La dualité du cyberespace en Égypte : entre mobilisation démocratique et instrument d'autoritarisme

Neil Falda

Neil Falda

La dualité du cyberespace en Égypte : entre mobilisation démocratique et instrument d'autoritarisme

---

FALDA, Neil. *La dualité du cyberespace en Égypte* **[en ligne]** *: entre mobilisation démocratique et instrument d'autoritarisme*. Sous la direction d'Ombeline LAKS. Mémoire de master professionnel 2e année : Relations internationales. Expertise et risques internationaux. Lyon : Université Jean Moulin Lyon 3, 2024.

Disponible sur : https://www.sudoc.fr/282874410

UNIVERSITÉ JEAN MOULIN LYON III

Année universitaire 2023/2024

LA DUALITÉ DU CYBERESPACE EN ÉGYPTE :

Entre mobilisation démocratique et instrument d'autoritarisme

MEMOIRE DE MASTER, RELATIONS INTERNATIONALES, EXPERTISE ET RISQUES INTERNATIONAUX

Par M. Neil FALDA

Sous la direction de :

Madame Ombeline LAKS, Responsable des Analystes Risque Cyber chez Intrinsec Sécurité

LA DUALITÉ DU CYBERESPACE EN ÉGYPTE :

Entre mobilisation démocratique et instrument d'autoritarisme

Mémoire de stage

Stage réalisé au sein d'Intrinsec Sécurité, une entreprise experte en sécurité des systèmes d'information, en tant qu'Analyse Risque Cyber du 17 Janvier au 12 Juillet 2024, dans le cadre du Master 2 Relations Internationales – parcours Expertise et Risques Internationaux.

Ce mémoire n’engage que la responsabilité de son auteur

AVANT-PROPOS

Présentation succincte du stage et de la structure d'accueil

Dans le cadre de ce stage de fin d'étude, j'ai intégré le pôle Cyber Threat Intelligence (CTI) du groupe Intrinsec Sécurité. Fondé en 1995, Intrinsec accompagne des entreprises et institutions dans la protection de leur système d'informations. La palette des services proposés s'étend de l'évaluation de la sécurité informatique aux tests d'intrusion ainsi qu'aux services de sécurité managés.

La CTI est une discipline se basant sur des techniques de renseignement visant à récolter les informations nécessaires à la qualification des risques sur le cyberespace. Il existe une dimension technique requérant des compétences basiques en informatique et techniques d'investigation en sources ouvertes (OSINT). Cependant, les compétences propres à l'étude des relations internationales telles que la connaissance des différentes aires culturelles et la compréhension des enjeux internationaux, régionaux, économiques et géopolitiques sont essentielles à l'analyse des menaces. En effet, le cyberespace est intrinsèquement lié aux mondes des relations internationales de par son caractère transnational mais aussi pour l'implication des acteurs étatiques et non-étatiques, parfois eux-mêmes affiliées à ces premiers ou en confrontation directe. De fait, ce milieu présente de nombreuses menaces et risques pour ses usagers.

Dans le cadre de mon rôle d'Analyste Risque Cyber au sein de la CTI, ma mission s'est concentrée sur l'investigation, l'analyse puis la mise en alerte des clients à propos des menaces pouvant planer sur eux au sein du cyberespace. Les différents outils internes de veille et de surveillance ont mis à ma disposition de nombreuses informations sur des réseaux de cybercriminels ou d'hacktivistes. Ainsi, il m'a été permis de récolter diverses données relatives aux groupes militants égyptiens mais aussi étatiques. Ces données m'ont permis de constater l'état géopolitique et politique du cyberespace égyptien et du Moyen-Orient.

Choix du sujet

Dans ce contexte, mon intérêt pour le paysage cyber moyen-oriental s'est dessiné, tout d'abord en raison de mon penchant pour les événements géopolitiques traditionnels s'y déroulant, mais aussi pour le regain d'activité cyber à la suite du conflit israélo-arabe vivement ranimé en octobre 2023. C'est donc tout naturellement que mes recherches bibliographiques s'y sont dirigées. A la suite de mes lectures, une question a vu le jour à propos de la nature du cyberespace égyptien. D'abord vecteur de la poussée démocrate s'opposant avec ferveur au régime autoritaire de Hosni Mubarak, il devient ensuite un outil d'oppression pour le pouvoir d'Al-Sissi. Ce changement de nature en une décennie à peine a nécessairement soulevé le questionnement des facteurs permettant une telle évolution structurelle.

Mon hypothèse première fut de considérer ce milieu comme un terrain neutre façonné par des acteurs eux-mêmes soumis à des tendances économique, sociologique, historique et politiques. C'est ainsi que mon travail sur l'Egypte et l'évolution de son cyberespace à l'aune de la lutte politique pour le pouvoir entre le régime et l'opposition commença. En d'autres termes, mon ambition fut de questionner cet espace, peut-être même ce territoire, à l'aune de la méthodologie géopolitique.

D'un point de vue pratique, ce sujet apparait comme parfaitement aligné avec les enseignements dispensés par mes deux années de Master ainsi qu'avec les activités effectuées lors de mon stage. Les recherches menées pour mon mémoire universitaire ont enrichi ma compréhension et mes analyses de la situation en Egypte. De même, mon travail quotidien de veille m'a permis d'identifier des faits concrets, de repérer des tendances et des dynamiques essentielles pour élaborer un travail exhaustif.

Remerciements

Je tiens à remercier toutes les personnes ayant contribuées, de près ou de loin, au bon déroulement de mon stage, de ma formation à mon intégration. Mes remerciements s'adressent particulièrement à mon tuteur de stage Thibault REIHLAC qui a pris le temps nécessaire pour me former et m'accompagner dans la bienveillance et la confiance.

Je souhaite aussi remercier ma directrice de mémoire, Ombeline LAKS, qui a su m'aiguiller dans la réalisation de ce mémoire tant dans sa conception que dans sa rédaction.

Enfin, j'adresse mes plus sincères remerciements à ma famille, mes parents, qui m'ont toujours accompagné, soutenu et encouragé tout au long de mes études.

Mots-clés : cyberespace ; politique ; Egypte ; autoritarisme ; mobilisations ; Moyen-Orient ; Printemps arabes ; Etats ; cybermilitantisme ; démocratie

Résumé : Pendant les Printemps arabes, le régime autoritaire égyptien cède face à l'opposition démocratique après 18 jours de manifestations. Ces mobilisations ont été largement facilitées par l'usage des réseaux sociaux. Ainsi, les Printemps arabes semblent valider les thèses des cyber-utopistes qui estiment que l'émergence du cyberespace favorise la démocratisation. Cependant, l'Égypte est le seul pays à avoir connu à la fois la chute de l'autoritarisme et son rétablissement sans effusion de sang. La lutte politique a en grande partie occupé l'espace virtuel faisant de ce milieu un outil favorisant chacun des acteurs entre les années 2000 et 2020. D'abord au service de mobilisations contestataires et de techniques de contournement de la censure, le cyberespace devient ensuite une arme de surveillance et de propagande. La question demeure quant à savoir ce qui a permis au cyberespace égyptien de basculer d'un usage à l'autre au cours de cette période. Ainsi, ce mémoire tend à démontrer, à travers une rétrospective socio-politique, que les évolutions structurelles du cyberespace sont dépendantes de la lutte de pouvoir entre l'opposition et le régime.

SOMMAIRE

INTRODUCTION

« *L'Egypte, en ce monde où tout change, - Trône sur l'immobilité.* », *Émaux et camées*, 1852, Théophile Gautier

L'Égypte reste immobile, intacte comme figée dans le temps des Raïs. Pourtant, les contemporains écrivaient, à l'instar de Bertrand Badie, que « *le printemps arabe a mis en mouvement des sociétés qui ont été longtemps apparemment immobiles* »[1]. Il est vrai que ce phénomène politique a été comme un vent de changement sur les anciennes dictatures arabes. D'autant plus que son militantisme a pris une forme nouvelle par l'utilisation des réseaux sociaux. Le progrès technologique entraînant des modifications sociétales semblait être l'élément déclencheur emportant l'Égypte vers la voie de la démocratie. Nonobstant, les écrits de Théophile Gautier raisonnent comme un lointain écho du passé décrivant à merveille la situation égyptienne. Tout change autour d'elle : Tunisie, Lybie, Syrie connaissent un avant et un après. Au Caire, seul un interlude fugace et puissant entre 2011 et 2013 fait croire à un changement. Il a été permis par un élément nouveau dont n'avait pas pris conscience le régime d'alors, le cyberespace. Perçu comme le vecteur de la démocratie, comme le fossoyeur des dictatures, ce nouveau milieu stratégique s'est aussi avéré être l'outil de la vieille élite pour restaurer et renforcer son pouvoir.

Il convient avant tout de définir ce qu'est le cyberespace. William Gibson est le premier à faire usage de ce concept dans son œuvre de science-fiction *Neuromancien* (1984) en le désignant comme « *une hallucination consensuelle vécue chaque jour par des dizaines de millions de participants volontaires répartis sur toute la planète* »[2]. Dès l'origine, cet espace s'agrège autour de l'idée d'un partage d'information instantané entre individus dans un monde en dehors du nôtre mais qui lui est pourtant transversal. Si cette définition pose les bases métaphoriques, voire littéraires, de la compréhension d'un tel espace, il convient de se rapprocher du concept de cyberespace développé par l'ANSSI dans le but de comprendre ce terme à l'aune des enjeux actuels. Ainsi, le cyberespace apparaît comme étant un espace de communication constitué par l'interconnexion mondiale d'équipements de traitement

[1]Badie, Bertrand. « Printemps arabe : un commencement », *Études*, vol. 415, no. 7-8, 2011, pp. 7-18.
[2]William Gibson. *Neuromancien*, New York City, 1984, ACE, p. 37

automatisé de données numériques. Il est alors question d'un espace reposant sur une « couche physique » au travers de divers équipements tels que les ordinateurs, les systèmes d'informations, les smartphones, mais aussi les infrastructures, les câbles, les serveurs et les systèmes de routages. Le cyberespace repose donc sur une dualité réelle et virtuelle. Afin d'y accéder, il convient d'utiliser un certain nombre d'équipements, d'infrastructures qui peuvent eux-mêmes être sujets à des blocages, des sabotages ou des destructions. Les tentatives de surveillance des cybercafés en Égypte, tout comme la fouille des appareils informatiques en marge des manifestations en 2011, sont autant d'exemple rappelant cette dualité. Cette « couche matérielle » signifie donc que le cyberespace pose autant d'enjeux dans le monde physique que virtuel.

Ayant le mérite d'être beaucoup plus descriptive, cette définition n'en reste pas moins incomplète dans la mesure où la composante humaine y est exclue. Pourtant, le cyberespace est le lieu où se rencontrent les individus et les groupes par l'échange d'informations, la création de contenus et les multiples interactions sociales propres à cet univers. C'est ainsi que Pierre Levy définit le cyberespace comme *« l'univers des réseaux numériques comme lieu de rencontres et d'aventures, enjeu de conflits mondiaux, nouvelle frontière économique et culturelle. […] Le cyberespace désigne moins les nouveaux supports de l'information que les modes originaux de création, de navigation dans la connaissance et de relation sociale qu'ils permettent* »[3]. Conséquemment, l'interaction entre collectivités et individualités est un élément central du cyberespace.

La distinction entre les termes d'Internet et de cyberespace s'imposent tant ces deux notions sont usuellement confondues. Si le cyberespace est désigné comme un ensemble de réseaux numériques, Internet en constitue un. Il s'agit d'un ensemble de réseaux utilisant tous le même protocole TCP/IP[4]. Ainsi, le cyberespace est en partie présent sur Internet, mais il n'en est pas un synonyme.

Cet espace est caractérisé par sa transnationalité, ce qui en fait une composante majeure des relations internationales. Les États se sont emparés de ce lieu comme d'un nouveau champ de confrontation stratégique[5]. Mais la véritable évolution se révèle aux acteurs non-étatiques. Les TIC ont délivré une véritable capacité d'action aux individus, groupes de criminels et d'activistes ainsi qu'aux acteurs privés. L'anonymat sur les réseaux est permis par l'opacité

[3]Lévy, Pierre. *L'intelligence collective: pour une anthropologie du cyberspace*. Éditions La Découverte, 1994.
[4]Le protocole TCP (Transmission Control Protocol**)** veille à la transmission des données de bout en bout. Le protocole IP identifie les différents appareils présents sur le réseau.
[5]Olivier, Kempf. *Introduction à la cyberstratégie*. Economica, 2012.

des informations générée par les pseudonymes, les VPN et le chiffrement de données. Il en résulte un avantage pour les groupes de cybercriminels, mais aussi les dissidents politiques. Comme l'expose Romain Lecomte, l'anonymat sur Internet a permis aux démocrates tunisiens de se dissimuler tout en diffusant leur message politique[6]. L'anonymat apparaît donc comme un moyen de protection pour la liberté d'expression et de conscience.

C'est pourquoi, l'innovation que constitue le cyberespace s'accompagne d'un présupposé sur son aptitude à devenir un outil au service de la société civile. Au regard des théories cyberutopistes, plus une société est liée au cyberespace, plus elle a de chance de devenir une démocratie. En effet, la diffusion rapide d'informations et la création de communautés en ligne en sont alors grandement facilitées. Il en résulte une plus grande autonomie des individus et une liberté d'expression accrue.

Dans le cas des Printemps arabes, l'interconnectivité entre les pays a permis la propagation de l'élan révolutionnaire entre la Tunisie et l'Égypte. Il serait alors question de l'émergence d'un « village global » baigné au sein du cyberespace abolissant les frontières géographiques et les hiérarchies traditionnelles. La « révolution Facebook » en Égypte, ou bien la « révolution Youtube » sont autant de concepts qui émergent en 2011 pour qualifier le pouvoir mobilisateur du cyberespace[7]. Car c'est bien par le Web 2.0[8] que se sont répandus les idéaux démocratiques au sein des pays arabes d'Afrique du Nord et du Moyen-Orient. Des personnalités comme Mohamed ElBaradei ou Omar Afifi ont su galvaniser la jeunesse tout en fustigeant les régimes autoritaires[9], tout comme les cybermilitants ayant organisé des actions via les pages Facebook ou des hashtags Twitter.

Cependant, le cas de l'Égypte pose question. Depuis le règne du premier raïs Nasser, l'Égypte est une « stratocratie », c'est-à-dire un État gouverné par l'armée[10]. Ce système politique autoritariste semble s'ébranler durant la tempête des Printemps Arabes en 2011, donnant en effet raison aux cyberutopistes. Si le régime s'écroule en 18 jours, la pérennisation de la

---

[6]Romain Lecomte, « L'anonymat comme « art de résistance » », *Terminal* , 2010.
[7]Clarke, Killian, and Korhan Kocak. "Launching Revolution: Social Media and the Egyptian Uprising's First Movers." *British Journal of Political Science* 50.3, 2020.
[8]Le Web 2.0 est une expression utilisée pour décrire la deuxième phase du développement du World Wide Web, caractérisée par un changement dans la manière dont les utilisateurs interagissent avec les sites web. Le Web 2.0 a facilité l'émergence de communautés en ligne, l'échange d'idées et de connaissances, ainsi que la création de réseaux sociaux virtuels. Il a transformé Internet en un espace plus interactif, où les utilisateurs peuvent non seulement consommer du contenu, mais aussi le produire et le partager avec d'autres.
[9]Clarke, Killian, and Korhan Kocak. "Launching Revolution: Social Media and the Egyptian Uprising's First Movers." *British Journal of Political Science* 50.3 2020.
[10]Tomiche Nadia. P. J. Vatikiotis, *The Egyptian Army in Politics. Pattern for new Nations ?*. In: *Annales. Economies, sociétés, civilisations*. 20e année, N. 4, 1965. pp. 851-852.

démocratie n'en a pas pour autant été assurée. Pays fortement connecté, quatre-vingts millions de personnes ayant accès à Internet en février 2010, il bascule dans la démocratie sans crier gare pour ensuite redevenir la stratocratie initiale en 2013 sous la coupe du général Abdel Fattah al-Sissi.

L'Égypte possède donc une spécificité dans ces Printemps arabes. Alors que la Tunisie se démocratise sans difficulté, la Syrie plonge dans une guerre civile, puis internationale, meurtrière. La Libye s'effondre en même temps qu'est déchu Kadhafi et les pétromonarchies ne ressentent que quelques secousses au travers de rassemblements sans lendemain. Seul le Caire connaît brièvement la démocratie puis le retour à l'autoritarisme, sans pour autant sombrer dans les troubles de la guerre civile. Le cyberespace est alors surveillé en masse, des frontières sont établies et l'État cherche à y instaurer sa souveraineté complète. Après avoir été l'outil de l'opposition démocratique, le cyberespace devient un outil au service de l'autoritarisme.

