Revue Internationale du Chercheur
ISSN: 2726-5889
Volume 6 : Numéro 4

LA DIPLOMATIE ET LA SOUVERAINETE NUMERIQUES: UNE RELATION PARADOXALE AU SERVICE DU MAINTIEN DU LEADERSHIP

DIGITAL DIPLOMACY AND SOVEREIGNTY: A PARADOXICAL RELATIONSHIP IN THE SERVICE OF MAINTAINING LEADERSHIP

LALLA MINA RIFKI

Doctorant en droit public & Sciences politiques

Faculté des Sciences Juridiques, Economiques et Sociales

Université Mohammed V Rabat-Agdal

Laboratoire de Recherche en Droit Public & Sciences Politiques

MAROC

Date de soumission: 15/11/2025

Date d'acceptation : 15/12/2025

Pour citer cet article:

RIFKI. L.M. (2025) «La diplomatie et la souveraineté numériques: une relation paradoxale au service du maintien du leadership», Revue Internationale du chercheur «Volume 6: Numéro 4» pp: 1461-1476

Résumé

L'ère numérique et le progrès fulgurant de l'intelligence artificielle, ont remodelé les bases de la diplomatie classique, prérogative et pouvoir régalien de l'Etat disposant des éléments constitutifs et jouissant de la souveraineté qui a depuis toujours été restreinte à une élite qui l'exerce. Dès lors, la diplomatie numérique s'est transformée en un instrument puissant d'influence employée dans les relations internationales. De même, la souveraineté numérique vise à appliquer directement les caractéristiques traditionnelles de la souveraineté à l'univers numérique est asseoir sa capacité à contrôler et réguler le cyberespace tout en veillant à la gestion des enjeux stratégiques des Etats.
Cette relation paradoxale mène à analyser les dynamiques et complexes qui redessinent les contours de la diplomatie et la souveraineté pour maintenir le leadership sur la scène internationale. Le présent article met en lumière les contours de la diplomatie numérique et la souveraineté numérique et interroge la capacité des Etats à assurer un leadership sur la scène internationale. En fin, il propose une réflexion sur une cette relation paradoxale entre ces deux champs des relations internationales.

Mots clés : Diplomatie numérique ; Souveraineté numérique, cyberespace ; cybersécurité, géants du numérique, GAFAM, gouvernance de l'Internet

Abstract
The digital era and the rapid advancement of artificial intelligence have reshaped the foundations of traditional diplomacy, a prerogative and sovereign power of the state, which possesses the constituent elements and enjoys sovereignty that has historically been restricted to an elite who wield it. Consequently, digital diplomacy has transformed into a powerful instrument of influence employed in international relations. Similarly, digital sovereignty aims to directly apply the traditional characteristics of sovereignty to the digital realm, establishing the capacity to control and regulate cyberspace while ensuring the management of states' strategic interests.
This paradoxical relationship leads us to analyze the dynamics and complexities that are reshaping the contours of diplomacy and sovereignty in order to maintain leadership on the international stage. This article highlights the contours of digital diplomacy and digital sovereignty and examines the capacity of states to assume leadership on the international stage. Finally, it offers a reflection on this paradoxical relationship between these two fields of international relations.

Keywords: Digital diplomacy; Digital sovereignty, cyberspace; cybersecurity, Big tech, GAFAM, Internet governance

INTRODUCTION

L'ère numérique et la progression rapide de l'intelligence artificielle, ont remodelé les bases de la diplomatie classique, prérogative et pouvoir régalien de l'Etat disposant des éléments constitutifs et jouissant de la souveraineté qui a, depuis toujours, été restreinte à une élite qui l'exerce « *La diplomatie est un exercice collectif mais n'y ont accès que ceux qui incarnent ou représentent une souveraineté*» (Robin G, 2000). Ce qui a donné naissance à une nouvelle forme de pratique diplomatique où l'influence et la formulation des décisions diplomatiques se font par le biais des réseaux et plateformes numériques. Cette mutation paradigmatique, caractérisée par l'émergence d'une diplomatie dématérialisée et instantanée, transforme substantiellement les modalités traditionnelles de la négociation internationale (Roumate.F, 2021).

Dès lors, la diplomatie numérique s'est transformée en un instrument puissant d'influence employée dans les relations internationales. De même, la souveraineté numérique vise à appliquer directement les caractéristiques traditionnelles de la souveraineté à l'univers numérique. Cette idée, surtout soutenue par les grandes puissances, se manifeste par le désir d'instaurer des « frontières numériques» qui favorisent un contrôle gouvernemental rigoureux sur les flux d'informations.

