Rapport à la loi des hacktivistes et Position de la loi face aux agissements des hacktivistes

Me Cécile DOUTRIAUX est avocate, diplômée du conservatoire national des Arts et Métiers, officier de la réserve citoyenne de la gendarmerie nationale et membre de la chaire cyberdéfense & cybersécurité des écoles de Saint-Cyr Quoëtquidan.

Octobre 2013 – Article n°II.4

Le cyberespace est devenu un enjeu de puissance, non seulement pour les États, mais également pour les groupes sociaux, revendiquant un certain idéal. Ainsi, Internet est devenu le mode d'action directe privilégié des hacktivistes, confrontés à un système politique qui restreint la contestation et l'opposition, par des moyens légaux. Les hacktivistes, qui utilisent les nouvelles technologies et les méthodes des hackers pour diffuser leurs revendications politiques, sont parfaitement conscients que les systèmes d'information peuvent constituer, pour les États, un outil stratégique de surveillance des populations. Quel est le rapport à la loi des hacktivistes face à cette tentative de contrôle ? Quels sont les moyens de répression mis en œuvre par les États pour maintenir l'ordre et la sécurité, face aux agissements des hacktivistes, notamment quand des informations classifiées secret défense sont divulguées au public et à des puissances étrangères ?

Rapport à la loi des hacktivistes et Position de la loi face aux agissements des hacktivistes.

Le cyberespace, perçu longtemps comme un environnement sans limites, universel et auto-régulé, est désormais très convoité. Dans la mesure où ses frontières sont incertaines et dictées essentiellement par ses réseaux, qui sont aussi bien publics que privés, commerciaux que gouvernementaux, il est devenu un territoire politique et idéologique important à investir et à conquérir. Cet espace est devenu un enjeu de puissance, non seulement pour les États, mais également pour les groupes sociaux qui revendiquent un certain idéal.

Le cyberespace est un lieu d'affrontements idéologiques, facilité par les outils numériques, qui permettent, au niveau mondial, la propagation facile et rapide d'idées. Ainsi, Internet est-il devenu le mode d'action directe privilégié des militants, confrontés à un système politique qui restreint la contestation et l'opposition, par des moyens légaux et illégaux pour les régimes les moins démocratiques.

Pour promouvoir leurs idées, faire une démonstration de leur force en matière de communication et de leur maîtrise des systèmes d'information, certains activistes vont franchir la limite du cyberactivisme, qui se caractérise par l'utilisation des réseaux sociaux à des fins contestataires, pour emprunter certaines méthodes des hackers. Ainsi, l'hacktivisme est-il l'utilisation des nouvelles technologies de l'information et de la communication et des techniques des hackers, par des activistes, pour diffuser leurs revendications politiques. Cette forme de protestation sociale est assez récente et les premières manifestations remonteraient à 1994, si on prend en considération l'utilisation importante de la

technologie, des téléphones satellites et d'Internet par l'Armée zapatiste de libération nationale, lors de la révolte au Chiapas.

Depuis, le recours à l'hacktivisme s'est multiplié, notamment ces dix dernières années. Pour certains auteurs, comme A.Samuel[1] l'hacktivisme est « l'utilisation non violente d'outils digitaux illégaux ou transgressifs à des fins politiques » et serait donc un mouvement essentiellement pacifiste. En effet, certains collectifs d'hacktivistes, tel que Télécomix, peuvent avoir des liens avec des organisations non gouvernementales, pour défendre des causes humanitaires[2].

Pourtant, l'OTAN a jugé que l'action de certains hacktivistes était « extrêmement dangereuse»[3] et le F.B.I. a identifié les hacktivistes comme un acteur malveillant du cyber-monde, au même titre que les services de renseignements étrangers, les groupes terroristes et les entreprises du crime organisé.[4] En effet, certains hacktivistes ont divulgué des documents classés secret défense, comme le collectif Anonymous qui a piraté des fichiers sensibles de l'armée américaine en 2011 et des documents de l'OTAN, relatifs à des opérations au Kosovo.[5] Dans un rapport publié le 5 décembre 2012 par le laboratoire Kaspersky, sur les menaces à venir pour 2013, il est prévu que les États se doteront de nouveaux outils destinés à renforcer la surveillance des individus[6]. Or, pour les hacktivistes, ces agissements des États entrent en conflits avec les droits démocratiques des individus. Ainsi, parallèlement au renforcement du contrôle et de la surveillance des populations, se développeraient les contestations liées à ces pratiques et nous devrions, a priori, assister à une montée en puissance du phénomène hacktiviste.