Il n'existe donc pas de lien entre démocratisation et développement du cyberespace. Pour les cyberpessismites il pourrait même s'agir de l'inverse : plus un pays est connecté, plus il a tendance à surveiller sa population. Mais au regard de la situation égyptienne, ce débat apparaît obsolète dans la mesure où le cyberespace est avant tout un milieu. Comme énoncé plus haut, des acteurs y évoluent et interagissent. En ce sens, le cyberespace est un espace géopolitique, c'est-à-dire un lieu où luttent et coopèrent des groupes humains dans le seul but de faire prévaloir leurs intérêts[11]. Conséquemment, la seule pénétration du cyberespace dans une société ne détermine pas sa trajectoire démocratique[12]. Il s'agit ainsi de considérer le cyberespace comme un milieu s'illustrant comme une arène et une agora, lieu d'échange et de coopération, mais aussi de tensions et d'affrontements. Ce mémoire s'intéresse donc à la lutte au sein du cyberespace entre l'opposition démocratique et le régime autoritaire dans un but politique c'est-à-dire le fait de garder ou prendre le pouvoir au sein d'une communauté[13]. Ainsi, il apparaît à première vue évident que la trajectoire du cyberespace égyptien est avant tout déterminée par des éléments extérieurs tels les acteurs et les évolutions socio-politiques structurelles.

Ceci étant posé, la question est de savoir comment le cyberespace égyptien a su profiter à l'opposition démocratique puis au régime autoritaire. En d'autres termes, quelles ont été les

[11]Zajec, Olivier. *Introduction à l'analyse géopolitique*. 2018.
[12]Kim, Elvis H. "Democratization and authoritarianism in the information age." *International area studies review* 24.3 (2021): 205-223.
[13] Freund, Julien. *Qu'est-ce que la politique?* 1965.

évolutions structurantes du cyberespace égyptien ayant participé au triomphe de la démocratie puis au retour de l'autoritarisme ?

L'histoire de cette lutte peut se scinder en trois grandes étapes chronologiques. Tout d'abord, la période pré-Printemps arabes semble avoir posé les bases d'un cybermilitantisme dans un contexte de développement de la connectivité et du manque d'investissement du régime dans le contrôle et la surveillance de cet espace (I). Ensuite, entre 2011 et 2013, cet espace devient un champ de bataille informationnelle où d'une part le régime est défait et d'autre part le cybermilitantisme démocratique des origines échoue (II). Enfin, la période allant de 2013 à nos jours se structure comme un retour en force du régime qui légitime son contrôle et sa surveillance sur le cyberespace (III).

PARTIE I – UN DÉFAUT DE CONTRÔLE ÉTATIQUE : ÉMERGENCE ET PROSPÉRITÉ DU CYBERMILITANTISME D'OPPOSITION

Durant les années 2000, les facteurs socio-politiques en Egypte amènent au développement et à la prospérité du cybermilitantisme arabe d'obédience démocratique. Sa montée en puissance lui permet d'aboutir à une mobilisation collective défiant le régime en 2011. Le cyberespace devient une ressource pour l'opposition, d'une part parce qu'il n'est pas investi par le régime autoritaire, empêchant ainsi l'émergence de mobilisations collectives (1) ; et d'autre part, parce que le cyberespace donne au mouvement les outils nécessaires pour mobiliser et élargir son champ d'action (2).

CHAPITRE 1 – UNE POLITIQUE NATIONALE EN DÉCALAGE AVEC LES ENJEUX DE CYBERCONTRÔLE PROPRE AUX RÉGIMES AUTORITAIRES

Le régime de Mubarak est un régime autoritaire qui ne s'approprie pas le cyberespace de sorte à en faire un outil de contrôle et de stabilité. Pourtant, l'Egypte le développe afin d'en faire un vecteur économique et un espace de divertissement (1). Il existe donc un désintéressement étatique pour la bataille politique au sein de ce milieu. Et lorsque celui-ci se manifeste, la politique de surveillance et de contrôle est en décalage avec les spécificités portées par l'avènement du cybermilitantisme (2).

Section 1 - Développement étatique du cyberespace et lacune du *cyber state capability*

La particularité égyptienne réside dans le précoce développement de sa connectivité au cyberespace. Le régime de Mubarak est porteur d'une dynamique visant à élargir l'offre

Internet, mobile et réseaux à l'ensemble de la société. Ainsi, de nombreux programmes et investissements sont mis en place pour favoriser l'extension des infrastructures des TIC. Soucieux de moderniser le pays, Mubarak encourage la création du premier réseau national baptisé Egyptian National STI NETwork (ENSTINET). Sous l'impulsion de l'ambition du régime de faire de l'Egypte un acteur de pointe des infrastructures réseaux, il devient le réseau le plus avancé d'Afrique. Sa fonction première est de permettre l'échange d'informations entre les universités du pays. Toujours dans une dynamique de développement, l'ENSTINET se raccorde au réseau mondial qu'est Internet en 1993. Le régime pousse l'Egypte à devenir le nœud de connexion de tous les réseaux régionaux en portant le projet de Regional Information Network for Africa (RINAF). Ce faisant, l'Egypte acquiert une place importante dans la région en permettant, via son réseau, de connecter de nombreux pays d'Afrique et du Moyen-Orient[14].

Nationalement, l'Egypte ambitionne de démocratiser l'usage d'Internet aux secteurs clef de la recherche et de l'économie. Ainsi, ce sont de nombreux sous-réseaux qui sont élaborés pour les domaines de la recherche, de l'enseignement, de l'énergie, de l'industrie et de l'agriculture. Parmi eux, le sous-réseaux HealthNet37 connecte de nombreux centres hospitaliers permettant la création d'une base de données médicale nationale. La démocratisation de l'accès à Internet pour la population est rendue possible par un partenariat public-privé avec deux entreprises américaines dont l'objectif est de fournir un accès Internet haut-débit. Conséquemment, la puissance de transmission du réseau égyptien passe de 9,6 Kb/s à 256 Kb/s entre 1993 et 1999 soit une augmentation de 26 fois plus. De même, dans le domaine de la téléphonie, la compagnie nationale Egypt Telecom passe de nombreux contrats auprès d'entreprises étrangères dans le but de produire et de fournir des téléphones cellulaires à la population tout en développant les infrastructures. En 1994, le réseau de téléphonie dessert 8 000 usagers avec une capacité de 70 000 lignes[15].

En parallèle de l'accroissement des infrastructures TIC, le gouvernement est conscient que la démocratisation du cyberespace ne peut être possible que si la population possède les outils adéquats. C'est pourquoi est mis en place une série de politiques d'aide à l'achat d'équipements de télécommunication pour les foyers égyptiens. À partir de 1999, elles incluent l'accès gratuit à Internet, la mise à disposition d'ordinateurs à bas prix, ainsi que

[14]ERCIM, « Le développement d'Internet dans les pays méditerranéens et la coopération avec l'Union européenne: une étude menée pour la Commission européenne». 1997
[15]Ordioni, Natacha. "Technologies de l'information et de la communication et développement du Sud de la Méditerranée: une problématique d'analyse du cas d'Internet." *Mondes en développement* 27.105 (1999): 71-78.

l'expansion des centres d'accès à Internet, tels que les cybercafés. Concrètement, en 2002, le ministre des Communications et des Technologies de l'information (MCIT) lance l'initiative « Un ordinateur pour chaque foyer ». Ce projet vise à augmenter l'utilisation des ordinateurs et d'Internet, en se concentrant sur les zones rurales et les familles à revenu limité. Dès 2008, un ordinateur ainsi qu'un abonnement ADSL à 512 Kb/s valables trois ans sont accordés aux familles modestes[16]. Par conséquent, en février 2011, plus de 21% de la population égyptienne, soit environ 18,69 millions de personnes, possèdent un accès à Internet ; et plus de 4,5 millions utilisent Facebook[17]. Par ailleurs, 70% de la population possède un abonnement de téléphone portable. Le marché de la téléphonie mobile atteint un taux de pénétration remarquable de 100 % en 2011[18]. En somme, sous l'impulsion de ces politiques de développement, l'Egypte est considérée dès 2010 comme « l'un des principaux marchés Internet en Afrique, en termes d'utilisateurs, de bande passante internationale et de services offerts »[19].

A première vue, l'Etat égyptien prend conscience des opportunités qu'offre le cyberespace pour son développement. En effet, le premier objectif de l'Etat égyptien consiste à transformer le cyberespace en un vecteur de croissance économique. La stimulation des TIC s'accompagne d'une augmentation de revenus dans le secteur. Au cours des années 2000, ce sont près de 2,5 milliards de dollars qui sont produits[20]. Parallèlement, l'Etat profite de ce dynamisme économique en constatant une augmentation de 10% son PIB chaque année entre 2000 et 2010.

Cependant, malgré l'augmentation du taux de connectivité du pays, le régime ne prend pas conscience de tous les avantages que peut lui offrir ce nouvel espace notamment en termes de stabilité politique. Selon les travaux de Christian Göbel, le pouvoir des régimes autoritaires s'appuie sur trois axes : les pouvoirs infrastructurel, discursif et despotique[21]. De surcroit, selon Christensen Britt, le cyberespace, peut être un moyen de les renforcer. Se dégage de ces études le concept de « *cyber state capability* » renvoyant à la volonté d'un Etat autoritaire à

[16]D'Urbano, Paolo. *Ikhwan web: digital activism and the Egyptian Muslim Brotherhood*. Diss. SOAS, University of London, 2012.
[17]Internet World Stats. "Internet world stats: Usage and population statistics." *Miniwatts Marketing Group*, 2011.
[18]Henry, Lancaster. *Egypt - Mobile Infrastructure, Operators and Broadband - Statistics and Analyses*. Budde Com, 2009.
[19]*Ibid*
[20]Arab Republic of Egypt: Ministry of Communication and Information Technology. ICT Indicators Report 2007–2011. 2011.. Retrieved from http://www.mcit.gov.eg/Upcont/Documents/Publications_1382012000_Indicator%20E%202012-final2.pdf
[21]Göbel, Christian. "The information dilemma: How ICT strengthen or weaken authoritarian rule." *Statsvetenskaplig tidskrift* 115.2013 (2013): 367-384.

s'approprier le cyberespace afin de renforcer son pouvoir et sa stabilité[22]. L'étude comparative de Britt met en exergue la différence entre l'Arabie Saoudite et l'Egypte au regard de de cette notion. Ainsi, il existe un écart significatif se traduisant par une faible volonté du régime égyptien à utiliser le cyberespace comme d'un outil de contrôle politique. Conséquemment, cette lacune se traduit par l'instabilité du régime lors des printemps Arabes, à l'inverse de l'Arabie Saoudite. Là où Riyad investit tous les champs possibles des trois axes du pouvoir autoritaire sur le cyberespace (infrastructurel, discursive et despotique), l'Egypte ne se concentre que sur le développement de son pouvoir infrastructurel par l'augmentation des gains économiques. La hausse des revenus permet au régime de consolider sa stabilité politique grâce une redistribution stratégique des richesses. Mais cet axe n'est pas suffisant à lui seul pour traduire un important *cyber state capability*.

Le cyberespace échappe donc au contrôle du pouvoir dans la mesure où très peu de politiques visent à encadrer les activités y ayant court. Pire encore, le régime y opère une stratégie de « *safety valves* » (soupape de sécurité)[23]. En effet, parallèlement au développement d'Internet, le régime opère une politique de relâchement de la surveillance des opinions dissidentes[24]. Les médias traditionnels connaissent une plus grande liberté de telle sorte que s'opère une « catharsis du mécontentement politique » autorisant les dissidents à s'exprimer afin de réduire leurs ardeurs révolutionnaires.

Le cyberespace se développe donc dans un environnement plus ouvert, alors même que le régime en place est une autocratie, ce qui y ouvre la porte à la protestation et à la mobilisation. Cet état de fait est d'autant plus accentué que cet espace demeure neuf. En outre, le régime n'opère pas, au début du moins, une grande politique de surveillance des activités sur Internet. De là, le cyberespace égyptien devient le terrain de jeu de l'opposition démocratique.

Pourtant, l'Etat n'est pas totalement dupe en ce qui concerne l'influence du cyberespace sur la population et la politique. Bien au contraire, sa stratégie de « *safety valves* » se couple avec l'ambition de couper la population de la politique par le divertissement. Cette stratégie « d'opium du peuple » a le mérite de renforcer le pouvoir discursif des Etats autoritaires. Dans

[22]Christensen, Britt. "Cyber state capacity: A model of authoritarian durability, ICTs, and emerging media." *Government Information Quarterly* 36.3 (2019): 460-468.
[23]Khamis, Sahar. "The role of new Arab satellite channels in fostering intercultural dialogue: can Al Jazeera English bridge the gap?." *New media and the new Middle East*. New York: Palgrave Macmillan US, 2007. 39-51.
[24]Khamis, Sahar, Paul B. Gold, and Katherine Vaughn. "Beyond Egypt's "Facebook revolution" and Syria's "YouTube uprising": Comparing political contexts, actors and communication strategies." *Arab Media & Society* 15.spring (2012): 1-30.

un premier temps, cela semble fonctionner. En 2010, 60% des jeunes égyptiens présents sur les réseaux sociaux passent leur temps sur des forums de discussions divers, 20% sur des sites pornographiques, 12% effectuent des affaires ou des recherches, et seulement 8% consultent du contenu politique[25]. Mais les opposants, malgré leur nombre minoritaire, réussissent à amplifier leurs actions et leurs propos via les réseaux sociaux qui leur offrent une caisse de résonnance immense et un répertoire d'action conséquent. De fait, le pouvoir discursif de l'Etat semble dépassé par la libre expression, permise par un défaut de surveillance du contenu sur Internet. En d'autres termes, la politique de cybersécurité de l'Egypte apparait inadaptée aux enjeux du pouvoir autoritaire.

Section 2 - Une politique de cybercontrôle tardive et inadaptée à la stabilité du pouvoir autoritaire

La politique de Mubarak sur le cyberespace est en décalage avec les enjeux de cybercontrôle permettant le renforcement des trois axes de pouvoir de l'autoritarisme. Le pays développe assez tôt sa connectivité mais tarde à prendre conscience des enjeux politiques. Malgré l'augmentation des revenus et le système de « *safety valve* », le pouvoir autoritaire égyptien ne développe pas son pouvoir despotique qui s'illustre par la surveillance de masse et la propagande. Du fait de son rôle dans le maintien de la stabilité du Moyen-Orient, l'Egypte se préoccupe davantage des questions liées à la sécurité régionale. Depuis Nasser et les guerres israélo-arabes, les dirigeants du pays conservent cette position traditionnelle[26]. C'est pourquoi, l'Etat transpose ses préoccupations géopolitiques dans le cyberespace. Si bien que le cyberterrorisme et la cybercriminalité demeurent des problèmes bien plus importants que le cybermilitantisme.

Au niveau régional, l'Egypte s'engage dans de nombreux accords et programmes internationaux visant à développer cette lutte. Le pays est partie prenante de la Déclaration du Caire contre la cybercriminalité de 2007. Cette initiative du Conseil de l'Europe, dans la

[25]Sawi, A., & Hady, Z. A. "Youth and Participation in Society." Egypt Human Development Report, edited by H. Handoussa, United Nations Development Program, and the Institute of National Planning, 2010, pp. 105–122.
[26]Hassib, Bassant, & Alnemr, Nardine. "Securitizing CyberSpace in Egypt: The Dilemma of Cybersecurity and Democracy." In *Securitizing CyberSpace: Current Policies, Challenges, and Opportunities*, edited by Francesca Spagnoli et al., Routledge, 2021, pp. 522. doi: 10.4324/9780429399718-44.

continuité de la Convention de Budapest de 2001, souligne la nécessité de législations nationales sur ce sujet. Le cadre ne prévoit donc pas de faire du cyberespace une extension de la souveraineté. Au lieu de cela, la cybersécurité est définie comme la capacité technique des pays arabes à lutter contre les violations de la vie privée, la cybercriminalité, le cyberterrorisme et la cyberguerre[27]. En outre, le Plan d'action UE-Égypte de 2007 spécifie une coopération mutuelle dans la gouvernance de l'Internet pour le développement socio-économique et la lutte contre la cybercriminalité et le cyberterrorisme. Par conséquent, le transfert de connaissances et de ressources vise à développer l'infrastructure Internet et non le cybercontrôle[28].

Au début des années 2000, il est aisé de constater que l'Egypte ne vise pas à étendre la surveillance sur les réseaux sociaux. Il existe, certes, une politique de surveillance et de répression malgré la politique de relâchement. La loi de 2003 sur les télécommunications donne aux institutions de l'État le pouvoir de contrôler tous les services, ressources et administrations de télécommunications en cas de manifestations générale ou de danger pour l'Etat[29]. Dès 2005, les cybercafés sont tenus de fournir les noms, numéros d'identification et adresses électroniques de tous les clients qui utilisent leurs services. Ces lieux restent à cette époque le seul moyen pour de nombreux égyptiens de se connecter à Internet. Leur surveillance représente donc le premier pas pour le régime afin de savoir qui se connecte. Mais elle traduit aussi un manque de volonté à véritablement surveiller ce qui se passe sur les réseaux. En effet, le régime ne s'accorde qu'à user de son pouvoir sur la « couche physique ».

