglementation ainsi qu'une obligation de non-ingérence, de devoir de diligence et de la protection des infrastructures tout en veillant au respect des principes normatifs tels que le respect du droit international, la paix et la coopération[22]. Cette conception s'est institutionnalisée notamment à travers la Cybersecurity Law 2017, la Data Security Law en 2021, qui impose des restrictions strictes aux entreprises opérant en Chine.

Dès lors, il existe une géopolitique plus large des technologies stratégiques, même en présence de visions contrastées et d'idéologies divergentes entre les grandes puissances numériques. En effet, au moment où les États prennent conscience de l'importance du cyberespace dans la reconfiguration des équilibres globaux et de la redéfinition des termes de la dépendance technologique, ils commencent à construire des alliances technologiques autour de chaînes de valeur numériques.

Un exemple frappant est celui d'une alliance réunissant trois États, à savoir l'Inde, l'Australie et le Japon, dont la préoccupation commune est la sécurité des données. À cet égard, ils

[21] *C'est quand le président Eisenhower choisit en 1953 pour secrétaire à la Défense le PDG de la firme automobile, Charles Wilson, que ce dernier répondit aux critiques par la phrase devenue célèbre (bien qu'elle ait été un peu arrangée) : « Ce qui est bon pour General Motors est bon pour les Etats-Unis. »*

[22] *Li Zhang, A Chinese Perspective on Cyber War, International Review of the Red Cross, vol. 94, n°886, été 2012, p. 806.*

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

investissent activement dans le développement d'alternatives à la 5G chinoise[23] (NDTV, 2020), ainsi que dans le projet franco-allemand de Cloud Souverain (Gaia-X) qui vise à créer des standards technico-juridiques communs appliqués aux services de Cloud Computing pour répondre aux besoins en stockage ultra-sécurisé des industriels européens[24].

Dans ce contexte, le Maroc offre un exemple particulièrement révélateur, en tant qu'acteur émergent du continent africain, et illustre bien une volonté stratégique de diversification des alliances, ce qui s'est traduit par son choix de coopérer avec le groupe chinois Huawei pour le déploiement de l'infrastructure 5G[25] nationale. Par cette orientation, le Maroc a choisi une diplomatie numérique pragmatique et multidimensionnelle, et prouve ainsi sa capacité à naviguer entre les pôles d'influence sino-occidentaux.

Dans un contexte de rivalités géopolitiques, l'éveil institutionnel du Maroc à l'importance des choix technologiques dans la projection de son influence ne peut être envisagé indépendamment de la sécurité des systèmes d'information face à l'augmentation des risques systémiques liés à la dépendance technologique.

C'est à ce stade que la cybersécurité s'érige comme un attribut de la souveraineté étatique, au même titre que la composante militaire ou économique. La maîtrise des flux d'informations, la résilience des infrastructures vitales conditionnent désormais l'exercice effectif de l'autorité étatique dans l'espace numérique. Il s'agit à présent de comprendre en quoi la sécurisation des infrastructures numériques permet aux États d'accroître leur positionnement stratégique dans les rapports de force sur l'échiquier international.

2.2. Cybersécurité : vers une redéfinition du pouvoir étatique

Après avoir appréhendé le cyberespace à l'aune des paradigmes fondamentaux des relations internationales, il apparaît désormais fondamental d'examiner comment un État peut s'appuyer sur la cybersécurité pour asseoir sa souveraineté et affirmer sa position sur la scène

[23] NDTV. (2020, October 7). *India, Japan finalise pact for cooperation in 5G tech, AI, critical infrastructure*. NDTV. https://www.ndtv.com/india-news/india-japan-finalise-pact-for-cooperation-in-5g-tech-ai-critical-infrastructure-2306798

[24] *Gaia-X, une alternative sérieuse au schéma européen de certification cloud »*, **Usine Digitale**, 23 septembre 2024, cité dans *Gaia-X in the Press (Gaia-X Weekly Press Review 16-23 septembre 2024)*, p. 1 https://www.usine-digitale.fr/article/gaia-x-une-alternative-serieuse-au-schema-europeen-de-certification-cloud.N2218775

[25] Guellaf, S. (2025, mars 15). *5G au Maroc : la concurrence se renforce entre géants technologiques*. Maroc Diplomatique. https://maroc-diplomatique.net/5g-au-maroc-la-concurrence-se-renforce-entre-geants-technologiques/

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

internationale.Comme évoqué précédemment, les États investissent massivement les infrastructures vitales à l'instar du Cloud Computing, de la 5G et de l'Intelligence Artificielle afin de consolider leur économie et leur leadership stratégique.