Quel est le rapport à la loi et la réaction des hacktivistes face à cette mise sous contrôle ?

Les hacktivistes ne prennent pas en compte ce qui est légal, mais ce qui leur semble légitime, c'est-à-dire ce qui leur semble juste en raison et en équité. Par conséquent, ils ne se réfèrent pas au droit positif élaboré par les États, mais à l'appréciation personnelle de ce qui leur paraît équitable.

Ce positionnement rejoint la désobéissance civile, analysée comme le refus de se soumettre à une loi, une organisation ou un pouvoir jugé inique par ceux qui le contestent et accomplie dans l'objectif d'amener un changement législatif ou sociétal, selon Henry David Thoreau[7] et John Rawls[8]. Si l'hacktivisme se distingue du hacking pratiqué sans motivation politique, les hacktivistes vont emprunter certaines idéologies des hackers qui définissent eux-mêmes leurs propres règles : " *Pensez par vous-même et remettez en cause l'Autorité, voilà ce qui devrait être l'essence même de la loi* " proclame " Le Manifeste du hacker " de 1986[9]. *" Vous n'avez aucun droit moral de dicter chez nous votre loi et vous ne possédez aucun moyen de nous contraindre ". "Vous n'avez pas de souveraineté où nous nous rassemblons. Le cyberespace ne se situe pas dans vos frontières. "* pose " La déclaration d'indépendance du cyberespace " de 1996[10]. Internet s'adapte fort bien à cette nouvelle conception de l'espace qui s'affranchit des frontières, telles que nous les concevons géographiquement. Comme les hackers, les hacktivistes pensent qu'Internet doit rester un outil accessible à tous, qu'il doit être possible d'utiliser de manière anonyme, sans être surveillé, ni contrôlé par les gouvernements ou les

[1] Alexandra Samuel, " Hacktivism and the Future of Political Participation " septembre 2004
[2] Telecomix a formé Reporters Sans Frontières afin d'échapper à la censure http:awni.fr/2012/03/04/hackers-forment-journalistes/
[3] Conclusions du Rapporteur Général Lord Jopling-OTAN : 7-10 octobre 2011; www.nato
[4] Déclaration de John Boles directeur adjoint de la division Cyber du F.B.I. 13 mars 2013
[5] L'Otan piraté par Anonymous » du 22/07/11- www.actudefense.com/anonymous-menace-lotan/
[6] Kaspersky Security Bulletin 2012. Malware Evolution sur www.kasperkylab.
[7] Henry David Thoreau, La Désobéissance civile, Le Passager Clandestin, 2007 (1re éd. 1849)
[8] John Rawls, *Théorie de la justice*, Paris, Seuil, 1987, p. 405
[9] http--www.dg-sc.org-phrack-fr-phrack-fr-phrack07-fr-conscience.txt
[10] A Declaration of the Independence of Cyberspace https://projects.eff.org/~barlow/Declaration- Final.html

forces armées. A ce titre, il est fort peu probable qu'ils partagent la volonté politique de certains États de mettre en place des outils d'identification sur Internet, tels qu'OpenID et IDénum.

Pour les hacktivistes, l'idéal serait de mettre en place un système qui s'affranchirait de l'obligation de souscrire un abonnement auprès des fournisseurs d'accès Internet pour pouvoir se connecter au réseau, ce qui priverait les États et les sociétés privées de tout contrôle. En effet, les hacktivistes sont parfaitement conscients que les systèmes d'information constituent un outil stratégique de contrôle des populations, ce qui a été confirmé publiquement par Edward Snowden, ancien consultant américain de l'Agence de Sécurité Nationale, dans ses déclarations au Guardian le 5 juin 2013. Dans la société de l'information, les intermédiaires techniques ont acquis un rôle déterminant et les hacktivistes souhaiteraient que ces médiateurs soient neutres, c'est-à-dire qu'ils transmettent l'information sans condition, ni discrimination à l'égard de la source, de la destination et du contenu.