En 2008, les émeutes de la faim marquent un véritable tournant. Les cyberactivistes créent une page Facebook pour se joindre aux ouvriers du textile de Mahalla lors d'une grève générale [30]. Ces événements font prendre conscience des problèmes politiques pouvant surgir des réseaux sociaux. En effet, cette page Facebook attire 70 000 internautes illustrant le fort retentissement du mouvement. Le régime développe sa méfiance envers cet espace qu'il ne contrôle que très peu. Cette mobilisation le pousse à adopter une politique de surveillance sur Internet. Celle-ci prend la forme d'une surveillance ciblée à l'instar de la surveillance traditionnelle que pratique déjà le régime dans le monde physique. Des technologies

[27]Dr. Ramadan Elaiess, "Action Plan Towards the Information Society in Developing Countries and the Arabic Speaking World". American Research Journal of Computer Science and Information Technology, Volume 2, 2017; pp:1-18.
[28]Hassib, Bassant, and Nardine Alnemr. "The dilemma of cybersecurity and democracy." *Routledge Companion to Global Cyber-Security Strategy*, 2021, p. 521.
[29]Telecommunication Regulation Law no. 10 of 2003 Article 65
[30]Flynn, Matthew J. "Cyber rebellions: The online struggle for openness." *Journal of International Affairs* 71.1.5 (2018): 107-114.

étrangères sont importées comme le logiciel espion « Fin Spy » de Gamma International, une entreprise britannique, permettant de compromettre des comptes Skype, de messageries ou pour contrôler des appareils ciblés[31]. Par ailleurs, le régime utilise des technologies d'inspection approfondie des paquets (DPI)[32] fournis par l'entreprise israélienne Narus[33]. En outre, les échanges téléphoniques ou SMS peuvent être captées grâce à la coopération d'entreprises de télécommunication privées. Par exemple, la société Nokia Siemens Networks accorde l'accès à grande échelle aux réseaux téléphoniques du pays.

Par conséquent, la répression se fait plus sévère sur les réseaux sociaux à partir de 2008. Sur cette années 100 blogueurs sont arrêtés par la police égyptienne. En 2011, un blogueur a été envoyé en prison pour une publication sur Facebook critiquant l'armée[34]. A cela s'ajoute les techniques courantes d'intimidation et de violence fréquemment utilisées contre les membres de l'opposition comme les appels téléphoniques menaçant et les passages à tabac[35]. Ce virage de la politique égyptienne est officialisé par l'adoption de la Convention arabe sur les infractions liées aux technologies de l'information de 2010 qui permet de suivre les utilisateurs et de contrôler les éléments stockés sur les ordinateurs et les appareils des individus et des organisations. Cette adhésion est significative des nouvelles priorités du gouvernement sur le cyberespace passant de la sécurité régionale à la lutte politique contre l'opposition.

Néanmoins, cette politique ne porte pas ses fruits car elle n'est pas adaptée au milieu cyber. Le régime de Mubarak ne fait que transposer les anciens modes de répression sur les réseaux sociaux. Ils visent à éliminer les noyaux des mouvements protestataires, c'est-à-dire les meneurs en les emprisonnant ou en les assassinant. Or, le cyberespace permet à une mobilisation de vivre sans qu'il n'y ait besoin de « chef ». L'organisation des manifestations dans l'espace virtuel élimine les noyaux centraux des manifestations car les partisans de ces mouvements sont dispersés dans différentes régions géographiques[36]. Par ailleurs les gouvernements ne peuvent avoir directement accès à certains militants opérant depuis

[31] *Ibid.*
[32] L'inspection approfondies des paquets (DPI) est une méthode d'examen du contenu des paquets de données transitant sur un réseau. L'inspection approfondies recueille les données tels que l'entête du paquet, contenant l'IP source et de destination et le numéro de port ; mais aussi les données que contient le paquet.
[33] Hassib, Bassant, and James Shires. "Manipulating uncertainty: Cybersecurity politics in Egypt." *Journal of Cybersecurity* 7.1 (2021): tyaa026.
[34] « Egypte. Il avait critiqué l'armée : le blogueur écope de trois ans de prison »., 11 avril 2011, www.letelegramme.fr/monde/spanegyptespan-il-avait-critique-larmee-le-blogueur-ecope-de-trois-ans-de-prison-1164191.php.
[35] Christensen, Britt. « Cyber state capacity : A model of authoritarian durability, ICTs, and emerging media » . Government Information Quarterly, vol. 36, no 3, juillet 2019, p. 460-68. https://doi.org/10.1016/j.giq.2019.04.004.

l'étranger. Le gouvernement s'appuie donc toujours sur une politique de répression et de blocage basée sur « la couche physique » du cyberespace en pratiquant arrestations et intimidations. Or, une telle approche se retrouve confrontée à certaines limites et ne peut pas devenir efficace si elle n'est pas couplée à des modes d'actions de la « couche réseau ».

Le contrôle du contenu numérique par le filtrage fait partie de ces mesures complémentaires que ne prend pas le régime. Britt l'expose comme l'une des plus grandes différences entre les politiques de cyber-répression saoudienne et égyptienne. A titre d'illustration, en 2010, cinq millions d'Égyptiens ont accès à Facebook, qui atteint un taux de pénétration de 5,49 % dans le pays[37]. Cette absence de filtrage des contenus permet à une culture numérique dynamique d'évoluer et de s'épanouir en Égypte[38]. Cette dernière échappe au contrôle de l'État en termes de création de contenu. Ainsi, les cybermilitants peuvent développer leurs idéologies et mouvements sans que le gouvernement ne puisse les réguler. Il n'existe pas non plus de propagande d'État sur le cyberespace égyptien venant battre en brèche le discours de l'opposition. Tout bien considéré, le monopole du discours sur les réseaux demeure entre les mains du cyberactivisme d'opposition.

CHAPITRE 2 – LE CYBERESPACE AU SERVICE DE LA MOBILISATION COLLECTIVE

En s'appuyant sur les principales théories des mobilisations collectives, il apparaît que le cyberespace est devenu un outil indispensable pour l'opposition face à un régime exerçant un cybercontrôle limité. Tout d'abord, l'opposition utilise le cyberespace pour préparer la mobilisation (1). Ensuite, elle en fait une ressource pour diversifier son répertoire d'actions collectives permettant ainsi des mobilisations qui seraient impossibles hors ligne sous le régime de Mubarak (2).

[36]Ahmadipor, Zahra, and Mahdi Karimi. "The impact of cyber space on Egypt's revolution." *The International Journal of Humanities* 23.1 (2016): 99-117.
[37]Christensen, Britt. "Cyber state capacity: A model of authoritarian durability, ICTs, and emerging media." *Government Information Quarterly* 36.3 (2019): 460-468.
[38]*Ibid.*

Section 1 - Émergence et développement du cyberactivisme comme ressource préalable à la mobilisation

Le cyberactivisme en Égypte favorise l'émergence de mobilisations collectives. L'État tolère l'essor d'une « cyberculture d'opposition », facilitant l'organisation de mouvements diversifiés, jetant ainsi les bases des manifestations des Printemps arabes. Contrairement à la révolte tunisienne, qui est spontanée, celle d'Égypte se développe progressivement tout au long des années 2000[39]. Ces nouveaux modes de communication permettent une forme d'activisme en ligne, définie ici comme « l'acte d'utiliser Internet pour promouvoir une cause politique difficile à promouvoir hors ligne »[40].

Le contexte socio-politique est déterminant dans l'expression du militantisme sur le cyberespace. Tout d'abord, l'Égypte pré-Printemps arabes connaît une situation socio-économique peu enviable. À cette période, près de 20 % de la population égyptienne se trouve sous le seuil de pauvreté, rendant de plus en plus difficile, pour les Égyptiens démunis, le fait de pourvoir à leurs besoins fondamentaux[41].

De plus, l'État est gangrené par une corruption latente couplée à un système autoritaire. Le pays est en état d'urgence presque constant depuis 1967, permettant au gouvernement de réprimer les manifestations, de censurer les médias et de détenir des citoyens pendant de longues périodes sans inculpation formelle. Cette situation engendre un sentiment de « privation relative »[42]. Ce décalage entre les aspirations des Égyptiens et ce qu'ils sont en mesure d'obtenir pour les satisfaire se creuse. La frustration publique et l'impatience envers le régime s'intensifient à mesure que le régime s'ancre dans l'immobilisme alors que Hosni Moubarak prépare la succession de son fils Gamal. Selon Ted Gurr, ce sentiment est une condition nécessaire pour qu'émerge une mobilisation protestataire. Les réseaux sociaux accentuent davantage ce sentiment de privation relative en rendant possible la comparaison avec les autres sociétés internationales plus développées et ouvertes.

---

[39]Faris, David M. « La révolte en réseau : le « printemps arabe » et les médias sociaux », *Politique étrangère*, vol. , no. 1, 2012, pp. 99-109.
[40]Howard, P.N. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam.* Oxford University Press, 2011, p. 145.
[41]Hassan, Hamdy A. "Civil society in Egypt under the Mubarak regime." *Afro Asian Journal of Social Sciences* 2.2.2 (2011).
[42]Gurr, Ted Robert. *Why men rebel* Routledge, 2015.

Ce phénomène favorise la prise de conscience de l'injustice. Selon William Gamson, le sentiment de défiance envers l'autorité est alimenté par un sentiment d'injustice[43]. Non seulement les problèmes politiques, économiques et sociaux doivent être associés à des responsables, mais les groupes militants doivent pouvoir y apporter des solutions. La généralisation de l'accès à Internet ainsi que la bloguisation créent un nouvel espace d'expression public à dominante politique où des citoyens et les militants politiques, en particulier, peuvent exprimer leurs opinions, partager leurs idées et leurs critiques, commenter les problèmes quotidiens et débattre de sujets culturels, sociaux et religieux[44]. En Égypte, il n'existe que 40 blogs en 2004. En 2008, il y en a plus de 160 000[4546]. Ce phénomène de « bloguisation » est déterminant pour faire prendre conscience de l'injustice aux Égyptiens. Les activistes créent des groupes Facebook, des blogs personnels et des comptes Twitter pour mobiliser des partisans et des followers dans des discussions sur les conditions actuelles. Les principaux problèmes politiques soulevés sont la corruption du régime, l'injustice et la brutalité dont fait preuve la police. En résumé, cela marque la transition d'un système médiatique strictement contrôlé et homogène vers un espace médiatique beaucoup plus pluraliste et diversifié.[47]. Comme l'explique le militant Bassem Fathy au lendemain de la révolution : « Nous utilisions Internet depuis dix ans ; c'était le seul espace de liberté que nous avions » [48]. Le gouvernement égyptien s'abstient largement de filtrer les activités sur Internet ou de bloquer des sites Web, préférant faire emprisonner ou harceler quelques blogueurs. Finalement, ces derniers poursuivent tout de même leurs activités.

Les cyberactivistes utilisent cet espace virtuel pour diffuser des informations sur les derniers méfaits du régime de Moubarak. ElBaradei se démarque parmi les figures majeures ayant exploité Internet pour communiquer avec ses partisans et diffuser des informations. En plus de sa page Facebook et de son compte Twitter, des pages Facebook pro-ElBaradei sont créées par l'Association nationale pour le changement et d'autres groupes similaires. De même, Omar Afifi, ancien policier égyptien devenu activiste, joue également un rôle significatif dans la révolution en utilisant les technologies des médias sociaux pour dénoncer les abus policiers.

[43]Gamson, William A. "Constructing social protest." *Social movements and culture*. Routledge, 2013. 85-106.
[44]Atia, Tarek. "Paradox of the free press in Egypt." *USEF Expert Panel Discussion Notes, Washington, DC* (2006).
[45]Freedom House. « Freedom on the net: Egypt ». 2011.
[46]OpenNet Initiative. « Internet filtering in Egypt ». 2009.
[47]Khamis, Sahar & Gold, Paul & Vaughn, Katherine. (2012). Beyond Egypt's "Facebook Revolution" and Syria's "YouTube Uprising:" Comparing Political Contexts, Actors and Communication Strategies. Arab Media & Society. 15.
[48]Faris, David M. « La révolte en réseau : le « printemps arabe » et les médias sociaux », Politique étrangère, vol. , no. 1, 2012, pp. 99-109.

Aussi, les médias sociaux comme YouTube permettent l'émergence du « citoyen-journaliste »[49]. N'importe quelle personne en possession d'un téléphone portable peut capturer ou partager des vidéos et des photos afin de dénoncer les abus du régime. Cette capacité à toucher la population par le biais de preuves accroît la capacité de mobilisation tout en permettant de contourner les médias traditionnels contrôlés par l'État. Ainsi, en 2007, le blogueur Wael Abbas poste une vidéo montrant un homme victime de torture et d'abus sexuel de la part de policiers. Cette vidéo provoque un tel scandale que les autorités sont contraintes d'arrêter et de juger les coupables. Un autre exemple de blog de citoyen-journalisme est celui de Noha Atef, *Torture in Egypt*, qui rassemble des témoignages de victimes de tortures et publie les noms et les portraits des officiers responsables. Cette prise de conscience de l'injustice connaît son point culminant en 2011 lors de la mort de Saïd Khaled relayée en masse sur les réseaux sociaux. Ce jeune homme d'Alexandrie est brutalement tué par deux policiers alors qu'il se trouve dans un cybercafé. Cet événement est d'une grande importance dans le déclenchement des manifestations de janvier 2011.

Section 2 - Le cyberespace comme répertoire d'action au service de l'activisme politique

Selon Charle Tilly : « Utiliser un répertoire d'action collective c'est faire passer un groupe de collection passives d'individus à un participant actif de la vie publique »[50]. De plus, Tilly et Oberschall expliquent que le répertoire d'actions collectives dépend de la structure sociohistorique et du contexte politique alors présent. C'est ainsi que la mobilisation égyptienne s'appuie sur le cyberespace de sorte à en faire un répertoire d'actions propres à ses besoins. Le répertoire d'actions apparaît alors comme central dans cette étude, non seulement parce qu'il est révélateur de la structure socio-politique des réseaux sociaux de l'époque, mais aussi parce qu'il met en exergue le potentiel d'actions qu'a su exploiter l'opposition démocratique pour servir sa lutte politique. En effet, comme évoqué précédemment, l'environnement numérique égyptien est propice aux actions militantes, à la liberté d'expression et à l'organisation de la société civile autour de pôles publics qui n'existent pas dans l'espace politique traditionnel. Par ailleurs, l'utilisation victorieuse du cyberespace

[49]Gillmor, Dan. "We the Media: The Rise of Citizen Journalist." *Nat'l Civic Rev.* 93 (2004): 58.
[50]Tilly, Charles. "Social movements and national politics." (1979). p.69.

comme un outil au service des aspirations démocratiques, démontre l'inappétence du régime pour son *cyber state capability,* tandis que les cybermilitants exploitent ce milieu de sorte à en faire une ressource.

Le monde politique et l'agora, comme lieu de débat et de médiation avec le pouvoir, restent cadenassés par le régime. Parallèlement, la liberté d'expression se fait plus ouverte sur l'espace numérique. Par l'effet des vases communicants, les actions militantes migrent vers ce nouveau lieu. Ce mouvement s'accompagne d'une repolarisation de la direction des manifestations des partis politiques vers les réseaux sociaux comme le souligne les manifestations du pain de 2008. L'action militante se nourrit désormais des ressources que lui lègue le cyberespace. Parmi elle, le cyberespace devient une ressource de capitalisation des connaissances en se nourrissant des expériences passées ou ayant cours dans le monde. Les meneurs du Mouvement du 6 Avril commencent à étudier les luttes non-violentes et à confectionner leur logo en s'inspirant des mouvements de jeunes Serbes. En 2008, le militant égyptien Ahmed Afifi publie un ouvrage destiné à conseiller les Égyptiens sur les moyens d'éviter la brutalité policière. Cet ouvrage est interdit mais Afifi utilise les technologies des médias sociaux pour continuer à transmettre ses conseils aux Égyptiens, notamment via des vidéos sur Facebook et Twitter. Lors des révoltes tunisiennes, il diffuse une série de vidéos détaillées sur YouTube, fournissant des instructions précises aux Égyptiens sur les techniques de révolte. Il spécifie de nombreux détails, tels que la date exacte de l'insurrection, les lieux de rassemblement des manifestants et les vêtements à porter.