La transformation numérique des services publics (e-administration) et la digitalisation de l'économie permettent aux États d'accroître encore leur attractivité et de créer de nouvelles dépendances technologiques. Toutefois, ces interdépendances technologiques génèrent de nouvelles vulnérabilités pour les États, qui se retrouvent de plus en plus dépendants des architectures numériques globales et exposés aux tensions géopolitiques liées aux chaînes d'approvisionnement (guerre des semi-conducteurs, souveraineté des données) et surtout aux cyberattaques, aux stratégies d'influence déployées par les grandes entreprises technologiques (GAFAM, Huawei, etc.).

C'est au regard de ces dynamiques que se comprend le prolongement stratégique de l'initiative chinoise «Belt and road», qui se traduit par un investissement massif dans les infrastructures de télécommunication (5G, fibre optique et centre de données) afin de connecter les pays partenaires et promouvoir les standards technologiques chinois. Cette stratégie n'est pas une simple entreprise économique mais plutôt un instrument de projection d'influence qui cherche à façonner les écosystèmes numériques en proposant un modèle moins exigeant en matière de protection des données et de gouvernance démocratique, que le modèle occidental[26].

En tissant un réseau dense d'interconnexions numériques, la chine a investi massivement entre 2015 et 2021 dans le financement de projets numériques dans 80 pays. D'ailleurs, Huawei pilote plusieurs projets sur le continent africain et a construit 70 % des infrastructures 4G, surpassant ainsi ses concurrents européens en Afrique. Il investit également dans les villes intelligentes pour mettre en œuvre des solutions de surveillance intelligentes basées sur les technologies chinoises. À travers cette initiative, la Chine pourrait augmenter la dépendance technologique des États partenaires et se conférer une capacité de surveillance et de pression politique, donnant naissance, donnant ainsi naissance à une reconfiguration des équilibres de pouvoir internationaux[27].

Nous assistons aujourd'hui, à une extension de l'influence géopolitique de la Chine, qui se matérialise par des investissements dans les infrastructures numériques en Afrique, donnant

[26] Segal, A. (2020). *The Weaponization of the Internet: How China Exports Digital Authoritarianism*, Council on Foreign Relations.

[27] Jonathan E. Hillman, *Competing with China's Digital Silk Road*, Commentary, Center for Strategic and International Studies (CSIS), 8 avril 2021, disponible en ligne : https://www.csis.org/analysis/competing-chinas-digital-silk-road(consulté le 24 Juillet 2025)

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

naissance au projet de « route de la soie numérique ». Huawei pilote plusieurs projets sur le continent africain et a construit 70 % des infrastructures 4G, surpassant ainsi ses concurrents européens en Afrique. L'entreprise investit également dans les villes intelligentes pour mettre en œuvre des solutions de surveillance avancées basées sur les technologies chinoises.

La Chine a su affermir sa présence géopolitique en Afrique via la dynamique de la route de la soie numérique comme le soulignent Chander et Sun dans "*Data sovereignty: From the Digital silk road to the return of the state".* La Chine a créé une dépendance technologique et juridique en finançant des projets numériques stratégiques[28], comme le *Diamniadio National Data Center* au Sénégal, ayant pour finalité la sécurisation de la souveraineté numérique nationale, soutenu financièrement par un prêt accordé par la China Export-import bank, techniquement confié à Huawei.Ainsi, ce projet consolide la totalité des données gouvernementales sénégalaises à l'étranger. Or, cette externalisation des données soulève une préoccupation majeure et pose la question de la réversibilité juridique et technologique dans l'exercice de la souveraineté numérique,laquelle s'exerce alors de manière fragmentée, ce qui aboutit à une souveraineté nominale, factuellement réduite par l'interdépendance technologique.

Cependant, cette dynamique illustre un phénomène plus large : le retour de la souveraineté étatique dans la gouvernance du cyberespace. Aujourd'hui, nous assistons à un nouvel ordre international où les rapports de force se mesurent à travers les données, les algorithmes et les flux informationnels. « Le piège de Thucydide» , tel que théorisé par Graham ALLISON, transposé au champ numérique non pas dans son acception guerrière classique mais comme une compétition entre les grandes puissances qui cherchent à étendre leur influence en créant une forme de dépendance technologique, dans un contexte où le contrôle effectif des données constitue désormais l'atout maître.

Cette réalité appelle à repenser la maîtrise des capacités cyber, dans un contexte de transformation de la conflictualité contemporaine, où le cyberespace devient à la fois le champ de bataille, la cible du conflit et l'arme de guerre. Au croisement du cyberespace et des rapports de force traditionnels une nouvelle forme de conflictualité s'installe : le conflit hybride qui estompe ainsi la frontière entre la guerre et la paix. Une cyberattaque peut être orchestrée parallèlement ou en amont d'opérations militaires conventionnelles.