Or, dans ce nouveau monde connecté la souveraineté s'étale aussi sur le champ numérique et chaque Etat souverain est poussé à se positionner dans un nouvel univers appelé cyberespace transnational dépassant le territoire national. Le cyberespace peut être traduit par un espace commun à l'instar des mers dont les lignes régulières sont perturbées par des pirates, ce qui pousse souvent des diplomates à estimer que la souveraineté numérique se jouerait dans l'arène d'un droit adapté et inspiré des principes du droit maritime (Thomas G, 2011).

De ce fait, la souveraineté numérique représente une extension, voire même un avatar, de la souveraineté et doit être débattue dans les enceintes internationales et même entre puissances. Par ailleurs, la révolution numérique pose un défi sans précédent aux conceptions traditionnelles de la souveraineté étatique, historiquement définie comme le contrôle exclusif exercé par un État sur un territoire délimité par des frontières physiques, la souveraineté se trouve profondément questionnée par l'émergence d'un cyberespace transnational qui transcende les démarcations géographiques conventionnelles. Face à cette remise en question fondamentale, les États développent des approches diverses pour tenter de préserver leur

autorité souveraine dans l'environnement numérique, donnant naissance au concept émergent de "souveraineté numérique".

Le présent papier est un article conceptuel, fondé sur une analyse de la littérature et des instruments internationaux. Dans ce contexte, une question centrale se pose : en quoi la souveraineté numérique reconfigure-t-elle les pratiques de diplomatie numérique et la capacité des Etats à maintenir leur leadership dans le cyberespace?

Pour comprendre ces dynamiques complexes qui redessinent les contours de la diplomatie et la souveraineté numériques au service du maintien du leadership, le présent article analyse d'abord les défis majeurs que pose l'hégémonie croissante des géants technologiques pour les États traditionnels, révélant les nouvelles formes de dépendance et de vulnérabilité qui en résultent notamment l'hégémonie des géants du numérique qui risquent de contester la souveraineté des Etats (**1**), puis examiner les stratégies développées par les États pour préserver et réaffirmer leur souveraineté numérique, illustrant les différentes conceptions et approches qui émergent face à ce défi commun en soulignant le rôle de la diplomatie numérique dans le maintien de la souveraineté numérique face aux défis de cybersécurité(**2**).

1- Hégémonie des géants du numérique: souveraineté des Etats contestée

L'émergence des GAFAM, ensemble d'acteurs sur la scène internationale, paraissait déjà irréversible ce qui incite à se demander s'ils puissent remettre en cause la souveraineté nationale sans s'exposer à d'éventuelles ripostes vigoureuses est alors incertain. Aujourd'hui, ces considérations font figure de lieux communs, tant la mise en données du monde échappe aux États et tant la puissance des acteurs américains de la Silicon Valley[1] détient le monopole quasi-total: tantôt alliées, tantôt rivales des États, tantôt indifférentes à leurs lois.

A travers un système de porosité unique, les géants du net veillent à ne jamais contester la primauté de l'intérêt national et contribuent même à sa promotion en adoptant le discours du pouvoir individuel (empowerment) via les TIC. Questionner une éventuelle politique étrangère de ces acteurs du numérique revient donc, en creux, à s'interroger sur leur degré de coopération et de compatibilité avec les objectifs internationaux (Kirkpatrick D, 2011).

Les dirigeants des géants du numérique sont néanmoins vus comme des chefs d'État lors de leurs déplacements ou quand ils reçoivent des responsables politiques de premier plan en quête de promesses d'investissements dans leurs pays. En effet, en février 2017, le Danemark

[1] *La Silicon Valley désigne le pôle des industries de pointe situé dans la partie sud de la région de la baie de San Francisco dans l'État de Californie*

annonçait la nomination d'un ambassadeur auprès des géants du numérique, au motif que «ces multinationales sont devenues un type de nouvelles nations, auxquelles [Copenhague] doit se confronter ». Cette initiative crée un rapport d'un nouveau type.