En s'inspirant des expériences internationales passées, notamment en Tunisie, les activistes égyptiens capitalisent sur ces enseignements[51]. Lorsque la révolution égyptienne a débuté le 25 janvier, des activistes publient des messages sur leurs blogs et leurs pages Facebook, relayant les témoignages et conseils provenant des manifestations tunisiennes. Ces messages contiennent des mots d'encouragement ainsi que des instructions détaillées et des suggestions basées sur les leçons tirées des événements en Tunisie. Parmi ces conseils, les protestataires tunisiens recommandent à leurs homologues égyptiens de manifester la nuit pour assurer leur sécurité ; d'éviter les actions suicidaires ; d'utiliser les médias pour diffuser leur message afin de susciter une pression internationale ; de peindre en noir les véhicules blindés des forces de

[51]Faris, David M. « La révolte en réseau : le « printemps arabe » et les médias sociaux », *Politique étrangère*, vol. , no. 1, 2012, pp. 99-109.

sécurité pour obstruer le pare-brise ; et de se laver le visage avec du Coca-Cola pour atténuer les effets des gaz lacrymogènes[52].

Enfin, les réseaux sociaux introduisent une rapidité et une interactivité qui font défaut dans les techniques traditionnelles de mobilisation[53]. En effet, l'échange en temps réel d'informations devient plus courant. Lors des rassemblements, les manifestants peuvent communiquer rapidement sur leur situation actuelle. Alors que traditionnellement il aurait fallu envoyer un fax, passer un appel téléphonique ou transmettre des informations par l'intermédiaire d'un messager pour obtenir de l'aide, de nombreux activistes égyptiens réduisent les délais de réponse et augmentent ainsi leur sécurité personnelle en utilisant des téléphones portables pour envoyer immédiatement des « tweets de SOS »[54].

En somme, l'utilisation simultanée et coordonnée de ces différents types de médias sociaux crée un réseau de communication robuste, devenant ainsi difficile à perturber[55]. Le cyberespace égyptien se structure autour d'une mobilisation démocratique à tel point que chaque réseau social joue un rôle distinct et complémentaire pendant la révolution de 2011. Par exemple, Facebook se révèle efficace pour trouver des personnes partageant des opinions politiques similaires et planifier des manifestations de rue. YouTube, quant à lui, promeut le journalisme-citoyen en diffusant des vidéos ou photos reprises ensuite par les chaînes de télévision par satellite et vues à l'échelle mondiale. Le service de messagerie courte (SMS) et Twitter facilitent la coordination et la communication en temps réel. De plus, Twitter a été utilisé pour sensibiliser les médias internationaux et les communautés diasporiques. L'accès généralisé et facile à ces outils de communication en ligne pose de nouveaux défis menaçants pour les régimes autocratiques et leurs médias censurés. Sous l'impulsion des cybermilitants, le cyberespace se restructure en un champ de bataille politique.

[52]Eltantawy, Nahed, and Julie B. Wiest. "The Arab spring| Social media in the Egyptian revolution: reconsidering resource mobilization theory." *International journal of communication* 5 (2011): 18.
[53]*Ibid.*
[54]Khamis, Sahar & Gold, Paul & Vaughn, Katherine. (2012). Beyond Egypt's "Facebook Revolution" and Syria's "YouTube Uprising:" Comparing Political Contexts, Actors and Communication Strategies. Arab Media & Society. 15.
[55]*Ibid.*

PARTIE II – LA RESTRUCTURATION DU CYBERESPACE COMME CHAMP DE BATAILLE : CHUTE DE L'AUTORITARISME ET ÉCHEC DU CYBERACTIVISME

La situation de l'opposition dans le cyberespace se révèle avantageuse, tandis que le régime peine à élaborer une stratégie efficace de lutte politique. Lorsque le cyberespace devient un champ de bataille informationnel, l'État échoue logiquement à atteindre ses objectifs stratégiques (1). Cela conduit à la victoire de l'opposition, confirmant ainsi la nature démocratique de cet outil. Cependant, cette victoire marque paradoxalement la fin du monopole de l'opposition démocratique sur le cyberespace, en raison d'une évolution structurelle majeure (2).

CHAPITRE 1 – LE REGIME AU SEIN DU CHAMP DE BATAILLE CYBER : LIEU DE CONFRONTATION NON-MAITRISE

Le régime de Mubarak s'engouffre malgré lui dans une bataille au sein d'un cyberespace qu'il ne maîtrise pas. L'enjeu principal de manipulation de l'incertitude n'est pas atteint en raison d'une pauvreté des modes opératoires de l'État dans le milieu cyber (1). Cela le déstabilise davantage d'autant plus qu'il évolue dans un environnement hostile où le soutien se dirige vers l'opposition (2).

Section 1 - La bataille pour la maîtrise de l'incertitude : un État dépassé

Durant les Printemps arabes, l'Égypte ne connaît pas de situation de guerre civile à l'instar de la Syrie ou de la Libye. Le pays connaît une vague de manifestations pacifiques et l'État ne la réprime pas par la violence armée. Cette situation se transpose dans le cyberespace. Là où la

Syrie et la Libye connaissent une « cyberguerre » dont l'enjeu est la poursuite des activités guerrière dans le monde physique, l'Égypte s'engage dans une lutte purement informationnelle[56]. Selon la définition de François-Bernard Huygue, la guerre informationnelle constitue « l'ensemble des méthodes visant à infliger un dommage à un rival ou à se garantir une supériorité par l'acquisition d'informations (données ou connaissances), par la dégradation de celle de l'adversaire ou par la propagation de messages favorables à ses desseins stratégiques »[57]. Elle peut être présente sur le cyberespace comme le suggère dès 1994 Winn Schwartau qui considère que les véritables enjeux de la guerre informationnelle se retrouvent dans le cyberespace. Il est alors question d'utiliser l'information et les SI comme des armes pour atteindre ces mêmes cibles adverses[58]. En Égypte, la cyberguerre se manifeste donc par la surveillance, l'identification des utilisateurs du réseau, la désinformation et la propagande.

Au sein de la cyberguerre informationnelle égyptienne se dessine un enjeu capital : « la manipulation de l'incertitude »**.** Elle apparaît comme la clef du changement politique autant pour le régime que pour l'opposition. Les objectifs sont donc de minimiser ou gérer sa propre incertitude et maximiser ou exploiter l'incertitude de ses adversaires.[59]. Dans cette lutte, le régime se fait surpasser en raison de la pauvreté de son mode opératoire. Une logique de surveillance et contre-surveillance s'engage entre les deux parties. Depuis 2008, les cybermilitants sont de plus en plus surveillés via Facebook et les services de téléphones portables[60]. L'État arrête 22 militants liés au soulèvement de 2008 en demandant à la société de télécommunication égyptienne Vodafone de transmettre ses données téléphoniques. La police parvient ainsi à tracer la localisation des manifestants et à procéder à des arrestations préventives. Malgré cela, l'opposition réussit à contourner ces logiques de surveillance ce qui les rend inopérantes en 2011. Leur méthode passe par l'utilisation de réseaux protégés via des VPN ou des messageries cryptées. L'État se retrouve dépassé face à ces techniques qu'il ne peut neutraliser faute de maîtriser l'environnement réseau national.

---

[56]Cepoi, Ecaterina. "Cyber components value in moderne conflicts. An overview on the Syrian conflict and the latest Egyptian uprising." *International Scientific Conference" Strategies XXI"*. " Carol I" National Defence University, 2013.
[57]Huyghe, François-Bernard. « Désinformation : armes du faux, lutte et chaos dans la société de l'information », *Sécurité globale*, vol. 6, no. 2, 2016, pp. 63-72.
[58]Boyer, Bertrand. « Le cyberespace : la nouvelle frontière de la guerre de l'information », Stéphane Taillat éd., *La Cyberdéfense. Politique de l'espace numérique.* Armand Colin, 2023, pp. 244-253.
[59]Hassib, Bassant, and James Shires. "Manipulating Uncertainty: Cybersecurity Politics in Egypt." *Journal of Cybersecurity*, vol. 7, no. 1, 2021
[60]OpenNet Initiative. « Internet filtering in Egypt ». 2009.

Il se tourne donc vers les contrôles dans le monde physique. Les appareils des militants sont confisqués et inspectés lors des manifestations. Ce retour aux méthodes de surveillance traditionnelles sonne comme un aveu d'échec. Inadaptées aux enjeux de l'information sur les réseaux, ces méthodes n'aboutissent à rien car l'information circule avant tout sur le cyberespace. Sans moyen de contrôler ou de neutraliser cette information, elle reste libre. D'autant plus que la fouille physique rencontre ses propres limites. Les manifestants se déplacent sans leurs appareils évitant ainsi qu'ils tombent entre les mains de la police. Certains utilisent plusieurs faux comptes Facebook afin de brouiller les pistes quant à leur affiliation politique. Ces pratiques de contre-surveillance ont accru l'incertitude du gouvernement quant à savoir où et quand l'activité politique aurait lieu, rendant plus difficile toute action préventive visant à la supprimer.[61].

L'État n'a que très peu de moyen de contourner la contre-surveillance. Cela s'explique par sa faible maîtrise du contenu présent sur les réseaux. La seule option restante est l'action sur la couche physique du cyberespace. Celle-ci touche à son paroxysme lorsque le dirigeant Mubarak décide de couper Twitter, Facebook et les communications mobiles dans tout le pays. Les services Internet sont fermés et, le 31 janvier, tout accès à Internet est bloqué. Cette fermeture est permise par la relation entre l'État et les principaux FAI encadrée par loi sur les télécommunications de 2003. Cette technique s'apparente à une réduction de l'espace, créant ainsi une plus grande incertitude chez l'opposition, mais par la même occasion privant le régime d'une source d'information[62]. Le calcul de l'État semble favorable compte tenu de son incapacité à extraire du cyberespace des informations pour la lutte informationnelle. Cependant, cette décision n'a pas l'effet escompté. En effet, la coupure des réseaux entraîne une augmentation du nombre de personnes descendant dans la rue, obligées de quitter leur domicile pour comprendre ce qui se passe [63]. Le black-out d'Internet et des téléphones portables pousse de nombreux Égyptiens ordinaires, inquiets de l'absence de nouvelles de leurs familles et amis et redoutant des massacres imminents par les forces de sécurité, à quitter précipitamment leurs maisons pour se rassembler dans les rues et les places de la ville afin de se protéger mutuellement[64]. Les coupures de communication offensent également de

[61]Hassib, Bassant, and James Shires. "Manipulating Uncertainty: Cybersecurity Politics in Egypt." *Journal of Cybersecurity*, vol. 7, no. 1, 2021

[62]Thompson, Karson K. "Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate." *Texas Law Review*, vol. 90, 2011, pp. 465.

[63]Christensen, Britt. "Cyber State Capacity: A Model of Authoritarian Durability, ICTs, and Emerging Media." *Government Information Quarterly*, vol. 36, no. 3, July 2019, pp. 460-468.

[64]Khamis, Sahar, Paul Gold, and Katherine Vaughn. "Beyond Egypt's 'Facebook Revolution' and Syria's 'YouTube Uprising:' Comparing Political Contexts, Actors and Communication Strategies." *Arab Media & Society*, vol. 15, 2012.

nombreux Égyptiens, qui, comme l'explique Adel Iskandar, « sont devenus plus déterminés [à se révolter], car ils ont refusé la tentative du gouvernement de les infantiliser. Leur message au régime était : L'Égypte ne peut pas être bloquée et son peuple ne peut pas être déconnecté »[65]. De plus, la coupure des réseaux génère un coût de 110 millions de dollars à l'économie égyptienne[66]. Cette baisse de revenu entraîne un défaut de légitimité pour le régime. Le pouvoir infrastructurel, basé entre autres sur le gain économique, s'en voit ébranlé. En définitive, cette décision intervient tardivement et s'avère inefficace. Les informations circulaient depuis des années dans le cyberespace, et les images du soulèvement tunisien avaient déjà marqué les esprits.

Section 2 - Le régime dans un milieu hostile : l'absence de soutien non-étatique

L'État perd la bataille informationnelle en partie parce qu'il ne bénéficie pas du soutien d'acteurs non-étatiques influents. Or, ces derniers ont un immense pouvoir de diffusion de l'information et de création de discours. Ils représentent donc un énorme potentiel. L'État n'a pas su s'appuyer sur eux pour faire valoir ses idées[67]. Ce manque de soutien se ressent dans l'échec du régime à transmettre sa propagande sur un terrain hostile qu'il ne contrôle pas. Le régime tente pourtant de créer un discours contre-révolutionnaire pour contrecarrer les manifestations. La société Vodafone a diffusé des messages texte pro-régime tels que « Oui à la stabilité », « Protégeons l'Égypte » et « Travaillons ensemble contre l'agitation ». Néanmoins ces tentatives s'avèrent infructueuses en raison d'une trop forte présence d'acteurs soutenant l'opposition [68].

En Syrie et en Arabie Saoudite, les groupe de propagandes pro-régimes non-affiliés sont des acteurs déterminants dans la consolidation de la légitimité du pouvoir. Dans le contexte syrien, l'Armée électronique syrienne (SEA), une équipe d'attaque informatique soutenue par le régime, combat les messages anti-régime de multiples façons. Par exemple, elle pirate,

[65]I Iskandar, Adel. "The Baltageya: Egypt's Counterrevolution." *The Huffington Post*, 2011.
[66]Greenemeier, Larry. "How Was Egypt's Internet Access Shut Off?" *Scientific American*, 28 Jan. 2011.
[67]Abrahams, Alexei, and Andrew Leber. "Electronic Armies or Cyber Knights? The Sources of Pro-Authoritarian Discourse on Middle East Twitter." *International Journal of Communication*, vol. 15, 2021.
[68]Khamis, Sahar, Paul Gold, and Katherine Vaughn. "Beyond Egypt's 'Facebook Revolution' and Syria's 'YouTube Uprising:' Comparing Political Contexts, Actors and Communication Strategies." *Arab Media & Society*, vol. 15, 2012.

perturbe, efface ou ferme des sites Web de l'opposition syrienne et occidentale. Des actions de spamming de commentaires pro-régime sont également menées à l'encontre de pages Facebook populaires rassemblant des militants d'opposition[69]. L'Égypte ne possède pas de « cyberarmée de partisans » comme la Syrie. A l'inverse, les soutiens à l'opposition sont plus importants.

De multiple groupes nationaux et internationaux entreprennent des actions de propagande et de déstabilisation visant le régime. Les figures antirévolutionnaires voient leurs sites Web ciblés. Les « Chevaliers égyptiens » font partie de ces groupes anti-régime agissant depuis l'Égypte. Mais il existe de nombreux autres groupuscules cyber venant de l'étranger et avançant leurs agendas politiques. Anonymous, le collectif de hackeurs international dont le but est de défendre la liberté d'expression, collabore avec Telecomix, un autre collectif afin d'apporter leur soutien aux opposants du régime. Ils fournissent une précieuse aide lors de la coupure d'Internet en accordant des méthodes de communications alternatives comme les fax ou des appareils de communication satellites. Les chaînes de télévisions satellites comme Al Jazeera, la BBC et CNN soutiennent également les militants[70]. Elles publient les images et vidéos captées par les manifestants leur donnant une plus grande résonance à tous les niveaux. En réponse, le régime tente de faire de la propagande en diffusant sur les chaînes de télévision d'État des rassemblements pro-Moubarak, sans succès. Il est important de souligner le rôle des entreprises privées comme Facebook, Google et Twitter. Pour aider les manifestants à communiquer malgré le black-out d'Internet, ces entreprises lancent un logiciel de « voix-texte » permettant aux citoyens de transmettre des messages vocaux en ligne sous forme de textes sur Twitter en utilisant l'hashtag #egypt.[71].

En combinant soutiens étrangers et lacune du mode opératoire étatique, les cybermilitants gagnent la bataille informationnelle. Le régime chute en 18 jours, en partie grâce à leurs actions. Toutefois, l'opposition démocratique victorieuse face au régime échoue à s'imposer dans le paysage post-Mubarak. En cause, la fragmentation du monopole du discours sur le cyberespace ainsi qu'un manque de légitimité.

---

[69]Shehabat, Ahmad. "The Social Media Cyber-War: The Unfolding Events in the Syrian Revolution 2011." *Global Media Journal: Australian Edition*, 2012.
[70]Rinnawi, Khalil. "Cyber Uprising: Al-Jazeera TV Channel and the Egyptian Uprising." *Language and Intercultural Communication*, vol. 12, no. 2, 2012, pp. 118-132.
[71]Arthur, Charles. "Google and Twitter Launch Service Enabling Egyptians to Tweet by Phone." *The Guardian*, 1 Feb. 2011.

CHAPITRE 2 - L'ÉCHEC DE LA TRANSITION DÉMOCRATIQUE OU LE MANQUE DE LÉGITIMITÉ DANS UN UNIVERS FRAGMENTE

La période post-Moubarak marque le début d'une restructuration du cyberespace égyptien. Le cyberactivisme d'opposition démocratique se retrouve en difficulté dans la phase d'influence du monde politique, en cause : un manque de légitimité face à des acteurs traditionnels (1). Parallèlement, le monopole du discours se fragmente à mesure que les acteurs politiques investissent de plus en plus le cyberespace ; s'ensuit une phase de divisions et d'affrontements entre acteurs non-étatiques (2).