En février 2022, avant l'invasion militaire russe de l'Ukraine, une série de cyberattaques et de campagnes de désinformation ont ciblé des banques et des réseaux de communication afin de

[28] Anupam Chander & Haochen Sun (dir.), *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford University Press, 2023.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

limiter la circulation d'informations entre les responsables militaires et gouvernementaux, et de paralyser le système de transactions financières. Les cyberattaques permettent à un État comme la Russie de déstabiliser son adversaire en amont, de perturber ses infrastructures vitales et d'influencer l'opinion publique.

Smeets, M. (21 juin 2022) Des chercheurs de l'Organisation du Traité de l'Atlantique Nord (OTAN) ont même soutenu pendant la guerre que « *Russian cyberattacks on government and military command and control centers, logistics, emergency services . . . were entirely consistent with a so-called thunder run strategy intended to stoke chaos, confusion, and uncertainty, and ultimately avoid a costly and protracted war in Ukraine* »[29].

Ce conflit russo-ukrainien marque un tournant géopolitique majeur, porté par le numérique, et fait émerger un impératif stratégique de souveraineté numérique et redéfinit l'architecture des rapports de force entre États. Cette dynamique nous incite à examiner de près l'émergence d'un champ de bataille invisible où les cyberattaques sont au cœur de la stratégie militaire. Compte tenu de ces paramètres, la maîtrise des infrastructures informationnelles et numériques est désormais inéluctablement une condition sine qua non pour la projection de la puissance et à la préservation de son autonomie.

2. Cyber-géopolitique : une lecture croisée des gains relatifs et des avantages comparatifs

Le cyberespace en tant que nouveau front géopolitique exige une relecture des concepts fondamentaux de cette discipline. Conçu comme un terrain de rivalité constitué d'un ensemble de points névralgiques localisés câbles (sous-marins, satellites, data centers) dans lequel s'affrontent les modèles antagonistes de gouvernance, il devient un espace où la notion même du territoire s'en trouve redéfinie: celle-ci, traditionnellement ancré dans le contrôle physique, englobe désormais la gestion de l'architecture numérique (Clouds souverains, OS), devenue elle aussi marqueur de souveraineté.

Selon une lecture structurelle du cyberespace en tant qu'espace géopolitique qui tend à réintroduire la territorialité dans un espace pensé comme déterritorialisé structuré par des rapports de force, de souveraineté sur les données et des normes techniques, nous assistons à de nouveaux équilibres et déséquilibres qui découlent de la volonté des États n'évaluent pas leur sécurité ou leur richesse uniquement en termes de gains absolus mais en fonction de ce que gagne ou perd l'autre ; qu'ils soient technologiques, économiques ou militaires, ils évaluent

[29] Smeets, M. (2022, June 21). *Cyber operations during the Russo-Ukrainian war*. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

également systématiquement leurs gains par rapport à ceux de leurs rivaux. Appliqués au cyberespace, les États ne cherchent pas seulement à développer leurs capacités numériques, mais surtout à s'assurer que leur adversaire n'obtienne pas un avantage. En ce sens, Grieco propose une « fonction qui illustre cette compréhension réaliste de l'utilité de l'État : U = V - k (W - V), où k représente le coefficient de sensibilité de l'État aux écarts de gains, qu'ils soient à son avantage ou à son désavantage »[30].

Pour en saisir toute la portée, le cyberespace devrait être examiné sous l'angle de la théorie des gains relatifs, notamment à travers une analyse de la politique économique numérique et de l'influence économique. Cette logique se manifeste clairement dans la méfiance croissante à l'égard des dépendances technologiques, comme en témoigne le rejet des équipements Huawei dans plusieurs pays occidentaux. Les États-Unis ont activement cherché à ralentir l'expansion de Huawei en faisant pression sur leurs alliés et en interdisant son utilisation sur leur territoire, puisque la Chine a pris une avance stratégique dans le déploiement de la 5G[31]. L'objectif des États-Unis n'était pas seulement d'avoir une 5G compétitive, mais plutôt d'empêcher la Chine d'acquérir une position dominante. La logique des gains relatifs réside dans le fait qu'il ne s'agit pas seulement de développer ses propres infrastructures, mais aussi de freiner le contrôle des réseaux stratégiques par l'adversaire.

À la lumière de cette théorie, nous reconnaissons que les cyberattaques ne sont pas seulement des outils défensifs, mais aussi des outils de rééquilibrage des pouvoirs. Ce constat trouve une illustration probante dans le cas de l'invasion russe de la Géorgie en 2008 : à l'époque, la Russie a eu recours à des attaques par déni de service distribué (DDoS) pour perturber les sites web du gouvernement et des médias, créant ainsi un climat de désinformation et bloquant les communications de la Géorgie avec le reste du monde. Cela a plongé la Géorgie dans le chaos et l'incohérence ; cette situation est communément appelée le « brouillard de la guerre », une expression empruntée à la célèbre métaphore forgée par le général prussien Carl von Clausewitz[32].