Les GAFAM investissent sur les marchés internationaux dont ils attendent des ressources considérables, lesquelles leur permettent de mieux développer les technologies à fort impact sur le public. Ces multinationales n'exportent pas un produit à partir d'une nation, mais façonnent partout leur propre modèle social parce qu'elles contrôlent l'économie de l'information numérique: en accumulant les données privées et en offrant des services, des connexions et des technologies qui structurent la consommation, elles interviennent directement en lieu et place des États.

Les services proposés par les plateformes numériques se trouvent parfois pris dans des polémiques à portée et aux conséquences diplomatiques: ainsi en est-il de la plateforme Google, qui appose sa propre conception des frontières sur les moteurs de recherche, en particulier dans les cas de territoires disputés (Israël-Palestine, Cachemire, Sahara marocain etc (Brown K, 2016). Ainsi la révolution numérique replace incontestablement le concept de souveraineté au cœur de divers enjeux. Chose qui se développera encore plus avec la convergence de l'économie des données, de la robotique et de l'intelligence artificielle

1.1. La Souveraineté: cadre conceptuel

La souveraineté constitue l'un des piliers fondamentaux de l'ordre international moderne. Ce concept, dont les racines théoriques remontent aux travaux de Jean Bodin au XVIe siècle et au système westphalien[2], désigne traditionnellement l'autorité suprême et exclusive qu'exerce un État sur un territoire déterminé et sur la population qui y réside. Cette conception classique repose sur plusieurs attributs essentiels qui méritent d'être examinés pour comprendre comment la révolution numérique vient les questionner en profondeur.

La dimension territoriale représente historiquement l'élément central de la souveraineté étatique. L'État souverain se définit avant tout par sa capacité à exercer une autorité exclusive à l'intérieur de frontières géographiques clairement délimitées. Cette territorialité de la

[2] Le système westphalien fait référence à l'ordre international établi par les traités de Westphalie en 1648, mettant fin à la guerre de Trente Ans en Europe. Il repose sur la reconnaissance de la souveraineté des Etats avec des frontières bien définies, l'égalité des Etats en Droit International et la non ingérence dans les affaires intérieures des autres Etats.

souveraineté s'est traduite par le développement d'un principe fondamental du droit international: la non-ingérence dans les affaires intérieures d'un État. Pour Stephen Krasner, la souveraineté territoriale signifie que les États ont le droit exclusif de gouverner à l'intérieur de leurs propres frontières, et les autres États ont l'obligation de respecter ce droit (Stephen D, 1999). Cette dimension territoriale, qui semblait aller de soi dans un monde d'interactions physiques, se trouve profondément remise en question par la nature transfrontalière intrinsèque des flux numériques.

Cette souveraineté englobe plusieurs dimensions à savoir politique, économique, informationnelle etc. Au-delà de ces dimensions constitutives, la souveraineté se caractérise également par sa reconnaissance internationale. Comme le soulignait déjà Hegel, la souveraineté n'existe pleinement que lorsqu'elle est reconnue par d'autres entités souveraines. Cette dimension relationnelle a été formalisée dans le système international moderne par des principes comme l'égalité souveraine des États, consacrée par la Charte des Nations Unies.

Or, la révolution numérique introduit une complexité nouvelle dans cette reconnaissance mutuelle, certains États développant des conceptions divergentes de ce que constitue la souveraineté dans l'espace numérique, rendant plus difficile l'émergence d'un consensus international sur ses contours légitimes.

Ces conceptions traditionnelles de la souveraineté se trouvent profondément bousculées par l'émergence de l'espace numérique, caractérisé par son immatérialité, sa transnationalité intrinsèque et la multiplicité des acteurs qui y opèrent. Face à ce défi, plusieurs approches théoriques tentent de redéfinir ce que pourrait être une "souveraineté numérique" adaptée aux réalités contemporaines.

Une première approche, que l'on pourrait qualifier de "souverainiste numérique", cherche à transposer directement les attributs classiques de la souveraineté à l'espace numérique. Cette conception, particulièrement défendue par des pays comme la Russie ou la Chine, se traduit par la volonté d'établir des "frontières numériques" permettant un contrôle étatique strict sur les flux d'information.

Une deuxième approche, plus libérale, reconnaît les limites intrinsèques de la souveraineté traditionnelle dans l'espace numérique mais cherche à préserver ses attributs essentiels par des mécanismes de régulation adaptés.