Section 1 - L'absence de légitimité et d'influence du cyberactiviste arabe sur le paysage politique post-Mubarak

Après la démission de Mubarak le 11 février 2011, le paysage cyber se restructure en même temps que s'amorce la transition démocratique encadrée par l'armée. Le cyberactivisme de la première heure ne réussit pas, après sa victoire sur le régime, à s'imposer comme un acteur déterminant au sein du monde politique. Là, où le régime n'a pas su investir « la couche virtuelle » du cyberespace, l'opposition n'a pas su convaincre la population égyptienne. A cela s'ajoute une divergence de point de vue quant à la direction politique que doit prendre le pays dans le contexte post-Mubarak. Les aspirations du peuple ne convergent pas avec celles des cybermilitants démocrates. Certes, le cyberactivisme détient le monopole du discours sur les réseaux sociaux. Ainsi, cette situation procure l'impression que la population, dans son entièreté, adhère à leur idéologie, d'autant plus qu'elle les a activement soutenus lors des manifestations. Toutefois, la fracture se ressent lors du référendum sur l'amendement de la constitution, qui a lieu en mars 2011. Alors que les jeunes révolutionnaires arabes, largement plus actifs en ligne, sont plutôt favorables au rejet des amendements et de la Constitution, les électeurs, en grande majorité influencés par des groupes religieusement orientés et beaucoup plus actifs sur le terrain, votent en leur faveur. Cet événement met en lumière que « les points

de vue et les discours qui dominent les espaces Facebook égyptiens ne représentent pas nécessairement la voix politique de la majorité des Égyptiens »[72].

L'influence du cyber activisme démocratique sur l'espace numérique est indéniable. Cependant, le décalage qui existe entre le monde réel et virtuel pose une limite quant à la perméabilité des idées d'un espace à l'autre. Même si la démocratisation d'Internet est une des réussites du régime de Moubarak, l'activité y reste tributaire de la disponibilité des ordinateurs et de l'accès à Internet qui peut être coûteux en cas de connexions fréquentes. Une large partie de la population ne participe pas aux débats, à l'échange d'informations et aux diverses activités en ligne portées par l'opposition démocratique. Les populations les plus vieilles se sentent certes concernées par les problèmes politiques, mais ne participent pas aux activités en ligne. Une grande partie des manifestants ne sont d'ailleurs pas des cyberactivistes et ils ne sont que 17% à posséder une connexion Internet à domicile lors des Printemps arabes. Par ailleurs, le taux d'analphabétisme en Égypte dépasse encore 40%, et la population demeure largement attachée aux médias traditionnels. Un sondage Gallup révèle que seulement 8% des Égyptiens obtiennent leurs informations de Facebook ou Twitter durant les manifestations de janvier et février 2011. En revanche, 63 % des Égyptiens s'informent sur les manifestations via la chaîne satellitaire Al Jazeera. Les médias traditionnels restent donc un moyen privilégié pour la population de s'informer politiquement. La légitimité du discours est par conséquent entre les mains de ces médias détenus par des acteurs politiques tels les Frères musulmans soutenus par le Qatar et la Turquie via la chaîne de Télévision Al Jazeera. Également, entre mars et avril 2011, 81 % des Égyptiens déclarent obtenir leurs nouvelles sur la transition politique du pays à partir de la télévision d'État. De plus, en décembre 2011, 59% des Égyptiens interrogés considèrent les médias d'État comme précis[73]. Ce constat renforce l'hypothèse que les médias et les acteurs traditionnels de la vie politique conservent leur légitimité malgré la forte expansion du cyberactivisme. Conséquemment, le discours de l'opposition démocratique largement actif sur les réseaux, ne réussit pas à s'imposer lors de la transition démocratique du pays. Les cybermilitant réussissent à faire chuter le régime en mobilisant le peuple, mais ne parviennent pas à s'imposer comme des acteurs politiques légitimes propres à prendre en main le pays.

[72]Iskander, Elizabeth. "Connecting the National and the Virtual: Can Facebook Activism Remain Relevant after Egypt's January 25 Uprising?" *International Journal of Communication*, vol. 5, 2011, pp. 1225-1237.
[73]Hellyer, H.A. "Violence and the Egyptian Military." *Foreign Policy*, 2012.

Conséquemment, le cyberactivisme se fait doubler par des partis plus traditionnels et mieux établis comme les Frères musulmans. La disparité entre les espaces en ligne et hors-ligne se manifeste également dans l'incapacité des jeunes cyberactivistes, qui sont la principale force inspiratrice derrière la révolution, à obtenir des gains significatifs lors des élections parlementaires de 2011. Les partis islamistes, tels que le parti al-Hurriya wa al-Adala des Frères musulmans et le parti al-Nour salafiste, tous deux moins actifs sur les réseaux mais beaucoup plus organisés sur le terrain, ont pu remporter 70 % des sièges. C'est une autre indication claire montrant que l'effet d'entraînement des discours en ligne doit encore s'étendre à une base plus large de la société égyptienne avant de pouvoir changer les tendances de l'opinion publique de manière significative ou de façonner efficacement l'avenir du pays[74]. À cela s'ajoute un essoufflement du cyberactivisme arabe des premiers jours. Après la chute de Moubarak, de nombreux cybermilitants adoptent une position de retrait. Épuisés par des années de lutte contre le régime et déçus par l'évolution de la révolution égyptienne et le retour des forces antirévolutionnaires, ils choisissent de se consacrer à leur vie privée ou à leur carrière professionnelle [75]. Ce constat se renforce à mesure que de nouveaux acteurs émergent sur le cyberespace, porteurs de discours novateurs propres à fragmenter le monopole de l'opposition démocratique.

Section 2 - Division et affrontement : la perte du monopole de l'opposition démocratique sur le cyberespace

Le cyberespace se restructure entièrement, faisant perdre à l'opposition démocratique les avantages dont elle bénéficiait initialement. Autrefois espace de contestation unifié contre le régime, il se fragmente désormais. Cette segmentation entraîne la fin d'un monopole : de nouveaux acteurs tels que le régime et les Frères musulmans utilisent le cyberespace comme un outil au service de leurs desseins politiques. Cette restructuration est une conséquence de l'augmentation du nombre d'internautes dans les mois qui suivent la chute de Hosni

[74]Khamis, Sahar, Paul B. Gold, and Katherine Vaughn. "Beyond Egypt's 'Facebook Revolution' and Syria's 'YouTube Uprising': Comparing Political Contexts, Actors and Communication Strategies." *Arab Media & Society*, vol. 15, Spring 2012, pp. 1-30.
[75]De Angelis, Enrico. "L'espace politique virtuel avant et après la chute de Moubarak: une critique des réseaux sociaux digitaux en Egypte." *Égypte/Monde arabe* 12 (2015): 195-227.

Moubarak. En Égypte, Facebook passe d'un peu moins de 5 millions d'utilisateurs fin 2010, à plus de 14 millions à la mi-2013. Eu égard à cet accroissement, l'expression des orientations politiques se diversifie. Une plus large partie de la population, exclue jusqu'alors de la « cyber vie politique », influe sur les activités en ligne créant ou alimentant des groupes d'obédiences idéologiques variées.

Conséquemment, le monopole de l'opposition démocratique laisse place à une multipolarité politique. En effet, l'arrivée d'acteurs plus traditionnels amorce une évolution structurelle majeure. Les mouvements révolutionnaires égyptiens ne sont plus les seuls à utiliser le web comme un instrument de lutte politique. D'autres groupes et organisations se réapproprient, parfois en les améliorant, les techniques et les pratiques de l'activisme en ligne. Si la toile fournit un « répertoire d'actions collectives » ce même répertoire, après la chute de Moubarak, devient accessible à d'autres acteurs politiques potentiellement « non démocratiques ». Tant et si bien que de nombreux activistes démocrates trouvent extrêmement difficile de se poser en alternative aux Frères Musulmans d'une part, et aux militaires ainsi qu'aux représentants de l'ancien régime d'autre part. Le Haut Conseil des Forces Armées, l'institution politique représentant l'ancienne élite politique elle-même en charge de la transition démocratique, est la première à ouvrir sa propre page Facebook, où nouvelles et décisions sont publiées avant même d'apparaître dans les médias traditionnels. Ainsi, « le consensus diffus contre le régime » s'estompe peu à peu pour laisser place aux affrontements idéologiques entre partis démocrates, salafistes, fréristes et pro-régimes[76]. Le cyberespace n'est plus structuré par l'opposition entre un régime impopulaire et le mécontentement populaire porté par des militants démocrates. Cet espace est sorti de « ce récit anti-hégémonie unique »[77] pour entrer dans un milieu de débat politique où la seule contestation ne compte plus.

Au point que le cyberespace perd de sa virginité politique. En effet, le consensus contre le régime n'était pas alimenté par une idéologie définie. Il demeurait flou de sorte à devenir large justement afin d'englober tous les pans de la population. Dès la chute du régime, il disparaît et devient un problème pour la recherche du consensus nécessaire au processus démocratique. Or, il est important d'en apporter un dans le contexte où toute la population n'est pas en phase idéologiquement parlant avec les cyberactivistes. Cette recherche de consensus à propos de la voie démocratique à adopter amène à une confrontation entre les

[76] *Ibid*
[77] *Ibid*

acteurs parfois violente sur le cyberespace. Il n'est plus question d'un espace, certes restreint numériquement mais où le dialogue est permis, mais plutôt d'un espace de confrontation extrême englobant une large partie de la population. L'agora devient une arène bloquant le caractère unitaire et consensuel du cyberespace ayant fait la force de l'opposition démocratique[78].

La continuation du champ de bataille idéologique durant la période post-Mubarak dans un contexte de multipolarité des acteurs politiques amène à la segmentation du cyberespace. Les internautes se rassemblent en cercle clos au sein de forums, de pages Facebook, de blogs et de comptes Twitter. Les réseaux sociaux favorisent la formation de ce que Sunstein appelle des « caisses de résonance pour gens du même avis » (*echo-chambers of like-minded people*)[79]. Le cyberespace n'est plus dominé uniquement par l'ancienne opposition. De fait, il continue à être un champ de bataille d'autant plus virulent que de nouveaux acteurs l'investissent avec de nouvelles méthodes. Les Frères musulmans, les partisans de l'ancien régime et les groupes salafistes, possèdent tous leurs pages Facebook et leur compte Twitter. Chacun est suivi par un grand nombre de citoyens égyptiens. Le cyberespace se peuple alors d'îlots idéologiques avec à sa tête des représentants tels que des influenceurs ou des hommes politiques que Enrico De Angelis définit comme « des micro-célébrités »[80]. Cette tendance s'accentue naturellement avec l'arrivée de millions de citoyens sur les réseaux. Au cœur de cette nouvelle bataille, la vieille élite tire les leçons de ses erreurs passées. En reprenant les armes de ses ennemis, elle réussit à revenir au pouvoir. De là, une nouvelle stratégie cyber s'amorce dont la fin est l'écrasement de toute opposition interne par la numérisation de son autoritarisme.

[78]Gonzalez-Quijano, Yves. "Internet, le «Printemps arabe» et la dévaluation du cyberactivisme arabe." *Égypte/Monde arabe*, no. 12, 2015, pp. 67-84.
[79]Sunstein, Cass R. *Republic.com 2.0*. Princeton University Press, 2007.
[80]De Angelis, Enrico. "L'espace politique virtuel avant et après la chute de Moubarak: une critique des réseaux sociaux digitaux en Egypte." *Égypte/Monde arabe* 12 (2015): 195-227.

PARTIE III – LA NUMÉRISATION DE L'AUTORITARISME ÉGYPTIEN

En 2013, la junte militaire reprend le pouvoir sous la coupe du maréchal Abdel Fatah Al-Sissi. Cette période marque le début de la numérisation de l'autoritarisme égyptien. Ce faisant, ce dernier devient un outil au service du régime. Le cybercontrôle est assuré par une étatisation du cyberespace national à travers une série de lois sécuritaires et la transposition de la violence étatique dans le domaine cyber (1). Mais il se traduit également par la transposition des méthodes autoritaire du monde physique vers le monde virtuel, notamment à travers une surveillance de masse et le contrôle de l'opinion publique (2).

CHAPITRE 1 – L'ETATISATION DU CYBERESPACE EGYPTIEN

Le régime d'Al-Sissi opère un changement structurel dans le cyberespace égyptien. En effet, l'État tente de s'y imposer comme la seule force régulatrice. Un processus d'étatisation du cyberespace prend forme dans le sens wébérien d'une mise en administration de la société. Ce processus se manifeste par l'avancée et la construction d'une sphère publique, contrôlée par l'État au détriment de la sphère privée. En Égypte, l'étatisation passe en premier lieu par la légitimation du cybercontrôle par sous-prétextes d'impératifs sécuritaires (1). Puis elle se réalise par la numérisation des méthodes répressives du régime, monopole de l'État, qui institue la violence étatique sur un espace où celle-ci ne possède, sous sa forme traditionnelle, aucune efficience (2).

Section 1 - Imposer le monopole de la cyberviolence légale et légitime

Le cyberespace est un immense champ de bataille informationnel et idéologique entre divers groupes d'activistes. Il existe donc une situation d'anarchie où aucune entité ne semble

prendre le rôle d'un organe régulateur et légitime. C'est dans ce contexte que s'amorce le processus d'étatisation du cyberespace égyptien. Historiquement, l'étatisation se matérialise par l'établissement d'un monopole de la violence légale[81]. Il est alors question d'utiliser la loi pour légitimer et encadrer l'usage de l'action répressive qu'elle soit policière ou armée. Le régime d'Al-Sissi s'appuie donc sur la popularité dont il jouit les premières années pour imposer ses lois sur le cyberespace. En 2013, l'Égypte est traversée par un sentiment d'hyper-patriotisme et d'anti-islamisme dû à la présidence de Mohammed Morsi, chef du parti politique des Frères Musulmans. Cette période est synonyme de trahison de l'élite politique envers le peuple, les engagements démocratiques se sont effacés derrières des considérations islamiques dans cette « illusion de l'électoralisme » fondant le sentiment de légitimité du pouvoir sur la simple victoire électorale[82]. Les groupes armées djihadistes du Sinaï se sont développés sous le regard approbateur du Président, accroissant ainsi l'instabilité régionale dont se veut pourtant garante l'Égypte. Ce sentiment anti-fréristе est alimenté par les chaînes de propagande du Conseil suprême des Forces armées (CSFA), l'institution militaire assurant la transition démocratique dès février 2011. Consciente de la force du cyberespace dans la lutte informationnelle, le CSFA ouvre sa page Facebook le 17 février 2011 afin d'y publier ses bulletins officiels[83]. Par le biais de nombreux organes de presse et des médias, les messages du CSAF sont relayés sur de nombreux réseaux sociaux. L'opinion publique est façonnée pour percevoir l'activisme civique comme un acte antipatriotique lié aux mouvements islamistes ou étrangers et qui entrave les actions sécuritaires antiterroristes du gouvernement[84].

Une phase importante de propagande pro-régime s'engage entre 2011 et 2013 afin de préparer la chute de Morsi. Les manifestations pilotées par l'armée en juin 2013 sont accompagnées de déclarations proclamant la guerre à « l'extrémisme » et au « terrorisme ». De ce fait, l'armée fait valoir la sécurisation au centre du débat public, c'est-à-dire mettre au centre des politiques publiques la problématique posée par une menace portant atteinte à la survie de la nation pour légitimer ses mesures législatives. Les médias ainsi que les réseaux sociaux sont désignés comme des vecteurs de danger. Cette rhétorique trouve un écho favorable au sein de la population. La chute de Morsi est accompagnée par une féroce campagne de lutte contre les

[81]Weber, Max. *Le savant et le politique*. Union Générale d'Édition., 1919

[82]Schmitter, Philippe C., and Terry Lynn Karl. "What Democracy Is. . .and Is Not." *Journal of Democracy*, vol. 2, 1991, pp. 75–88.

[83]Khamis, Sahar, et al. "Beyond Egypt's 'Facebook Revolution' and Syria's 'YouTube Uprising': Comparing Political Contexts, Actors and Communication Strategies." *Arab Media & Society*, vol. 15, spring 2012, pp. 1-30.

[84]Hassib, B. "Egypt's Counter-Terrorism Policy Post 9/11 and Beyond: Shrinking Civic Space." *Terrorism and Civil Society: Post-9/11 Progress and Challenges*, edited by Romaniuk SN, Mullins S, Ruteere M, Manchester University Press, 2020.

dissidents politiques et en premier lieu contre les islamistes. Les manifestations démocratiques défendant le régime en place malgré ses déboires sont rapidement assimilées à des mobilisations pro-terroristes dirigées par les ennemis de l'État[85].

L'État, de nouveau entre les mains de la junte militaire, se sert du sentiment anti-islamiste et anti-terroriste pour adopter toute une série de lois répressives venant réguler la liberté d'expression sur le cyberespace. Il est vrai que le cyberterrorisme est un phénomène prenant de l'ampleur dès le début des années 2000. Les réseaux de djihadistes partagent de nombreuses informations comme des tutoriels ou des guides dans le but de commettre des attentats[86]. Les réseaux sociaux sont aussi une importante caisse de résonance pour leur idéologie à l'instar des mouvement démocratiques arabes.