[30] ibid.p. 499.

[31] Council on Foreign Relations. (2023). *Is China's Huawei a Threat to U.S. National Security?* https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security

[32] Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War", International Security, Vol. 17, No. 3 (Winter, 1992-1993), 76-77.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

2.1. Cyber-souveraineté et théorie des avantages comparatifs

Adapter le concept de cyber souveraineté à la théorie des avantages comparatifs nécessite une transposition critique d'un cadre purement économique à un cadre stratégique de gouvernance numérique dans la cybersphère.

Dans la théorie des gains comparatifs développée par David Ricardo, celui-ci explique comment et pourquoi les pays ont intérêt à se spécialiser dans la production de biens et de services – même s'ils ne sont pas les plus productifs en termes absolus – dans lesquels ils sont relativement plus efficaces par rapport aux autres États.

Cependant, le socle de cette théorie repose sur la spécialisation relative. Elle implique qu'un État devrait puiser son efficacité dans les domaines où son rendement est le plus élevé , même s'il n'est pas le plus performant de manière absolue, il peut capitaliser sur des domaines où il a une maîtrise sectorielle. Si l'on souhaite transposer cette perspective à la cybersouveraineté, on peut considérer que l'État X n'a pas besoin de connaissances technologiques de haut niveau ni d'expertise approfondie dans le domaine, il peut simplement développer les segments où il démontre une maîtrise, comme l'éducation numérique par exemple. Un pays comme l'Estonie constitue un exemple éclairant pour cette approche, étant un pays qui développe des infrastructures de cybersécurité mais ne produit pas de matériel informatique. Il a su se positionner dans le domaine de la gouvernance numérique grâce à une maîtrise relativement forte de la cybersécurité, en assurant le vote en ligne sécurisé, ainsi que l'identité numérique universelle, grâce à ses choix stratégiques, l'Estonie a réussi à asseoir sa visibilité géopolitique.

La théorie des gains relatifs portée par Joseph Grieco dans *Anarchy and the limits of cooperation*[33], basée sur une approche réaliste des interactions interétatiques, postule que le calcul stratégique de puissance constitue un enjeu central dans l'analyse des dynamiques de l'ordre mondial, où les États cherchent à accroître leur position relative vis-à-vis de leurs rivaux et non pas seulement à maximiser leurs gains absolus. Cette lecture s'avère particulièrement pertinente dans le cyberespace, afin de comprendre les stratégies de domination, de surveillance et de contrôle technologique, d'autant plus que le cyberespace constitue un terrain fertile à l'émergence de nouvelles formes d'hiérarchies.

2.2. La quête de souveraineté stratégique marocaine à l'aune de la théorie des gains relatifs

Conformément à la logique de *Grieco,* la stratégie du Maroc en matière de transformation numérique et de cybersécurité s'inscrit fondamentalement dans une logique de puissance

[33] Joseph Grieco, "Anarchy and the Limits of Cooperation", *International Organization*, 1988.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

relative. Dans un contexte régional marqué par une intensification des rivalités géostratégiques, le Maroc fait face à un dilemme d'interdépendance asymétrique, et il s'efforce de préserver une marge de manœuvre stratégique en ne dépendant pas de puissances étrangères à un niveau qui compromettrait sa souveraineté décisionnelle, en s'appuyant sur des choix stratégiques très pointus tant au niveau de diversification de partenariats (UE, Etats-Unis, Chine), au lieu de s'aligner exclusivement sur un bloc géopolitique, ce qui lui permet de renforcer la résilience numérique propre du Royaume du Maroc en appliquant une stratégie d'équilibre.

Comme l'a mis en lumière le Dr. Bennani dans une tribune parue dans le journal L'Opinion, le Maroc ne doit ni copier l'Europe ni s'aligner sur la Chine et les États-Unis, mais plutôt trouver un équilibre entre ces deux pôles, ce qui constitue l'option optimale, une vision pragmatique et réfléchie[34].

Toutefois, pour éviter une dépendance excessive, le Maroc a lancé plusieurs initiatives visant à créer des centres de données nationaux. Un accord de partenariat, prévoyant l'ouverture prochaine de deux régions Cloud Oracle au Maroc a été signé entre le ministère de la Transition numérique et de la Réforme de l'administration, le ministère de l'Investissement, de la Convergence et de l'Évaluation des politiques publiques, l'Agence marocaine pour le développement des investissements et des exportations (AMDIE) et Oracle, leader mondial des technologies de l'information[35].