Une troisième approche, plus radicale, propose de repenser fondamentalement la notion même de souveraineté à l'ère numérique. Des théoriciens comme Milton Mueller suggèrent que l'inadéquation fondamentale entre la logique territoriale de la souveraineté westphalienne et la nature transfrontalière du cyberespace exige l'élaboration de nouveaux concepts politiques. Cette perspective, qualifiée parfois de "constitutionnalisme numérique", propose de remplacer la souveraineté étatique exclusive par des formes de gouvernance multi-niveaux et multi-acteurs plus adaptées aux spécificités du monde numérique.

Comme l'observe Joseph Nye, "*le cyberespace remet en question les fondements mêmes de l'ordre westphalien en créant un domaine d'activité humaine qui transcende naturellement les frontières nationales tout en affectant profondément des intérêts que les États considèrent comme relevant de leur souveraineté traditionnelle*".

Cette analyse des fondements conceptuels de la souveraineté amène naturellement à examiner comment ce principe fondamental de l'ordre international se confronte aux caractéristiques spécifiques du cyberespace, créant des tensions inédites qui exigent une adaptation profonde des conceptions traditionnelles du pouvoir étatique.

1.2. La souveraineté et exigences du cyberespace

La souveraineté numérique est aujourd'hui un vecteur majeur de pouvoir politique et géopolitique. Elle désigne la capacité d'un État à exercer un contrôle légitime sur les données, les infrastructures numériques, les flux d'information, ainsi que sur la régulation des marchés et des contenus en ligne dans son territoire. Cette capacité est un levier essentiel du pouvoir car elle permet à l'État de moduler ou d'interrompre les flux d'information, de protéger ses institutions, de défendre ses intérêts et de renforcer sa sécurité nationale face aux enjeux croissants du numérique.

La maîtrise du numérique est désormais associée à la puissance politique. Par exemple, des États comme la Chine ont développé un modèle de souveraineté numérique fondé sur un contrôle centralisé et une régulation autoritaire, justifiant la surveillance accrue et la régulation stricte des flux numériques pour maintenir l'ordre public et renforcer le pouvoir central. Cette stratégie leur permet d'étendre leur influence à l'échelle internationale, notamment via des initiatives comme la «Digital Silk Road» (De NARDIS L, 2014) qui exporte ce modèle dans plusieurs pays partenaires.

Le cyberespace présente des caractéristiques intrinsèques qui défient les conceptions traditionnelles de la souveraineté étatique. Cet environnement numérique, loin d'être un simple outil technique, constitue un domaine d'activité humaine doté de propriétés spécifiques qui entrent en tension directe avec les fondements territoriaux et juridictionnels de l'ordre westphalien. Ces propriétés structurelles du cyberespace, inhérentes à son architecture même, créent un cadre contraignant auquel les conceptions souverainistes doivent nécessairement s'adapter.

La dématérialisation constitue une autre caractéristique déterminante du cyberespace qui transforme les conditions d'exercice de la souveraineté. Alors que la souveraineté classique s'exerce sur des personnes physiques et des biens matériels localisés sur un territoire défini, le cyberespace se caractérise par la prédominance d'actifs immatériels – données, algorithmes, propriété intellectuelle – dont la localisation s'avère problématique. Cette dématérialisation se manifeste particulièrement dans l'économie numérique, où la création de valeur repose largement sur des actifs intangibles circulant à travers les frontières.

Aussi, la logique multi-acteurs du cyberespace constitue une caractéristique structurelle qui transforme les conditions d'exercice de la souveraineté. Contrairement aux domaines traditionnels où les États occupaient une position dominante, le cyberespace se caractérise par une gouvernance partagée entre entités étatiques, entreprises privées, organisations techniques et communautés d'utilisateurs, «*la gouvernance d'Internet n'a jamais été l'apanage exclusif des États, mais s'est structurée historiquement autour d'une constellation d'acteurs aux rôles complémentaires*» (SEGER.A, 2018). Cette réalité multi-acteurs contraste avec le modèle westphalien où l'État souverain dispose d'un monopole décisionnel sur son territoire.

La dimension infrastructurelle du cyberespace complexifie l'exercice de la souveraineté, en effet l'Internet repose sur des infrastructures physiques (câbles sous-marins, data centers, routeurs) qui sont soumises à des juridictions territoriales, mais dont le fonctionnement global transcende ces mêmes juridictions. Ainsi, un État peut contrôler les infrastructures numériques présentes sur son territoire, mais ce contrôle ne lui garantit pas une autorité effective sur les flux d'information qui les traversent. Cette limitation infrastructurelle de la souveraineté traditionnelle explique pourquoi certains États développent des stratégies d'autonomie numérique visant à rapatrier physiquement les infrastructures critiques sur leur territoire.