Néanmoins, le régime envisage avant tout de réprimer plus globalement tous les mouvements politiques d'opposition. C'est pourquoi les textes de lois restent assez flous sur la définition du « terrorisme ». La loi 94 anti-terroriste de 2015 use de définition tautologique pour désigner ce qu'est un acte terroriste. Elle stipule ainsi que les crimes de nature terroriste sont « Toute infraction prévue par la présente loi et tout crime ou délit commis en utilisant un moyen de terrorisme ou en vue de réaliser ou de commettre un acte terroriste »[87]. A titre de comparaison, l'État français dans La loi n° 86-1020 du 9 septembre 1986 relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État définit le terrorisme dans son Article 1 comme « des infractions en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur ». Cette définition possède elle aussi des lacunes dans le sens où il est difficile de fonder une notion juridico-politique sur un état émotionnel : « la terreur »[88]. Cependant, elle reste bien plus précise que le concept égyptien de terrorisme. En entretenant un brouillard sémantique et en conservant le caractère inhérent à cette notion « à définition introuvable »[89], le régime tente d'englober sous ce terme de nombreuses activités en ligne. Concrètement, le discours politique n'est pas anti-terrorisme mais anti-démocratique. Ce constat se renforce avec l'article 18 de la même loi qui affirme que « Quiconque tente par la force, la violence, la menace, l'intimidation, ou un autre

[85]Abozaid, Ahmed M. "Digital Baltaga: How Cyber Technology Has Consolidated Authoritarianism in Egypt." *SAIS Review of International Affairs*, vol. 42, no. 2, 2022, pp. 5-19.
[86]Hecker, Marc, and Élie Tenenbaum. *La Guerre de Vingt Ans: Djihadisme et Contre-Terrorisme au XXIe Siècle*. Robert Laffont, 2022.
[87]Arab Republic of Egypt. "Article 1 Law No. 94/2015 on Anti-Terrorism."
[88]Cumin, David. "Pour une Définition Objective du Terrorisme à l'Aide des Critères de la Polémologie et du Droit des Conflits Armés." In Bourgou, T., & Chabbi, M. (Eds.), *Regards Croisés dans l'Après-11 Septembre*, l'Harmattan, 2011, pp. 63-102.
[89]*Ibid*

moyen d'actes terroristes de renverser le régime ou de changer la Constitution de l'État, son système républicain, ou la forme de gouvernement sera puni d'emprisonnement à vie ou d'emprisonnement avec travaux forcés pour une durée de pas moins de dix ans ». De plus plusieurs tentatives visant à classer l'hacktivisme parmi les menaces persistantes avancées (APT) sont portées par le régime plaçant ainsi l'activisme politique en tête des priorités en matière de cybersécurité. Cette régulation étatique se justifie par comparaison avec les efforts des autres pays qui luttent contre le cyberterrorisme. La Chine et les États-Unis sont mis en avant comme des États ayant adopté un cadre de cybersécurité combattant l'extrémisme. Au niveau régional, en 2017 est lancé un Centre mondial de lutte contre l'idéologie extrémiste, baptisé Etidal. Cette initiative est portée par le régime saoudien, égyptien et les États-Unis. Elle renforce la légitimité des mesures de contrôle prise par Al-Sissi à l'échelle mondiale. Le régime s'appuie sur ses partenaires pour combattre les mouvements politiques d'opposition sur les réseaux sociaux.

Le discours ambiant est alors à la répression et à la pénalisation des partis d'opposition démocratiques et islamiques. Toute une série de lois normalisent la violation des libertés et l'oppression de l'opposition sur le cyberespace[90]. Cette légitimation s'accompagne d'une socialisation des moyens de domination caractéristiques du processus d'étatisation[91]. Ainsi, la stratégie nationale égyptienne en matière de TIC de 2014-2017 affirme que certains articles de loi de 2003 rentrent en contradiction avec les idéaux de la transition démocratique porteurs de la liberté d'expression et du droit à la vie privé. En affirmant cela, le régime se dote d'une légitimité continuatrice, c'est-à-dire s'inscrivant dans le cheminement politico-historique de l'Égypte post-Mubarak. Les idéaux démocratiques sont réaffirmés, mais d'un autre côté les nouveaux objectifs sécuritaires ne considèrent pas la disponibilité d'informations comme pouvant nuire à la sécurité nationale de l'Égypte de même que l'ingérence étrangère, sous la bannière de la liberté, devient acceptable. Al-Sissi jongle donc entre une large définition de la sécurité nationale et un adoubement abstrait des droits de l'Homme. Cette stratégie rhétorique permet de conserver une certaine aura démocratique tout en avançant l'étatisation du cyberespace national, processus qui accroît la sphère publique sous la domination de l'État et sa loi, le tout au détriment de la sphère privée.

Conséquemment, l'État s'impose comme un acteur légitime de régulation du contenu sur les réseaux. De cette façon, en 2014, le gouvernement institue le Conseil suprême de

[90]Abozaid, Ahmed M. "Digital Baltaga: How Cyber Technology Has Consolidated Authoritarianism in Egypt." *SAIS Review of International Affairs*, vol. 42, no. 2, 2022, pp. 5-19.
[91]Fayat, Hervé. "ÉTAT, sociologie." *Encyclopædia Universalis*, 8 septembre 2015.

cybersécurité, un comité en charge de surveiller le cyberespace pour détecter toute opinion publique « déviante » et tout contenu « terroriste ». Toujours dans une logique de légitimation ce comité est décrit comme un outil venant compléter les opérations militaires dans le Sinaï afin de lutter contre l'extrémisme en ligne. De même, la loi de 2016 sur la régulation de la presse et des médias autorise le Conseil suprême de régulation des médias (CSRM) à contrôler le contenu des médias numériques et à les bloquer si l'éthique publique et la sécurité nationale sont menacées[92]. Certains médias sont systématiquement censurés sur les réseaux. La loi sur les ingérences étrangères légitime cette pratique faisant passer des médias occidentaux, des ONG ou bien des médias islamistes, comme Al-Jazeera, pour des éléments menaçant la sécurité interne du pays. Si bien que, plusieurs ONG promouvant les droits de l'homme sont ciblées en 2017 par l'État à la suite de la révélation de financements étrangers n'ayant pas été autorisés. L'arsenal juridique mis en place permet à l'État de réprimer légalement les activités sur le cyberespace. Ce faisant, il tente de s'imposer comme le seul organe légitime contrôlant le contenu et les comportements transitant sur les réseaux numériques. Cette étatisation du cyberespace national s'accompagne alors d'une numérisation des actes de répression ce qui ancre davantage le régime dans ce milieu.

Section 2 – La numérisation des pratiques violentes et répressives du régime

Le processus d'étatisation est lié à la monopolisation des moyens de coercition[93]. Dans le cas égyptien, la violence d'État est spécifique au régime autoritaire. La répression comme mode de gouvernance lui est intrinsèque. Elle lui sert à transformer les personnes en sujets impuissants sans capacité à parler et à agir ensemble[94]. En Égypte elle se manifeste par les actions de la police, mais aussi par des milices pro-gouvernementales nommées « baltagiya » (البلطجية). Dans les pays arabes, ces groupes sont assez répandus. Ils désignent des bandes de criminels, de délinquants et d'anciens prisonniers mis au service de l'État. La police sous-traite à ces réseaux des tâches de répressions politiques. Ces bandes sont formées au maniement des armes et utilisées pour faire pression notamment lors d'élections. Leurs

[92]Egyptian Supreme Council for Media Regulation. "Law No. 180 of 2018 on Regulating the Press, Media, and the Supreme Council for Media Regulation." 2018.
[93]Elias, Norbert. *Le Processus de Civilisation*. Calmann-Lévy, 1973.
[94]Linz, Juan. *Totalitarian and Authoritarian Regimes*. Rienner, 2000.

actions sont assez variées et elles se manifestent par des actes d'intimidation, des passages à tabac, des assassinats ou des viols. Entre les années 1980 et 1990, leur brutalité se dirige principalement vers les groupes islamistes pour ensuite se tourner vers les mouvements démocratiques en 2011. Mais leur utilisation ne permet pas d'empêcher le renversement du régime. Pour cause, l'activité politique est passée du monde physique aux réseaux sociaux. Or sur ces derniers, la violence d'État n'a que très peu fonctionné.

L'objectif central de l'État autoritaire à l'ère des réseaux sociaux est alors de contrôler l'information, les images et les idées circulant sur la toile afin de les dépolitiser. Dans un premier temps, l'Égypte échoue en raison d'une numérisation trop faible de son système de répression et de surveillance. Les seules actions répressives sont exercées sur la « couche physique » comme l'utilisation de la baltagiya et la coupure d'Internet. Celles-ci sont pourtant lourdes de conséquences car elles endommagent l'économie tout en ravivant les manifestations. En réalité, sous Mubarak, les méthodes de coercitions virtuelles n'existent pas, ou alors sous des formes incomplètes. Principalement le régime surveille et espionne des individus ciblés. La violence étatique sous sa forme traditionnelle, la baltagiya, est difficilement transposable sur le cyberespace. En effet, sa fonction première est d'imposer la domination directe de l'État sur des individus. Or, sur le cyberespace l'organisation sociale se base sur des relations et des connexions entre individus au sein de réseaux numériques[95]. La domination sur les personnes par la violence physique directe n'est donc pas possible. De plus, les utilisateurs peuvent être hors d'atteinte de l'État s'ils opèrent depuis un pays étranger. Les cyberactivistes s'organisent autour de structures transnationales dépassant le cadre de la souveraineté étatique. Le système de baltagiya apparaît alors dépassé. L'enjeu demeure donc le contrôle de l'information dans la logique de la cyber guerre informationnelle.

Les autorités égyptiennes perdent cette bataille durant les Printemps arabes. La perte de contrôle sur l'information, les oblige à durcir leur méthode autoritaire sur le cyberespace[96]. Ainsi, le régime d'Al-Sissi se donne comme objectif d'imposer, comme dans le monde réel, l'autocensure, la dénonciation, le blocage et l'intimidation. L'État opte ainsi pour la numérisation de la baltagiya avec pour objectif de répondre à la dissidence sur les réseaux sociaux tout en l'étouffant sans avoir à exercer une violence physique comme s'était résigné à

[95]Kempf, Astrid. "Pour une Sociologie du Cyberespace." *Revue Défense Nationale*, vol. 785, no. 10, 2015, pp. 77-82.
[96]Loudiy, Fadoua, and Andrew R. Smith. "Cyber-baltagiya in Morocco: A Critical Rhetorical Analysis." *Revue Langues et Littératures*, vol. 24, 2015, pp. 1-27.

le faire Mubarak[97]. De facto, l'État se repose sur des groupes de sympathisants pro-régimes ou bien des cybercriminels à la recherche de gains. Leurs actions se décomposent en trois grandes catégories : le blocage ou le sabotage de sites web ; la désinformation et la propagande ; l'intimidation et le harcèlement.

Les techniques utilisées dans la rue par la baltagiya trouvent leur forme numérique. Ainsi, la violence physique devient symbolique. Les usines à troll[98] sont utilisées pour décrédibiliser les idéologies, les groupes et les personnes dans le but de manipuler les psychés[99]. Ensuite les attaques à l'encontre des SI de l'opposition visent à bloquer l'accès à ses blogs ou forums. L'attaque par DDoS[100] est utilisée comme une arme pour combattre les contre-discours venant confronter la propagande officielle de l'État, tout comme les techniques d'effacement des sites web qui servent à faire perdre en crédibilité [101]. L'utilisation de spyware[102] contre les appareils de militants permet d'espionner des cibles précises en vue d'arrestation. Ahmed Eltantawy, un ancien député égyptien membre de l'opposition démocratique, est ciblé par un groupe d'hackers mercenaires nommé Cytrox à la suite de son annonce de candidature pour les prochaines élections présidentielles. Par le biais du spyware Predator, son téléphone est mis sous surveillance. Le lien entre ce groupe de cybercriminel est plusieurs États est mis en avant par un rapport de CitizenLab[103]. Ainsi, la cyber-baltagiya, comme dans le monde physique, est utilisée lors des échéances électives pour exercer une pression sur l'opposition.

Enfin, l'intimidation et le harcèlement sont les actes de violence symbolique touchant directement les personnes. Elles sont la forme numérique la plus proche des méthodes utilisées par les baltagiya « dans la rue ». Au sein du cyberespace, la protection de la vie

[97]Abozaid, Ahmed M. "Digital Baltaga: How Cyber Technology Has Consolidated Authoritarianism in Egypt." *SAIS Review of International Affairs*, vol. 42, no. 2, 2022, pp. 5-19.
[98]Une ferme à trolls, ou usine à trolls, est un groupe institutionnalisé de trolls sur Internet (De Seta, 2017) qui cherche à façonner l'agenda politique d'une société spécifique et à s'immiscer dans les opinions politiques et les processus décisionnels.
[99]Ayeb, Marina, and Tiziano Bonini. "'It Was Very Hard for Me to Keep Doing That Job': Understanding Troll Farm's Working in the Arab World." *Social Media+ Society*, vol. 10, no. 1, 2024
[100] Une attaque par déni de service ou *Distributed Denial of Service attack* (DDoS) est un type de cyberattaque dans lequel plusieurs systèmes compromis sont utilisés pour inonder un site Web ou un réseau ciblé avec une grande quantité de requête saturant le trafic réseau et provoquant un blocage ou une indisponibilité pour les utilisateurs légitimes. Ce type d'attaque est souvent utilisé par les acteurs malveillants pour perturber les services et causer un préjudice financier ou d'atteinte à l'image aux organisations.
[101]Deibert, Ronald, and Rafal Rohozinski. "Beyond Denial: Introducing Next-Generation Information Access Controls." (2010).
[102]Un spyware, ou logiciel espion, est un type de logiciel malveillant conçu pour infiltrer un ordinateur ou un appareil mobile afin de collecter des informations sur l'utilisateur à son insu. Les spywares peuvent capturer divers types de données, tels que les frappes au clavier, les captures d'écran, les courriels, les historiques de navigation, les mots de passe, et même activer des périphériques comme les webcams et les microphones pour espionner l'utilisateur en temps réel.
[103]Marczak, Bill et al. "Predator in the Wires – Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions." *The Citizen Lab*, 22 septembre 2022, consulté le 20 mai 2024.

privée accordée par l'usage de pseudonymes ou de VPN fait la force des individus. Ils peuvent ainsi contourner la peur de la répression et exprimer leur opinions politiques, en d'autres termes cette caractéristique permet la politisation dans un contexte d'autoritarisme. La levée de l'anonymat constitue donc l'enjeu central du régime. Ainsi, les groupes de cyber-baltagiya cherchent à lever le voile d'anonymité des cyber-dissidents en usant de techniques de doxxing[104]. Cette pratique est utilisée pour nuire à la cible en partageant, de manière publique sur les réseaux sociaux, des informations sur son identité et sa vie privée. L'Égypte recourt ainsi à des campagnes de phishing à grande échelle visant les acteurs de la société civile égyptienne et les journalistes travaillant sur les questions des droits de l'homme, y compris la liberté d'expression et les droits des femmes. Par exemple, le groupe Nile Phish réussit à récupérer plusieurs informations sur des cybermilitants à la suite d'une intense campagne de phishing. Plus de 92 messages ont été envoyés en utilisant une technique de manipulation sociale sophistiquée. Les messages contenaient un programme malveillant visant à voler des informations personnelles en usurpant l'identité d'institutions ou d'entreprises légitimes[105]. La menace de publier les informations suffit à dissuader les militants de continuer leurs actions. Sinon, les campagnes de harcèlements à la suite de la révélation de leurs données personnelles peuvent se répercuter dans le monde réel par de la violence psychologique, mais aussi physique : « Les menaces de mort et autres messages violents sur les réseaux sociaux ne sont pas seulement des mots vils : ils équivalent souvent à de l'incitation à la haine ou à d'autres actes illégaux et peuvent parfois conduire à une véritable violence. Cela est particulièrement vrai si les menaces sont dirigées contre des activistes locaux que leurs gouvernements dépeignent comme des ennemis et des laquais des puissances étrangères »[106].