La ministre Ghita Mezzour a déclaré : « *Cette expansion stratégique, portée par un hyperscaler comme Oracle, positionne plus que jamais le Maroc comme un acteur incontournable au niveau régional, et permet un développement encore plus dynamique des compétences et des opportunités de croissance*. »[36] Cette déclaration met en avant l'importance de la souveraineté numérique, qui passe par la maîtrise des données, c'est-à-dire que lorsque le Cloud Computing est déployé sur le territoire national, il permet de stocker, de traiter et de sécuriser localement les données publiques et privées, et permet également de réduire la dépendance du Maroc aux

[34] Bennani, A.-E. (2025, 3 février). *Un modèle marocain d'IA est possible : Faut-il suivre l'Europe ou innover comme la Chine et les États-Unis ?* L'Opinion. https://www.lopinion.ma/Un-modele-marocain-d-IA-est-possible-Faut-il-suivre-l-Europe-ou-innover-comme-la-Chine-et-les-Etats-Unis_a63302.html

[35] Oracle. (2024, May 30). *Oracle Plans to Open Two Public Cloud Regions in Morocco*.

https://www.oracle.com/au/news/announcement/oracle-plans-to-open-two-public-cloud-regions-in-morocco-2024-05-30/

[36] Oracle. (2024, May 9). *Oracle Increases Research and Development Investments in Morocco*. https://www.oracle.com/news/announcement/oracle-increases-research-and-development-investments-in-morocco-2024-05-09/

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

infrastructures étrangères basées en Europe et aux États-Unis, ce qui nous oriente vers la souveraineté numérique, où l'État détient le contrôle de ses flux d'informations et de ses données critiques et sensibles.

La déclaration de la ministre soulève également la question de l'influence numérique régionale. Le Maroc ne cherche pas seulement à préserver sa souveraineté en interne, mais vise à la projeter à l'échelle régionale, en renforçant sa capacité d'influence et en devenant un fournisseur régional de solutions technologiques, ce qui lui permettra d'affirmer sa position d'acteur clé dans la reconfiguration des équilibres numériques en Afrique.

Cette montée en puissance dans le domaine du numérique accroît l'exposition du Maroc aux cybermenaces : en effet, plus un État s'affirme comme un acteur technologiquement influent et interconnecté, plus il devient une cible stratégique dans le cyberespace. Dans ce contexte, nous nous concentrerons ci-après sur les cybermenaces et les réponses stratégiques que le Maroc mobilise pour préserver sa sécurité nationale et sa sécurité numérique.

2.3. Le Maroc face aux cybermenaces et les réponses stratégiques mobilisées

Comme l'indique le rapport Baromètre des risques 2025 d'Allianz, le Maroc figure parmi les 23 pays identifiés comme vulnérables aux cyberattaques. Aux côtés du Maroc, on trouve des pays comme les États-Unis, la France, le Nigéria, l'Afrique du Sud, l'Allemagne et l'Inde[37]. Le nombre d'États ciblés par des cyberattaques continue d'augmenter, reflétant une tendance mondiale qui touche non seulement le secteur technologique, mais aussi la sphère économique et un large éventail d'industries, notamment les entreprises technologiques et les institutions financières. Dans ce contexte, la cybersécurité apparaît comme un impératif transversal et stratégique, tant au niveau national qu'au niveau international.

Bien que le Maroc soit très actif dans les événements et initiatives mondiales visant à renforcer la cybersécurité, il n'est pas à l'abri de la vague croissante de cybermenaces. Le Royaume fait partie des rares pays du continent africain à avoir ratifié la Convention de Budapest, une étape cruciale vers l'harmonisation de son cadre juridique national pour lutter contre les formes émergentes de cybercriminalité. Cette ratification renforce également la position du Maroc dans les efforts de coopération internationale en matière de cybersécurité.

Le Maroc a signé le deuxième protocole additionnel à la Convention de Budapest en 2022, dans le cadre d'une conférence internationale sur la coopération renforcée et la divulgation des

[37] Allianz Commercial.(2025,January). Allianz Risk Barometer: Identifying the major business risks for 2025. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

preuves électroniques. Ce protocole, qui vise à compléter ladite Convention, a été signé au Conseil de l'Europe par le ministre de la Justice, Abdellatif Ouahbi. Il a déclaré que: « *le Royaume du Maroc œuvrera à la réalisation de ces objectifs et réaffirme sa pleine volonté de coopérer avec les autres États pour garantir la cybersécurité pour toutes les parties* »[38].

Fidèle à son engagement envers les normes internationales, l'administration marocaine a mis en place un ensemble de mécanismes institutionnels et législatifs. Par l'intermédiaire de la Direction générale de la sécurité des systèmes d'information (DGSSI), elle-même placée sous la tutelle de l'Autorité de défense nationale, une nouvelle feuille de route a récemment été dévoilée. Ce document stratégique reflète la ferme volonté du Royaume de se doter d'un cadre juridique et opérationnel capable de répondre aux menaces croissantes sur ce champ de bataille numérique en pleine évolution.