Ces caractéristiques intrinsèques du cyberespace engendrent des exigences spécifiques qui transforment l'exercice de la souveraineté étatique. Elles imposent notamment une redéfinition de la juridiction souveraine, traditionnellement fondée sur le principe de territorialité.

Le cyberespace exige également une adaptation des mécanismes d'application effective du droit souverain (law enforcement). Les difficultés techniques d'identification des acteurs, la volatilité des preuves numériques et la dispersion géographique des infrastructures compliquent considérablement l'application unilatérale des lois nationales. Cette réalité a conduit au développement d'une coopération internationale accrue en matière de cybercriminalité, illustrée notamment par la Convention de Budapest, mais aussi à des tensions croissantes concernant l'accès transfrontalier aux preuves numériques.

Au final, la rencontre entre souveraineté étatique et exigences du cyberespace engendre une transformation profonde des modalités d'exercice du pouvoir souverain plutôt que son obsolescence. Comme l'observe Milton Mueller, "*nous assistons moins à la fin de la souveraineté qu'à sa reconfiguration dans un environnement où la territorialité, bien que toujours pertinente, ne constitue plus le principe organisateur exclusif de l'autorité politique légitime*". Cette reconfiguration se manifeste par l'émergence de formes hybrides de souveraineté numérique qui combinent affirmation de principes souverains traditionnels et adaptation aux contraintes spécifiques de l'espace numérique.

Cet examen des tensions fondamentales entre les principes traditionnels de la souveraineté et les caractéristiques intrinsèques du cyberespace amène naturellement à examiner comment la diplomatie numérique émerge comme un instrument essentiel pour répondre aux défis spécifiques que pose la cybersécurité pour l'autorité souveraine des États.

2 - Souveraineté numérique et défis de la cybersécurité: rôle de la diplomatie numérique

2.1. Diplomatie numérique pour des dispositifs juridiques

La diplomatie numérique joue un rôle crucial dans l'élaboration des dispositifs juridiques visant à réguler le cyberespace et à protéger la souveraineté des États face aux menaces numériques. Cette fonction normative de la diplomatie numérique s'avère particulièrement complexe en raison des caractéristiques spécifiques du domaine cyber, notamment son caractère transnational, la diversité des acteurs impliqués et l'évolution rapide des

technologies concernées. Malgré ces défis, les efforts diplomatiques ont permis l'émergence progressive d'un cadre juridique international, encore fragmentaire mais en constante évolution, qui tente de concilier les exigences parfois contradictoires de la sécurité nationale et de la préservation d'un cyberespace ouvert et fonctionnel.

Les premières initiatives diplomatiques significatives en matière de régulation juridique du cyberespace remontent au début des années 2000, avec l'adoption de la Convention de Budapest sur la cybercriminalité en 2001. Ce traité, élaboré sous l'égide du Conseil de l'Europe mais ouvert à la signature d'États non-européens, constitue encore aujourd'hui le seul instrument juridique international contraignant spécifiquement dédié aux infractions commises via Internet.

À travers ses dispositions concernant l'incrimination de certains comportements (accès illégal aux systèmes informatiques, interception illégale, atteintes à l'intégrité des données, etc.), l'harmonisation des procédures d'investigation et les mécanismes de coopération internationale, cette convention illustre parfaitement comment la diplomatie peut contribuer à l'élaboration d'un cadre juridique adapté aux spécificités du numérique. Alexander Seger souligne que, «la Convention de Budapest représente un équilibre délicat entre les impératifs de sécurité, la nécessité d'une coopération internationale efficace et la protection des droits fondamentaux dans l'environnement numérique» (SEGAL. A, 2017).

Toutefois, la portée de cet instrument reste limitée, tant par son champ d'application axé principalement sur la criminalité de droit commun que par son adhésion incomplète. Des puissances majeures comme la Russie et la Chine ont refusé d'y adhérer, invoquant des préoccupations liées à la souveraineté nationale, notamment concernant les dispositions permettant l'accès transfrontalier à certaines données. Cette situation illustre la tension fondamentale entre l'exigence d'efficacité dans la lutte contre les menaces numériques transnationales et le principe de souveraineté territoriale exclusive au cœur du système international westphalien.