En somme, la cyber-baltagiya réussit à perturber les nœuds et à détruire les liens sur les réseaux sociaux [107]. Sous la peur de la répression de l'État, les journalistes se dénoncent mutuellement pour leurs opinions en ligne. Un individu peut rejoindre n'importe quel groupe

[104]Le doxing, également connu sous le nom de doxxing, est l'acte de rechercher et de partager publiquement des informations personnelles sur un individu ou une organisation sans son consentement. Cela peut inclure des informations sensibles telles que des adresses, des numéros de téléphone et des informations financières. Il est souvent utilisé comme une forme de harcèlement en ligne ou pour intimider et menacer des individus ou des groupes.
[105]Scott-Railton, John, et al. "Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society." 2017.
[106]Privacy International. "Their Eyes on Me: Stories of Surveillance in Morocco." (2015). Retrieved from https://privacyinternational.org/sites/default/files/Their%20Eyes%20on%20Me%20-%20English_0.pdf
[107]Loudiy, Fadoua, and Andrew R. Smith. "Cyber-baltagiya in Morocco: A Critical Rhetorical Analysis." *Revue Langues et Littératures*, vol. 24, 2015, pp. 1-27.

pro-gouvernemental sur Facebook et Twitter comme في حب السيسي (L'amour pour Al-Sissi) et signaler un compte activiste spécifique aux autres membres du groupe, puis tous les membres peuvent signaler en masse ce compte comme abusif ou faux à Facebook pour qu'il soit fermé. Cette violence par l'État et entre les citoyens peut être rapprochée de la notion de « folie autorisée » *(licensed lunacy)* théorisé par Orlando Patterson. Elle fait référence à des comportements ou des actions normalement inacceptables, mais qui sont autorisés ou tolérés par la société ou les autorités sous certaines conditions. Cette idée est souvent utilisée pour décrire des situations où les normes sociales et morales sont temporairement suspendues, permettant des actes de violence, de cruauté ou de répression sous l'égide de l'autorité légitime. Dans le cas égyptien, cet état se manifeste par « un double acte d'auto-annihlation » où la surveillance étatique remplace l'acte de tuer et l'acceptation de celle-ci, voire même sa participation, fait de l'individu un « fils de la surveillance »[108]. Le régime d'Al-Sissi réussit donc à faire du cyberespace un espace n'échappant pas à la domination légale et violente de l'autoritarisme. Le deuxième enjeu pour le régime est de contrôler ce qui se passe sur les réseaux, autant par la surveillance que par la maîtrise du discours.

CHAPITRE 2 – LE CYBER-AUTORITARISME : SURVEILLANCE ET CONTRÔLE DE L'OPINION PUBLIC

Afin de contrôler totalement le cyberespace, l'État passe par une double politique de domination, faisant des réseaux sociaux un puissant outil au service de son autoritarisme. S'amorce l'émergence d'un cyber-autoritarisme qui se traduit d'abord par une surveillance de masse du contenu numérique et des individus (1), puis par une maîtrise du discours sur les réseaux sociaux à des fins de propagande (2).

[108]Fouda, Radwa. "Through the Keyhole: Ethnographic Analysis of Cyber Violence in Egypt." 2019.

Section 1 - Surveillance de masse et contrôle des identités sur l'espace numérique comme numérisation de l'autoritarisme.

En 2011, les réseaux sociaux s'imposent comme une menace pour le régime autoritaire égyptien parce qu'ils ont su stimuler le partage d'informations et la création de communautés échappant relativement bien à toute surveillance. Cependant, bien que le cyberespace puisse favoriser la liberté des individus par l'anonymat et le partage, il crée parallèlement une opportunité pour les régimes autoritaires soucieux de surveiller l'entièreté de leur population. En effet, l'immense production de données numériques, allant des courriels aux messages instantanés en passant par les appels téléphoniques, favorise la logique panoptique où la surveillance de l'État devient omniprésente[109].

L'Égypte se saisit de cette opportunité pour renforcer son autoritarisme. En effet, l'essor de la surveillance en ligne sous le régime d'Abdel Fattah Al-Sissi marque une transformation significative dans l'approche égyptienne de la cybersécurité et de la surveillance numérique. La stratégie nationale égyptienne en matière de TIC 2014-2017 reflète ce changement, passant d'une surveillance ciblée à une surveillance de masse du contenu produit dans le cyberespace. Cette nouvelle approche est facilitée par l'acquisition de technologies de surveillance sophistiquées auprès d'entreprises étrangères spécialisées dans les logiciels espions. Entre autres, l'Égypte achète des logiciels de sécurité ProxySG à la société américaine BlueCoat pour censurer et intercepter du contenu en ligne. Plus tard, des contrats sont conclus avec Hacking Team, FinFisher et NSO Group. Ces technologies sont déployées pour scanner les médias sociaux à la recherche de sujets spécifiques, notamment la diffamation, les manifestations illégales, les grèves, le terrorisme[110]. Par ailleurs, le soutien des pays occidentaux et des alliés régionaux joue un rôle crucial dans cette transformation. La France vend un système de surveillance aux Émirats arabes unis, lequel est offert à l'Égypte sous le nom de code « Tobleron »[111]. De plus, les Émirats arabes unis et l'Arabie saoudite soutiennent activement les efforts égyptiens. Ces technologies permettent une surveillance efficace et

[109]Hassib, Bassant, and Nardine Alnemr. "Securitizing Cyberspace in Egypt: The Dilemma of Cybersecurity and Democracy." Routledge Companion to Global Cyber-Security Strategy, Routledge, 2021, pp. 521-533.
[110]Fathy, Noha. "Freedom of Expression in the Digital Age: Enhanced or Undermined? The Case of Egypt." *Journal of Cyber Policy*, vol. 3, no. 1, 2018, pp. 96-115.
[111]Franceinfo. "Cybersécurité: La Surveillance de masse en Égypte et la Désinformation dans les Pays baltes." Franceinfo, 3 octobre 2023, www.francetvinfo.fr/replay-radio/le-club-des-correspondants/cybersecurite-la-surveillance-de-masse-en-egypte-et-la-desinformation-dans-les-pays-baltes_6069963.html. Consulté le 14 avril 2024.

relativement peu coûteuse des journalistes, des activistes et de l'opposition politique, installées via le fournisseur d'accès Internet privé Etisalat. Enfin, l'entreprise Uber est contrainte de transmettre les données de ses utilisateurs égyptiens au gouvernement illustrant la volonté de collecter le plus d'informations possible sur la population[112].

L'émergence de la surveillance de masse en Égypte peut être considérée comme l'élaboration d'un « autoritarisme en réseau » (*network authoritarism*)[113]. Cette notion avancée par MacKinnon met en avant la confrontation entre la société civile et l'État autoritaire dans la lutte pour la liberté d'expression. En reprenant les trois axes du pouvoir autoritaire élaborés par Göbels, il aisé de constater que de telles pratiques de surveillance renforcent « le pouvoir despotique » écrasant les libertés. Les cybermilitants se trouvent davantage exposés à la possibilité de blocages ou d'arrestations. De surcroît, les technologies de surveillance et d'écoute confèrent au régime une capacité accrue de contrôler la société. L'examen des données collectées lui permet de saisir les motifs de mécontentement pouvant donner lieu à des troubles publics et d'agir en conséquence, potentiellement en apaisant ces griefs. Ces fonctions de rétroaction revêtent une importance particulière dans les régimes autoritaires où les enquêtes d'opinion publique sont peu fréquentes. Par le biais de la cyber surveillance, les gouvernements interceptent les conversations en ligne, surveillent les contenus et réagissent en conséquence. Ces données peuvent être analysées en temps réel pour détecter d'éventuels mouvements contestataires ou des menaces contre l'État.

Dans cette logique, le régime tente de créer une identité numérique nationale afin d'accroître la surveillance et la dissuasion qu'elle entraîne. Sous Mubarak, les clients de cybercafés donnaient leur identité aux gérants, il existait ainsi un contrôle des identités, mais seulement dans le monde physique. Al-Sissi les numérise dans un processus s'apparentant aux méthodes d'identification des États modernes au XIXe siècle soucieux de contrôler leur population pour des considérations fiscales, martiale mais aussi de surveillance[114]. La création de l'identité numérique est un pas de plus vers la numérisation du régime autoritaire. Elle est d'abord justifiée par les problèmes que posent l'anonymat et le droit à la vie privé des cybercriminels. La délivrance de cartes SIM est soumise à la présence physique des individus ainsi qu'à la

[112]Abozaid, Ahmed M. "Digital Baltaga: How Cyber Technology Has Consolidated Authoritarianism in Egypt." *SAIS Review of International Affairs*, vol. 42, no. 2, 2022, pp. 5-19.
[113]MacKinnon, R. 2010. "Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom." Paper presented at the liberation technology in authoritarian regimes, Stanford University, October 11-12.
[114]Aghroum, Christian, et al. *Identification et Surveillance des Individus*. Éditions de la Bibliothèque Publique d'Information, 2010. https://doi.org/10.4000/books.bibpompidou.1192.

présentation de leur carte d'identité. Les opérateurs de téléphonies coopèrent donc avec les agences de police pour permettre l'accès aux réseaux téléphoniques et 4G[115]. Parmi les projets de lois du régime, l'accès à un Facebook réglementé permettrait de contrôler les identités. Son accès serait soumis à un enregistrement payant auprès de Telecom Egypt. Des permis seraient délivrés en conséquence et les données récoltées stockées dans une base de données. Les personnes qui se connectent à Facebook sans abonnement seraient soit condamnées à une amende de 5 000 livres égyptiennes, soit à une peine de six mois de prison, ou bien les deux la fois. Ce système, selon un député, aiderait la surveillance de l'État dans sa mission de lutte contre les contenus en ligne qui mettent en cause la sécurité nationale[116]. Cette loi reste encore en débat, mais traduit la volonté de contrôle des individus sur les réseaux. L'objectif est d'avoir connaissance des potentielles menaces planant sur la stabilité du régime, mais encore il existe une volonté de contrôler le discours et les idées au sein même du cyberespace.

Section 2 - Contrôle du discours sur le Net

Le filtrage du contenu est étroitement lié à la surveillance et au pouvoir despotique selon Gobel. Cependant, à l'aune de l'étude de Christensen Britt, il apparaît plus pertinent de l'inclure dans le pouvoir discursif, c'est-à-dire la manière dont les gouvernements tentent de contrôler et d'influencer le discours public en produisant de la propagande et de la désinformation, en contrôlant le contenu et en participant à la formation des récits publics[117]. En effet, à l'ère du numérique, le contrôle de l'information sur les réseaux sociaux s'associe davantage au contrôle du discours public. Si les informations disponibles dans une société affectent les discussions et le brassage d'idées, alors le contrôle de l'information permet d'orienter le discours public et les revendications politiques. A travers toute une série de lois et de mesures visant à propager un récit public en faveur du pouvoir en place, le régime d'Al-Sissi tente d'instaurer un peu plus le cyber-autoritarisme. Cette restructuration du cyberespace

[115]Hassib, Bassant, and James Shires. "Manipulating Uncertainty: Cybersecurity Politics in Egypt." *Journal of Cybersecurity*, vol. 7, no. 1, 2021, article tyaa026.
[116]Marquis-Boire, M., Dalek, J., McKune, S., et al. *Planet Blue Coat: Mapping Global Surveillance and Censorship Tools*. Citizen Lab, janvier 2013.
[117]Christensen, Britt. "Cyber State Capacity: A Model of Authoritarian Durability, ICTs, and Emerging Media." *Government Information Quarterly*, vol. 36, no. 3, 2019, pp. 460-468.

égyptien suit la logique Gramscienne de symbiose entre le pouvoir répressif, par la violence et la surveillance, avec l'obsession de fabriquer une force de consentement[118]. Elle se manifeste par une double politique de blocage ou de filtrage du contenu dissident, et de la création d'un discours pro-régime virulent sur les réseaux sociaux.

La politique de filtrage fait son apparition dès 2012 avec une décision de justice n'ayant pas grand-chose à voir avec la dissidence politique. En novembre, le tribunal émet l'interdiction des sites pornographiques en affirmant que « la liberté d'expression et les droits publics doivent être restreints en maintenant les fondements de la religion, de la moralité et du patriotisme », tout en les qualifiant de « venimeux et ignobles »[119]. A titre de comparaison, l'Arabie Saoudite procède de la même manière en interdisant le contenu pornographique par le filtrage, de même que le Pakistan. La raison est d'ordre religieux et sert le régime en place. Dans le cas égyptien, ce blocage reste motivé par une concurrence avec les Frères Musulmans qui, par leur mouvement « Pure Net », souhaitent accorder la culture du web avec les mœurs religieuses des égyptiens. Malgré cela, cette première tentative ouvre la voie au mécanisme de filtrage du web sous couvert d'idéologie. Les dispositifs législatifs ne tardent pas : l'article 19 de la loi 180 donne pour mission au CSRM de bloquer les sites Web, blogs ou un compte personnel qui enfreint les dispositions de la loi, à savoir tout contenu extrémiste, terroriste ou remettant en cause la stabilité et la sécurité de l'État et de sa Constitution.

Très rapidement la sphère publique en ligne subit une répression autoritaire visant en premier lieu les opposants démocratiques et les défenseurs des droits de l'Homme. Durant l'état d'urgence suivant les attentats dans des églises coptes en mai 2017, ce sont 21 sites critiques envers le régime qui sont fermés par la CSRM. Parmi eux, des sites d'informations indépendants comme Mada Masr, mais aussi étrangers comme Al-Jazeera et la branche arabe du Huffington Post. Officiellement, ces pages web sont accusées de relayer de fausses informations pour le compte de puissances étrangères hostiles à la stabilité du pays ou au service des islamistes. En septembre 2017, le nombre de blocages augmente pour atteindre 432 sites, notamment des agences de presse et des sites Web d'organisations de défense des droits de l'homme. Le blocage généralisé vise à restreindre systématiquement l'espace civique et à réprimer la société civile sous prétexte de lutte contre le terrorisme.

[118]Abozaid, Ahmed M. "Digital Baltaga: How Cyber Technology Has Consolidated Authoritarianism in Egypt." *SAIS Review of International Affairs*, vol. 42, no. 2, 2022, pp. 5-19.
[119]Galperin, E. "Egyptian Prosecutor Orders a Ban on Internet Porn." *Electronic Frontier Foundation*, 7 novembre 2012. Consulté le 6 février 2018.

Les politiques de blocages se traduisent de même sur les réseaux sociaux. L'Égypte déclare son intention de bloquer les applications mobiles Viber et WhatsApp pour des raisons sociales et sécuritaires. La National Telecommunications Regulatory Authority (NTRA) annonce la création d'un comité pour surveiller les communications sur les applications mobiles gratuites. Depuis octobre 2015, les services de voix sur IP (VoIP) sont bloqués de manière intermittente sur les réseaux mobiles. Bien que la NTRA nie les restrictions de ces services, les fournisseurs signalent que ces services sont désactivés depuis une déclaration de la NTRA.[120] De plus, les mesures techniques de NetBlocks montrent que le gouvernement ralentit et désactive des applications comme Messenger de manière intermittente. Ces coupures empêchent les utilisateurs de partager leurs emplacements ainsi que des photos pendant les manifestations. Plus généralement, l'accès aux médias sociaux devient indisponible sur certains réseaux de FAI.

Ces pratiques de censure vont plus loin avec un contrôle total des comportements en ligne. Non seulement les idées politiques dissidentes sont sévèrement réprimées par des peines de prison pouvant aller jusqu'à dix ans pour un tweet, une publication sur Facebook ou une vidéo sur YouTube ou TikTok, mais les comportements apolitiques tendent à être de plus en plus concernés. Par exemple, le Parquet suprême de la sécurité de l'État et le Bureau du procureur général ont emprisonné deux jeunes célébrités des plateformes des médias sociaux TikTok et Lookie pour avoir publié des vidéos les montrant en train de danser et de s'amuser chez elles. Ce changement majeur d'approche fait basculer le système de contrôle du discours d'une dimension autoritaire à une dimension quasi-totalitaire. En effet, selon Juan Linz, la frontière entre ces deux notions se trouve dans la volonté de l'État totalitaire de contrôler tous les aspects de la vie de sa population. Jusqu'à ce virage brutal, le régime égyptien n'aspirait qu'à contrôler le discours politique de sorte à légitimer son pouvoir et à le sécuriser. La question se pose donc de savoir jusqu'à quel degrés l'Égypte est prête à aller dans le contrôle de l'opinion.

Les techniques de filtrage et de blocage ne sont qu'une partie de la stratégie globale de l'Égypte dans le contrôle de l'opinion publique en ligne. Ainsi, la création d'une propagande virulente apparaît nécessaire pour rassembler le peuple autour du régime et consolider son pouvoir discursif. L'enjeu pour l'État est de transmettre un récit sur la situation politique, sociale et économique dans le but d'embellir l'image du gouvernement. Cette stratégie est

[120]Fathy, Noha. "Freedom of Expression in the Digital Age: Enhanced or Undermined? The Case of Egypt." *Journal of Cyber Policy*, vol. 3, no. 1, 2018, pp. 96-115.

d'autant plus importante à l'arrivée d'Al-Sissi au pouvoir que la situation économique du pays se détériore. Pour ce faire, l'État compte sur le soutien de personnalités publiques influentes ou reconnues dans leur domaine. Ainsi, un conseil des directeurs des comités électroniques pro-Sissi est établi avec pour but de rassembler des personnalités, comme des rédacteurs en chef et des universitaires, chargées d'abreuver les réseaux sociaux de messages célébrant les autorités militaires et d'accuser les Frères musulmans de tous les maux du pays[121]. L'appui sur des personnalités reconnues des réseaux permet à Égypte de donner plus de poids à son récit. Par exemple, les influenceurs Farida Salem et Hussien Elgohary véhiculent une image du régime comme étant un régime ouvert et à l'écoute des revendications citoyennes. En échange, l'État s'engage à renforcer la visibilité de leur contenu numérique[122].