La stratégie nationale de cybersécurité s'articule autour de plusieurs piliers clés : la protection des infrastructures critiques, la consolidation de la coopération internationale, le renforcement du cadre juridique et réglementaire, ainsi que le renforcement des systèmes d'information nationaux, pour assurer une veille et une détection continues des menaces numériques[39].

Au-delà de l'aspect opérationnel, cette démarche constitue une stratégie qui vise à consolider un cadre juridique cohérent et global pour la sécurité nationale, à travers l'adoption de lois et l'adaptation de mécanismes réglementaires afin de garantir une réponse efficace et une résilience numérique conforme aux engagements internationaux. En ce sens, une avancée majeure dans la construction d'une base juridique en la matière a abouti à la promulgation de la loi n° 05-20 relative à la cybersécurité. Cette loi vient encadrer les obligations des établissements publics, des administrations gérant des infrastructures critiques, mais aussi des opérateurs privés en matière de protection des systèmes d'information (SI).

La loi 05-20 met l'accent sur le signalement des incidents et sur la mise en œuvre de mesures techniques de sécurité, et prévoit également des sanctions en cas de non-respect. Cela s'inscrit dans une logique de conformité aux normes internationales, et permettra de créer un cadre juridique favorable, propice au renforcement de la confiance numérique, constituant ainsi un

[38] Council of Europe. (2022, May 12).Morocco signs the 2nd additional protocol to the Budapest Convention on Cybercrime. https://www.coe.int/fr/web/rabat/-/renforcement-de-la-cooperation-et-de-la-divulgation-de-preuves-electroniques

[39] National Defense Administration. National Information Systems Security Directive (version No. 2-2023) https://www.dgssi.gov.ma/sites/default/files/publications/pdf/2024-07/National_information_security_directive_vf_12012023-3%20in%20french.pdf

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

pilier de la stratégie nationale en la matière[40]. Parallèlement aux efforts de régulation, les Forces Armées Royales ont intégré le cyber domaine dans leur doctrine de défense en reconnaissant cet espace comme un théâtre d'opérations à part entière. À l'occasion du 63e anniversaire de la création des FAR Sa Majesté le Roi Mohammed VI, Que Dieu l'assiste, a adressé une ordonnance aux Forces Armées Royales :

« *Dans le même contexte, Nous avons donné Nos Hautes Instructions pour actualiser les méthodes de formation militaire à ses différents niveaux, les rendre plus harmonieuses et complémentaires, et unifier les programmes et manuels militaires ; (....) Ce programme comprend également le développement des Forces Armées Royales et la modernisation de leurs capacités militaires et de défense et l'amélioration de leur préparation au combat pour les différentes armes afin de faire face aux menaces et dangers actuels et futurs, notamment les menaces terroristes, électroniques et cybernétiques.* »[41]

La stratégie des FAR s'articule autour de deux axes essentiels : premièrement, l'adaptation de la politique de défense face aux nouvelles formes de manœuvres numériques et hybrides; deuxièmement, l'élargissement du champ d'action des FAR pour inclure la cybersécurité comme composante sine qua non de la défense nationale, notamment dans la lutte contre le terrorisme régional, précisément dans la région du Sahel (Niger, Burkina Faso et Mali), foyer du terrorisme djihadiste. Cette approche de défense ne se limite pas à rendre ce corps de défense flexible et réactif, mais vise également à la rendre capable de mieux gérer et répondre aux différentes formes de menaces, et plus encore à préserver la souveraineté du Royaume du Maroc[42].

Comme le souligne Rachid EL HOUDAIGUI (2019) dans *« Les forces armées marocaines face aux mutations géopolitiques »*[43]La défense et la sécurité ne peuvent plus être traitées de manière compartimentée ; elles sont interconnectées, formant un continuum où la coordination entre l'armée et la sécurité nationale (police, gendarmerie) est une obligation et non plus un choix.

[40] NATIONAL DEFENSE ADMINISTRATION.PRESENTATION NOTE RELATING TO LAW NO. 05-20 ON CYBERSECURITY

[41] Message from His Majesty the King Mohamed VI to the Royal Armed Forces, 63rd anniversary of the creation of the FAR: HM the King addresses an order of the day to the Royal Armed Forces

[42] Bernard Le Gorgeu. La stratégie numérique du Maroc: Vers l'émergence d'un hub numérique régional ?. p.31

[43] El Houdaigui, R. (2019). Moroccan Armed Forces in the Face of Geopolitical Mutations. p 42-44.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

CONCLUSION

Cet espace, longtemps marginalisé dans l'analyse géopolitique, est aujourd'hui un nouveau terrain de rivalités. Cette étude démontre que le cyberespace ne peut être appréhendé comme un espace purement technique ou neutre, mais plutôt comme un vecteur de compétition entre États, au sein duquel se jouent des enjeux de souveraineté. L'analyse du cyberespace à travers les théories des relations internationales, combinée à une étude géopolitique mettant en évidence l'influence accrue de la technologie, met en lumière une dynamique stratégique multidimensionnelle. Le cas du Maroc, avec son positionnement numérique, illustre clairement comment le numérique devient un levier d'influence.