Cependant, les limites de cette approche sont apparues clairement lors de l'échec du GGE de 2016-2017, qui n'est pas parvenu à un consensus sur les modalités d'application de certains principes du droit international, notamment concernant la légitime défense et le droit des conflits armés dans le contexte cyber. Cet échec reflète des divergences fondamentales entre les principales puissances sur la conception même de la souveraineté numérique et la répartition des responsabilités dans la gouvernance du cyberespace. Nul doute, l'absence de

consensus au sein du GGE traduit une fracture géopolitique profonde entre les États-Unis et leurs alliés d'une part, privilégiant une approche fondée sur le droit international existant, et la Russie et la Chine d'autre part, prônant l'élaboration de nouveaux instruments juridiques spécifiques au cyberespace (NYE. J, 2014).

Cette fracture diplomatique a conduit à l'émergence de processus parallèles au sein des Nations Unies. En 2018, deux initiatives distinctes ont été lancées: un nouveau GGE à composition limitée et un Groupe de travail à composition non limitée (OEWG) ouvert à tous les États membres. Cette dualité institutionnelle, sans précédent dans l'histoire des Nations Unies, illustre l'intensité des enjeux géopolitiques liés à la régulation juridique du cyberespace. Malgré ces tensions, ces processus continuent de jouer un rôle crucial dans la clarification progressive des normes applicables aux comportements des États dans le cyberespace, notamment à travers l'élaboration de normes volontaires non contraignantes qui peuvent constituer la base d'un futur régime juridique plus formalisé.

Au-delà de ces efforts multilatéraux globaux, la diplomatie numérique s'est également déployée dans des cadres régionaux, permettant l'émergence d'instruments juridiques adaptés à des contextes spécifiques. L'Union africaine a ainsi adopté en 2014 la Convention sur la cybersécurité et la protection des données à caractère personnel, tandis que l'Association des nations de l'Asie du Sud-Est (ASEAN) a développé plusieurs accords-cadres sur la cybersécurité. Ces initiatives régionales permettent souvent de surmonter les blocages rencontrés au niveau mondial, en réunissant des États partageant des préoccupations et des approches similaires. Elles contribuent à l'émergence d'un paysage juridique international complexe et multi-niveaux, mieux adapté aux spécificités du cyberespace que ne le serait un cadre monolithique global.

La diplomatie numérique s'est également attachée à clarifier les questions de responsabilité internationale dans le cyberespace, un enjeu particulièrement complexe en raison des difficultés d'attribution technique des cyber-opérations. L'élaboration de critères et procédures d'attribution politiquement légitimes et techniquement crédibles constitue un défi majeur pour la diplomatie juridique contemporaine. Des initiatives comme le "Cyber Attribution Network" proposé par Microsoft, qui suggère la création d'une organisation internationale indépendante chargée d'attribuer les cyber-attaques majeures, illustrent les tentatives innovantes d'établir des mécanismes de responsabilité adaptés aux spécificités du domaine numérique.

En définitive, la diplomatie numérique s'affirme comme un vecteur essentiel de l'élaboration progressive d'un cadre juridique international adapté aux spécificités du cyberespace. À travers des processus multilatéraux, régionaux et bilatéraux, elle contribue à clarifier les normes applicables, à développer des mécanismes de coopération et à établir des procédures de résolution des différends. Toutefois, cette construction juridique reste fragile et incomplète, reflétant les tensions géopolitiques profondes qui traversent le système international contemporain. Comme le précise Joseph Nye, «*l'élaboration de normes juridiques pour le cyberespace constitue non seulement un défi technique complexe, mais aussi un enjeu géopolitique majeur où se jouent des conceptions divergentes de la souveraineté, de la sécurité et des libertés à l'ère numérique*» (Nocetti. J, 2017).

La capacité de la diplomatie numérique à surmonter ces divisions et à forger un consensus international minimal sur les règles juridiques fondamentales régissant le cyberespace conditionnera largement la stabilité et la sécurité de cet environnement devenu critique pour le fonctionnement des sociétés contemporaines. Dans cette perspective, l'innovation diplomatique, combinant approches traditionnelles et formats nouveaux intégrant l'ensemble des parties prenantes de l'écosystème numérique, apparaît comme une nécessité pour répondre aux défis inédits que pose la régulation juridique d'un domaine aussi complexe et évolutif que le cyberespace.