Le régime ne s'appuie pas uniquement sur des personnalités pour propager son récit, il est aussi question d'usines à troll inondant les réseaux sociaux de messages soutenant l'État à l'aide de bots ou de communautés fidèles au régime. Cette méthode plus virulente passe par des campagnes de trolling massif sur Twitter notamment avec pour but de transmettre de la désinformation. La société New Waves basée aux Émirats Arabes Unis, mais opérant en Égypte, avait jusqu'en août 2019 plus de 378 faux comptes sur Facebook par lesquels elle transmettait des messages en faveur du gouvernement égyptien. De même la société DotDev, également basée aux Émirats Arabes Unis, gérait 271 comptes Twitter pour coordonner des campagnes de propagande. Ces deux entreprises créent et véhiculent de nombreux hashtag pro-régimes tels que #هندعم_السيسي_ل2030 (« Nous soutiendrons El-Sisi pour 2030 ») ou encore #كل_الدعم_لرجال_ الشرطة (« Soutien total aux policiers »). Pendant quelques temps ces hashtag se sont maintenus dans la tendance Twitter en Égypte. Le but est de construire la fausse perception d'un soutien généralisé au gouvernement, tout en fustigeant les manifestations. Parallèlement, ces groupes délégitiment par le même procédé les utilisateurs mettant en doute le régime et sa popularité. Ainsi, Saheeh Masr, une agence de vérification des faits (fact-checking), s'est retrouvée visée par une campagne portant l'hashtag : #صحيح_مصر_لجنة_ننوس_مامته (« Saheeh Masr sont les trolls de sa maman »)[123]. Il est alors question d'une « Guerre des hashtag » sur Twitter dont l'objectif est l'orientation de l'opinion publique. La numérisation de l'autoritarisme se traduit par une double politique de

[121]Lavrilleux, Ariane. "Égypte: L'Armée 2.0 d'Abdel Fattah al-Sissi." *JeuneAfrique.com*, 30 décembre 2020, Consulté le 2 juin 2024.
[122] Michaelson, Ruth, and Michael Safi. "Sugar-coated propaganda? Middle East taps into power of influencers." *The Guardian.* 29 janvier 2021. Consulté le 2 juin 2024.
[123]"Egyptian Twitter Network Amplifies Pro-Government Hashtags, Attacks Fact-Checkers." *Digital Forensic Research Lab*, 23 mars 2023. Consulté le 2 juin 2024.

surveillance du contenu et des individus mais aussi d'un contrôle du discours public sur les réseaux sociaux. L'enjeu est d'éliminer les potentielles menaces tout en imposant la légitimité du pouvoir en place par l'exaltation nationale et anti-terroriste.

CONCLUSION

L'évolution du cyberespace égyptien oscille entre des périodes de démocratisation éphémère et un retour prédominant à l'autoritarisme, dévoilant ainsi un panorama complexe de changements structuraux et de stratégies antagonistes orchestrées par les différents acteurs impliqués.

Initialement, sous l'égide de Hosni Mubarak, le cyberespace égyptien bénéficie d'une certaine libéralisation affranchie en partie des contraintes étatiques. Cette ouverture favorise l'émergence d'une opposition démocratique dynamique, qui exploite habilement le potentiel du cyberespace au service d'un activisme politique sans précédent qui s'exprime lors des soulèvements des Printemps arabes. Ainsi, le cyberespace devient le foyer de la mobilisation et de la coordination des forces contestataires.

Dans un second temps, l'analyse se concentre sur le cyberespace comme champ de bataille informationnel entre l'État et l'opposition démocratique. L'État, déconcerté par cette nouvelle forme de résistance, perd initialement le contrôle sur le cyberespace, accélérant ainsi sa propre chute, une illustration frappante de l'impact du monde virtuel sur le monde réel de la politique. Cependant, l'opposition, confrontée à une légitimité fragile après la chute de Mubarak et à la fragmentation du cyberespace en factions idéologiques divergentes, peine à maintenir son influence. Cette fragmentation corrosive mine la cohésion et l'efficacité de la contestation en ligne, ouvrant ainsi la porte à de nouveaux acteurs attirés par les outils ayant permis la « Révolution d'Internet ».

Enfin, le retour graduel de l'autoritarisme dans le cyberespace égyptien est rendu possible par une transformation majeure : l'étatisation. Le régime exploite astucieusement la fragmentation pour instaurer un processus de numérisation de son autorité, se traduisant par la recherche de légitimation de la régulation et l'imposition de la violence numérique. Des stratégies autoritaristes méticuleusement conçues, telles que le contrôle subtil de l'opinion par la propagande et la désinformation ainsi que la censure et la surveillance rigoureuse des informations circulant sur les réseaux sociaux, sont mises en œuvre.

L'analyse met en lumière le parcours du cyberespace égyptien, une trajectoire marquée par des périodes de « libéralisme », en faveur d'une opposition démocratique qui en devient active, suivies d'une instrumentalisation systématique au service d'un régime autoritaire. Cette

évolution, ponctuée d'épisodes libéraux, de tensions et de résurgences autoritaires, illustre la dualité et la complexité de cet environnement numérique, reflet fidèle des aspirations démocratiques et des réalités autoritaires dans la société égyptienne contemporaine.

Considérant les récents changements structurels du cyberespace égyptien, il est clair que les ambitions de l'État se tournent désormais vers une vision de cyberpuissance. Après avoir réaffirmé la puissance politique du régime, il s'agit maintenant de consolider la place régionale de l'Égypte en matière de cybersécurité. Le président Abdel Fattah Al-Sissi entend faire de son pays le prochain grand hub numérique de la région, comme le traduit le plan de développement « Egypt Vision 2030 ». L'objectif politique semble clair : « garantir un cyberespace sûr et fiable » pour reprendre les mots d'Ahmed Abdel-Hafez, vice-président de la NTRA.

Après avoir étudié la question du pouvoir au sein même de l'Égypte entre le régime et l'opposition, se pose alors la question de la place de l'Égypte dans l'espace géopolitique numérique de la région. Dans un environnement dominé par des acteurs étatiques agressifs tels que l'Iran, Israël et la Syrie, la place de l'Égypte dans la lutte pour la cyberpuissance reste à déterminer. D'autant plus que cet environnement voit émerger des groupes non-étatiques tout aussi importants comme le Hezbollah et le Hamas, qui se sont révélés très actifs et innovants en termes de cyberattaques comme l'illustre le conflit israélo-arabe ravivé depuis octobre 2023. Dans ce contexte, il semble pertinent de questionner la place de l'Égypte au sein de la géopolitique du numérique entre affrontements et coopération au Moyen-Orient.

BIBLIOGRAPHIE

Articles de revues scientifiques :

Abozaid, Ahmed M. "Digital Baltaga: How Cyber Technology Has Consolidated Authoritarianism in Egypt." *SAIS Review of International Affairs*, vol. 42, no. 2, 2022, pp. 5-19.

Abrahams, Alexei, and Andrew Leber. "Electronic Armies or Cyber Knights? The Sources of Pro-Authoritarian Discourse on Middle East Twitter." *International Journal of Communication*, vol. 15, 2021.

Ahmadipor, Zahra, and Mahdi Karimi. "The Impact of Cyber Space on Egypt's Revolution." *The International Journal of Humanities*, vol. 23, no. 1, 2016, pp. 99-117.

Badie, Bertrand. "Printemps Arabe: Un Commencement." *Études*, vol. 415, no. 7-8, 2011, pp. 7-18.

Christensen, Britt. "Cyber State Capacity: A Model of Authoritarian Durability, ICTs, and Emerging Media." *Government Information Quarterly*, vol. 36, no. 3, July 2019, pp. 460-468.

Clarke, Killian, and Korhan Kocak. "Launching Revolution: Social Media and the Egyptian Uprising's First Movers." *British Journal of Political Science*, vol. 50, no. 3, 2020.

Cumin, David. "Pour une définition objective du terrorisme à l'aide des critères de la polémologie et du droit des conflits armés." *T. Bourgou, M. Chabbi, Regards croisés dans l'après-11 Septembre, Paris, l'Harmattan* 2011: 63-102.

De Angelis, Enrico. "L'espace politique virtuel avant et après la chute de Moubarak: une critique des réseaux sociaux digitaux en Egypte." *Égypte/Monde arabe,* vol 12, 2015: 195-227.

Deibert, Ronald, and Rafal Rohozinski. "Beyond Denial: Introducing Next-Generation Information Access Controls." *Information Revolution And Global Politics*, 2010.

Dr. Ramadan Elaiess. “Action Plan Towards the Information Society in Developing Countries and the Arabic Speaking World”. *American Research Journal of Computer Science and Information Technology*, Volume 2, 2017, pp. 1-18.

Faris, David M. "La Révolte en Réseau: Le « Printemps Arabe » et les Médias Sociaux." *Politique Étrangère*, vol 1, no. 1, 2012, pp. 99-109.

Fayat, Hervé. "ÉTAT, sociologie." *Encyclopædia Universalis*, 8 septembre 2015.

Fouda, Radwa. "Through the Keyhole: Ethnographic Analysis of Cyber Violence in Egypt." *American University in Cairo American University in Cairo*. 2019.

Gillmor, Dan. "We the Media: The Rise of Citizen Journalist." *Nat'l Civic Rev.*, vol. 93, 2004, p. 58.

Göbel, Christian. "The Information Dilemma: How ICT Strengthen or Weaken Authoritarian Rule." *Statsvetenskaplig Tidskrift*, vol. 115, 2013, pp. 367-384.

Gonzalez-Quijano, Yves. "Internet, le «Printemps arabe» et la dévaluation du cyberactivisme arabe." *Égypte/Monde arabe*, no. 12, 2015, pp. 67-84.

Greenemeier, Larry. "How Was Egypt’s Internet Access Shut Off?" *Scientific American*, 28 Jan. 2011.

Hassan, Hamdy A. "Civil Society in Egypt Under the Mubarak Regime." *Afro Asian Journal of Social Sciences*, vol. 2, no. 2.2, 2011.

Hassib, B. "Egypt’s Counter-Terrorism Policy Post 9/11 and Beyond: Shrinking Civic Space." *Terrorism and Civil Society: Post-9/11 Progress and Challenges*, edited by Romaniuk SN, Mullins S, Ruteere M, Manchester University Press, 2020.

Hassib, Bassant, and James Shires. "Manipulating Uncertainty: Cybersecurity Politics in Egypt." *Journal of Cybersecurity*, vol. 7, no. 1, 2021

Hellyer, H.A. "Violence and the Egyptian Military." *Foreign Policy*, 2012.

Iskander, Elizabeth. "Connecting the National and the Virtual: Can Facebook Activism Remain Relevant after Egypt’s January 25 Uprising?" *International Journal of Communication*, vol. 5, 2011, pp. 1225-1237.

Kempf, Astrid. "Pour une Sociologie du Cyberespace." *Revue Défense Nationale*, vol. 785, no. 10, 2015, pp. 77-82.

Khamis, Sahar, et al. "Beyond Egypt's 'Facebook Revolution' and Syria's 'YouTube Uprising': Comparing Political Contexts, Actors and Communication Strategies." *Arab Media & Society*, vol. 15, spring 2012, pp. 1-30.

Kim, Elvis H. "Democratization and Authoritarianism in the Information Age." *International Area Studies Review*, vol. 24, no. 3, 2021, pp. 205-223.

Loudiy, Fadoua, and Andrew R. Smith. "Cyber-altagiya in Morocco: A Critical Rhetorical Analysis." *Revue Langues et Littératures*, vol. 24, 2015, pp. 1-27.

Privacy International. "Their Eyes on Me: Stories of Surveillance in Morocco." *The Journal of North African Studies* 22(3) 2015. pp. 361-385

Rinnawi, Khalil. "Cyber Uprising: Al-Jazeera TV Channel and the Egyptian Uprising." *Language and Intercultural Communication*, vol. 12, no. 2, 2012, pp. 118-132.

Schmitter, Philippe C., and Terry Lynn Karl. "What Democracy Is. . .and Is Not." *Journal of Democracy*, vol. 2, 1991, pp. 75–88.

Shehabat, Ahmad. "The Social Media Cyber-War: The Unfolding Events in the Syrian Revolution 2011." *Global Media Journal: Australian Edition*, 2012.

Thompson, Karson K. "Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate." *Texas Law Review*, vol. 90, 2011, pp. 465.

Tomiche, Nadia. "P. J. Vatikiotis, The Egyptian Army in Politics. Pattern for New Nations ?" *Annales. Économies, Sociétés, Civilisations*, 20e année, N. 4, 1965, pp. 851-852.

Articles de journal :

"Egypte. Il Avait Critiqué l'Armée : Le Blogueur Écope de Trois Ans de Prison.", *Le Télégraphe ,* 11 avril 2011. Consulté le 4 avril 2024

"Egyptian Twitter Network Amplifies Pro-Government Hashtags, Attacks Fact-Checkers." *Digital Forensic Research Lab*, 23 mars 2023. Consulté le 2 juin 2024.

Arthur, Charles. "Google and Twitter Launch Service Enabling Egyptians to Tweet by Phone." *The Guardian*, 1 Feb. 2011.

Ayeb, Marina, and Tiziano Bonini. "'It Was Very Hard for Me to Keep Doing That Job': Understanding Troll Farm's Working in the Arab World." *Social Media+ Society*, vol. 10, no. 1, 2024

Iskandar, Adel. "The Baltageya: Egypt's Counterrevolution." *The Huffington Post*, 2011.

Lavrilleux, Ariane. "Égypte: L'Armée 2.0 d'Abdel Fattah al-Sissi." *JeuneAfrique.com*, 30 décembre 2020. Consulté le 5 avril 2024.

Marczak, Bill et al. "Predator in the Wires – Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions." *The Citizen Lab*, 22 septembre 2022, consulté le 20 mai 2024.

Michaelson, Ruth, and Michael Safi. "Sugar-coated propaganda? Middle East taps into power of influencers." *The Guardian.* 29 janvier 2021.

Scott-Railton, John, et al. "Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society." *The citizen Lab*. 2017. Consulté le 29 mai 2024.

Ouvrages et Chapitres :

Boyer, Bertrand. « Le cyberespace : la nouvelle frontière de la guerre de l'information », Stéphane Taillat éd., *La Cyberdéfense. Politique de l'espace numérique.* Armand Colin, 2023, pp. 244-253.

D'Urbano, Paolo. *Ikhwan Web: Digital Activism and the Egyptian Muslim Brotherhood*. Diss. SOAS, University of London, 2012.

Elias, Norbert. *Le Processus de Civilisation*. Calmann-Lévy, 1973.

Gibson, William. *Neuromancer.* ACE, 1984.

Hassib, Bassant, and Nardine Alnemr. "Securitizing Cyberspace in Egypt: The Dilemma of Cybersecurity and Democracy." Routledge Companion to Global Cyber-Security Strategy*, Routledge*, 2021, pp. 521-533.

Howard, P.N. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford University Press, 2011.

Kempf, Olivier. *Introduction à la Cyberstratégie*. Economica, 2012.

Lévy, Pierre. *L'Intelligence Collective: Pour une Anthropologie du Cyberspace*. Éditions La Découverte, 1994.

Linz, Juan. *Totalitarian and Authoritarian Regimes*. Rienner, 2000.

Tilly, Charles. *Social Movements and National Politics,* 1979.

Weber, Max. *Le savant et le politique*. Union Générale d'Édition*.,* 1919

Lois :

Arab Republic of Egypt. "Article 1 Law No. 94/2015 on Anti-Terrorism."

Egyptian Supreme Council for Media Regulation. "Law No. 180 of 2018 on Regulating the Press, Media, and the Supreme Council for Media Regulation." 2018.

Telecommunication Regulation Law no. 10 of 2003 Article 65

Etudes, analyses statistiques :

Arab Republic of Egypt: Ministry of Communication and Information Technology. *ICT Indicators Report 2007–2011*. 2011.

ERCIM, "Le Développement d'Internet dans les Pays Méditerranéens et la Coopération avec l'Union Européenne: une Étude Menée pour la Commission Européenne." 1997.

Internet World Stats. "Internet World Stats: Usage and Population Statistics." Miniwatts Marketing Group, 2011.

Sawi, A., & Hady, Z. A. "Youth and Participation in Society." In H. Handoussa (Ed.), *Egypt Human Development Report*. United Nations Development Program, and the Institute of National Planning, 2010, pp. 105–122.

Henry, Lancaster. *Egypt - Mobile Infrastructure, Operators and Broadband - Statistics and Analyses*. Budde Com, 2009.

OpenNet Initiative. « Internet filtering in Egypt ». 2009.