La posture coopérative adoptée par le Maroc, fondée sur le partage de son expertise numérique et l'exportation de son modèle réglementaire, reflète une logique de puissance relative. Cette logique lui permet d'étendre sa présence et sa maîtrise du cyberespace africain, où le numérique devient un levier d'influence.

Une compétition silencieuse autour de la gouvernance du cyberespace africain se déroule, révélant un conflit d'intérêts sous-jacent qui se traduit par une coopération surchargée de logiques de rivalité. Ce conflit s'exprime par des affrontements indirects et un jeu de pouvoir autour de l'influence technologique, infrastructurelle et normative, où chaque État tente de sécuriser des positions géostratégiques, d'imposer ses normes et de s'approprier les dépendances d'un espace en construction.

Des lignes de tension géopolitique se dessinent. Derrière cette montée en puissance numérique, le cyberespace africain devient le théâtre d'un conflit latent entre plusieurs puissances régionales et extra-continentales, où chaque État cherche à imposer sa vision de la gouvernance numérique ainsi que ses propres standards technologiques. Le Maroc, en adoptant une stratégie prudente et ambitieuse, soucieuse de préserver sa souveraineté, se positionne à l'intersection de ces dynamiques afin de dessiner les contours du cyberespace régional.

Cela nous invite à considérer la diplomatie numérique comme un instrument de puissance à part entière, et non comme un simple outil de soutien à la politique étrangère. Dans un monde où les frontières s'estompent et deviennent de plus en plus virtuelles, le cyberespace représente un théâtre géopolitique où se dessinent les équilibres de demain.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

BIBLIOGRAPHIE

SEGAL Adam, 2016, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, New York, PublicAffairs, p. 140-141.

ALLIANZ Commercial, 2025, *Allianz Risk Barometer: Identifying the Major Business Risks for 2025*. Consulté en ligne le 24 juillet 2025, URL : https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf

AXWORTHY Lloyd, 1999, « La nouvelle vocation de sécurité de l'OTAN », *Revue de l'OTAN*, vol. 47, n° 4, hiver, p. 8-11.

BENNANI A.-E., 2025, « Un modèle marocain d'IA est possible : Faut-il suivre l'Europe ou innover comme la Chine et les États-Unis ? », *L'Opinion*, 3 février. Consulté en ligne le 24 juillet 2025, URL : https://www.lopinion.ma/Un-modele-marocain-d-IA-est-possible-Faut-il-suivre-l-Europe-ou-innover-comme-la-Chine-et-les-Etats-Unis_a63302.html

BEYERCHEN Alan, 1992-1993, « Clausewitz, Nonlinearity, and the Unpredictability of War », *International Security*, vol. 17, n° 3, p. 76-77.

CHANDER Anupam et Haochen SUN (dir.), 2023, *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford, Oxford University Press.

CHOUCRI Nazli, 2012, *Cyberpolitics in International Relations*, Cambridge, MIT Press.

CONSEIL DE L'EUROPE, 2001, *Convention on Cybercrime (Budapest Convention)*, ETS n° 185. Consulté en ligne le 23 juillet 2025, URL : https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

CONSEIL DE L'EUROPE, 2022, *Morocco Signs the 2nd Additional Protocol to the Budapest Convention on Cybercrime*, 12 mai. Consulté en ligne le 24 juillet 2025, URL : https://www.coe.int/fr/web/rabat/-/renforcement-de-la-cooperation-et-de-la-divulgation-de-preuves-electroniques

COUNCIL ON FOREIGN RELATIONS, 2023, *Is China's Huawei a Threat to U.S. National Security?* Consulté en ligne le 24 juillet 2025, URL : https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security

EL HOUDAIGUI Rachid, 2019, *Moroccan Armed Forces in the Face of Geopolitical Mutations*, Policy Center for the New South, document électronique.

EUROPEAN COMMISSION, 2020, *Shaping Europe's Digital Future*, Luxembourg, Publications Office of the European Union.