2.2- Diplomatie numérique: vecteur de régulation du cyberespace

La diplomatie est diluée dans une gouvernance globale, des formes de régulation transnationale qui se multiplient et desquelles les acteurs nationaux sont parfois écartés. Un grand nombre de normes internationales, de standards, dans le domaine de l'internet, se sont mis en place sans passer par les canaux habituels de la diplomatie, ce qui rend celle-ci encore plus complexe.

La gouvernance de l'internet est l'un des enjeux de la diplomatie numérique qui s'ajoute à d'autres, comme la problématique qui s'impose comme paramètre fondamental, de la circulation et du stockage des données et leur traitement par des acteurs privés et par des États. La question du cryptage des données a occupé le devant de la scène, articulant la tension entre les intérêts supérieurs de l'État et les exigences de confidentialités requises par le public. Corollaire de ce problème, le clivage traditionnel entre démocraties et régimes autoritaires sur l'internet ne correspond plus à la réalité, alors que de nombreux pays

occidentaux adoptent des lois numériques particulièrement intrusives (Royaume-Uni, France, etc.).

Au niveau stratégique, la transition numérique crée une certaine rivalité entre les grandes puissances, notamment entre les États-Unis et la Chine. Plus que jamais, l'autonomie stratégique nationale repose sur la maîtrise du numérique. Cependant, cet intérêt est mis à rude épreuve par des menaces informatiques de natures et d'origines diverses, émanant d'acteurs malveillants aux motivations diverses. Les attaques augmentent en fréquence et en ampleur jusqu'à ce qu'elles présentent un éventail de risques surtout le spectre d'intensité. Là où les cybermenaces frôlent l'espionnage économique, la guerre politique et le crime organisé, le plus grand risque provient d'Etats pouvant mobiliser des capacités offensives à grande échelle à des fins déstabilisatrices et subversives. Aux risques physiques connus (cyberattaques contre des infrastructures vitales, par exemple), s'ajoute le recours agressif à l'arme informationnelle à des fins stratégiques qu'amplifie le numérique.

Ainsi, les diplomaties des pays concernés font face à de multiples défis, en plus de la difficulté de comprendre les modes opératoires et leur cohérence avec les stratégies d'influence des États. Cette nouvelle forme de prolifération, relative aux moyens employés et transformation de l'espace numérique en scène d'affrontement international, requiert l'élaboration de normes de régulation. Cependant, face à la multiplicité des menaces et des attaques conjuguées au problème de leur imputabilité, le règlement des différends et conflits dans le cyberespace s'avère délicat.

Cependant, face à la pluralité d'origine des menaces, à la nature des attaques et au problème de leur imputabilité, réguler les conflits dans le cyberespace s'est jusqu'à présent avéré délicat. L'incapacité d'identifier son adversaire rend caduc le droit à la légitime défense et fait de l'escalade une initiative très risquée, en empêchant toute dissuasion.

Autrement exprimé, la diplomatie numérique joue un rôle fondamental dans la régulation du cyberespace qui va bien au-delà de l'élaboration d'instruments juridiques formels. Elle constitue un vecteur d'influence multidimensionnel qui contribue à façonner l'environnement numérique mondial à travers une variété de mécanismes allant des normes de comportement responsable aux standards techniques, en passant par les arrangements institutionnels de gouvernance partagée. Cette fonction régulatrice de la diplomatie numérique s'avère particulièrement importante dans un domaine où les cadres juridiques contraignants restent

limités et où l'innovation technologique constante crée des défis inédits nécessitant des réponses adaptatives et évolutives.

Dans ce contexte, la diplomatie numérique contribue à l'émergence progressive d'un cadre régulateur adapté aux spécificités du cyberespace tout en préservant certaines fonctions essentielles de la souveraineté étatique. Cette diplomatie innovante, mobilisant simultanément canaux traditionnels et mécanismes multi-acteurs, représente ainsi une tentative d'adaptation créative du système international aux défis inédits de l'ère numérique.

CONCLUSION

Au terme de cette analyse consacrée à l'étude de la souveraineté et de la diplomatie numérique comme vecteur de transformation des relations internationales contemporaines au service du leadership, plusieurs enseignements majeurs se dégagent quant à la nature et implications de cette évolution fondamentale de la pratique diplomatique.

En effet, la diplomatie numérique ne constitue ni un simple ajustement technique de la diplomatie traditionnelle, ni un phénomène entièrement nouveau qui romprait avec les fondements historiques de l'action diplomatique. Elle représente plutôt une reconfiguration profonde des pratiques et conceptions diplomatiques en réponse aux transformations structurelles induites par la révolution numérique dans l'espace mondial. Cette reconfiguration affecte simultanément les acteurs impliqués, les espaces d'interaction, les méthodes d'influence et les objets mêmes de la négociation internationale.

Or, l'influence considérable acquise par certaines entreprises technologiques mondiales – dont la capitalisation, les ressources et l'influence dépassent celles de nombreux États – crée une situation inédite où la diplomatie doit intégrer des interlocuteurs non-étatiques comme parties prenantes essentielles de la régulation internationale. Cette réalité contraste fortement avec le modèle westphalien centré sur les relations interétatiques, et exige l'élaboration de nouvelles approches diplomatiques adaptées à cette configuration multipolaire et multi-acteurs.

Ces tensions, loin d'être résolues, structurent le paysage diplomatique contemporain et détermineront largement l'évolution future de la gouvernance numérique mondiale. Elles révèlent que la diplomatie numérique ne constitue pas simplement un nouveau domaine thématique de l'action extérieure des États, mais bien un vecteur de transformation fondamentale des relations internationales, comparable par son ampleur aux grandes

mutations historiques du système mondial comme l'émergence de l'ordre westphalien au XVIIe siècle ou la reconfiguration post-Guerre froide.

In fine, il convient d'admettre ce nouveau paradigme diplomatique qui ouvre des perspectives inédites et crée de nouvelles opportunités pour les acteurs du système international, redéfinissant ainsi les contours de l'influence et du leadership à l'ère numérique, ce qui trace nettement les contour d'une relation paradoxale entre, d'une part, la diplomatie numérique en tant que vecteur d'ouverture multi-acteurs et, de l'autre part, la souveraineté numérique contrainte à une certaine logique de fermeture, un contrôle du cyberespace et une reterritorialisation.

De facto, la diplomatie et la souveraineté numériques renforcent ainsi le leadership de l'Etat en favorisant le contrôle de ses infrastructures, assurent l'interaction directe et instantanée avec les publics étrangers via les réseaux sociaux, et favorisent une gouvernance indépendamment des géants technologiques. Elles contribuent également à préserver la suprématie de l'Etat en consolidant sa position stratégique sur la scène internationale grâce à des actions coordonnées et des alliances pour la sauvegarde de ses intérêts nationaux et l'adaptation aux évolutions géopolitiques.

BIBLIOGRAPHIE

(1) Adam SEGAL, « *Chinese Cyber Diplomacy in a New Era of Uncertainty* », Hoover Institution Essay, Aegis Series Paper No. 1703, 2017, p. 8-10

(2) Alexander SEGER, « *The Budapest Convention on Cybercrime: A Framework for Capacity Building*», Global Cyber Security Capacity Centre, University of Oxford, 2018, p. 12-18.

(3) D. Kirkpatrick, « *Does Facebook Have a Foreign Policy*? », Foreign Policy, 28 novembre 2011.

(4) Joseph S. NYE, « *The Regime Complex for Managing Global Cyber Activities* », Global Commission on Internet Governance Paper Series, No. 1, 2014, p.15.

(5) K. Brown, « *How Airbnb, Google, and Microsoft View Disputed Territories Differently*? », Fusion,10 février 2016.

(6) Laura De NARDIS, *The Global War for Internet Governance*. New Haven, Yale University Press, 2014, p.48.

(7) Nocetti, Julien. *« La diplomatie à l'heure du numérique. De la diplomatie numérique à la diplomatie du numérique* », Thierry de Montbrial éd., Ramses 2018. La guerre de l'information aura-t-elle lieu, Institut français des relations internationales, 2017, pp. 150-155.

(8) Robin, G. « *Diplomatie* » in Thierry de Montbrial et Jean Klein, Dictionnaire de stratégie, PUF, 2000, p.178-179

(9) Roumate, F. (Ed.). (2021). *Artificial intelligence and digital diplomacy: Challenges and opportunities*. Leiden: Brill Academic Publishers, 241 p.

(10) Stephen D. KRASNER, *Sovereignty: Organized Hypocrisy*. Princeton, Princeton University Press, 1999, p. 20-22.

(11) Thomas Gomart, « *Ecrire l'histoire des relations internationales après Wikilieaks* », Revue des deux mondes, mai 2011, p.88-89