GAIA-X, 2024, « Une alternative sérieuse au schéma européen de certification cloud », *Usine Digitale*, 23 septembre. Cité dans *Gaia-X in the Press (Gaia-X Weekly Press Review 16-23*

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

septembre 2024), p. 1. Consulté en ligne le 24 juillet 2025, URL : https://www.usine-digitale.fr/article/gaia-x-une-alternative-serieuse-au-schema-europeen-de-certification-cloud.N2218775

GRIECO Joseph, 1988, « Anarchy and the Limits of Cooperation », *International Organization*.

GUELLEF Souad, 2025, « 5G au Maroc : la concurrence se renforce entre géants technologiques », *Maroc Diplomatique*, 15 mars. Consulté en ligne le 24 juillet 2025, URL : https://maroc-diplomatique.net/5g-au-maroc-la-concurrence-se-renforce-entre-geants-technologiques/

HILLMAN Jonathan E., 2021, *Competing with China's Digital Silk Road*, Commentary, Center for Strategic and International Studies (CSIS), 8 avril. Consulté en ligne le 24 juillet 2025, URL : https://www.csis.org/analysis/competing-chinas-digital-silk-road

INTERPOL, 2023, *African Cyberthreat Assessment Report 2022*, African Cybercrime Operations Desk, p. 31.

KEOHANE Robert O., 1984, *After Hegemony: Cooperation and Discord in the World Political Economy*, Princeton, Princeton University Press, p. 67.

KEOHANE Robert O. et Joseph S. NYE, 1977, *Power and Interdependence: World Politics in Transition*, Boston, Little, Brown and Company, pp. 24-25.

LE GORGEU Bernard, 2021, *La stratégie numérique du Maroc : vers l'émergence d'un hub numérique régional ?*, Paris, L'Harmattan, coll. « Histoire et perspectives méditerranéennes ». Google Books+1

MACRON Emmanuel, 2017, *Initiative pour l'Europe : Discours pour une Europe souveraine, unie, démocratique*, 26 septembre. Consulté en ligne le 24 juillet 2025, URL : https://www.elysee.fr/emmanuel-macron/2017/09/26/initiative-pour-l-europe-discours-d-emmanuel-macron-pour-une-europe-souveraine-unie-democratique

MORGENTHAU Hans J., 1948, *Politics Among Nations: The Struggle for Power and Peace*, New York, Alfred A. Knopf.

MUSIANI Francesca, 2019, « Gouverner l'Internet : Entre logiques de pouvoir et gouvernance distribuée », dans BADIE M., VIDAL D. et FROMENT A. (dir.), *Vers une diplomatie des interconnexions ?*, Paris, HAL-SHS, p. 141-152.

NATIONAL DEFENSE ADMINISTRATION, 2023, *National Information Systems Security Directive* (version n° 2-2023). Consulté en ligne le 24 juillet 2025, URL : https://www.dgssi.gov.ma/sites/default/files/publications/pdf/2024-07/National_information_security_directive_vf_12012023-3%20in%20french.pdf

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

NDTV, 2020, « India, Japan finalise pact for cooperation in 5G tech, AI, critical infrastructure », *NDTV*, 7 octobre. Consulté en ligne le 24 juillet 2025, URL : https://www.ndtv.com/india-news/india-japan-finalise-pact-for-cooperation-in-5g-tech-ai-critical-infrastructure-2306798

NYE Joseph, 2004, *Power in the Global Information Age: From Realism to Globalization*, Londres, Routledge, p. 88.

ORACLE, 2024, *Oracle Plans to Open Two Public Cloud Regions in Morocco*, communiqué de presse, 30 mai. Consulté en ligne le 24 juillet 2025, URL : https://www.oracle.com

SEN Amartya, 1999, *Development as Freedom*, Oxford, Oxford University Press.

SEGAL Adam, 2020, *The Weaponization of the Internet: How China Exports Digital Authoritarianism*, Council on Foreign Relations.

SMEETS Max, 2022, « Cyber operations during the Russo-Ukrainian war », *CSIS*, 21 juin. Consulté en ligne le 24 juillet 2025, URL : https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

UNITED NATIONS, 2024, *Global Digital Compact: Zero Draft*, Office of the Secretary-General's Envoy on Technology.

UNITED NATIONS, 2025, « Le Pacte numérique mondial proposé vise à tracer les grandes lignes de la coopération numérique pour un avenir inclusif et sûr », *Nations Unies*. Consulté en ligne le 23 juillet 2025, URL : https://www.un.org/fr/summit-of-the-future/global-digital-compact

WENDT Alexander, 1999, *Social Theory of International Politics*, Cambridge, Cambridge University Press, p. 334.

ZHANG Li, 2012, « A Chinese Perspective on Cyber War », *International Review of the Red Cross*, vol. 94, n° 886, été, p. 806.

ZETTER Kim, 2014, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, New York, Crown Publishing Group.

--