Pour les hacktivistes, le manque de neutralité des intermédiaires techniques et la mise en place de systèmes de surveillance par les États, tel que XKeyscore, constituent d'ores et déjà des atteintes aux libertés fondamentales des individus. En effet, ceux qui maîtrisent les réseaux ont la capacité d'exercer des actions de surveillance et une censure en dehors de toute décision de justice, ce qui revient à leur confier la possibilité d'écrire les lois applicables sur tout le territoire et aboutit à la privatisation des pouvoirs de justice et de police. Face à cette menace, les hacktivistes veulent agir collectivement, de manière spontanée et autonome. Pour les hacktivistes, il n'y a pas de chef identifié, pas d'autorité, ce qui est cohérent avec leur volonté d'avoir un pouvoir " déconcentré ", non détenu par un seul organisme ou un seul groupe. Ces caractéristiques font qu'ils ne sont pas dotés d'une organisation hiérarchique et leur force réside essentiellement dans le pouvoir collectif exercé par leurs participants. Ils sont imprévisibles et veulent constituer une menace en échappant à tout contrôle et revendiquent dès lors le pouvoir agir, sans que les États puissent surveiller leurs discours, leurs évolutions et leurs actions. Ils réclament le droit de circuler en toute confidentialité sur la toile et utilisent par conséquent des logiciels d'anonymisation et la cryptologie pour chiffrer leurs échanges, ce qui n'est pas illégal.

Cela rend leur identification difficile, même s'il est toutefois possible d'en identifier certains, regroupés en collectif, qui en coordonnant leurs actions ont acquis une place sur la scène médiatique. C'est le cas pour les Anonymous, Télécomix, les Yes Men, les LulzSec pour n'en citer que quelques-uns. Les hacktivistes ont aussi pour but de redonner l'information aux citoyens qui en seraient privés et de leur permettre de s'exprimer en toute liberté. En effet, la liberté d'expression est à dimension variable selon les systèmes politiques mis en place par les États. « *Où il y a des conflits réels, où des dommages sont injustement causés, nous les identifierons et les traiterons avec nos propres moyens* » proclamait John P. Barlow en 1996.

Quels sont les outils utilisés par les hacktivistes pour agir et diffuser leurs messages politiques ?

Pour porter leurs revendications et exercer leur pouvoir de déstabilisation, notamment en termes d'image, les hacktivistes peuvent procéder à des intrusions informatiques (Dos, DDos, Dox…)[11], afin de collecter des informations confidentielles pour les divulguer au public ensuite. Les hacktivistes se sont aussi emparés d'Internet pour alerter et mobiliser l'opinion publique internationale, notamment face aux régimes dictatoriaux. A cette fin, les réseaux sociaux (Facebook, Twitter, Youtube…) ont été utilisés en Égypte, en Tunisie et en Libye, lors du printemps arabe en 2010 et 2011. Le but des hacktivistes est d'obtenir des soutiens au niveau international pour infléchir le rapport de forces engagé, au profit des opposants, auxquels ils apportent leur aide. Ainsi, Internet a profondément modifié le rapport des gouvernements et des régimes autoritaires avec les forces de l'opposition et les

[11] Dos : attaque informatique par déni de service - DDos : attaque informatique à l'aide de botnets - Dox : intrusion et extraction de données.

autorités étatiques ont très bien compris qu'il était dans leur intérêt de renforcer la maîtrise des outils numériques et de contrôler l'usage qui en est fait par les opposants et les hacktivistes.

Quels sont les moyens de répression mis en œuvre par les États pour maintenir l'ordre et la sécurité face aux agissements des hacktivistes ?

L'action des hacktivistes ne constitue plus seulement un contre-pouvoir au niveau national, mais également un facteur de déstabilisation au niveau international, notamment quand des informations classifiées secret défense sont livrées au public et à des puissances étrangères[12]. Par ailleurs, la participation active et directe aux hostilités de nombreux hacktivistes, lors des conflits armés, pose la question de leur possible assimilation à la catégorie des combattants. En principe, les hacktivistes ne peuvent pas être qualifiés de combattants puisqu'ils ne sont pas sous le « contrôle effectif » d'un État, partie au conflit. Cependant, ils peuvent perdre leur immunité de personnes civiles et être pris pour cible par les forces armées, quand leur objectif est de provoquer des pertes en vie humaine, des blessures aux personnes, des dommages aux biens mais aussi de nuire directement aux opérations militaires ou à la capacité militaire de l'adversaire, selon les limitations du droit international humanitaire. Le Manuel de Tallinn de 2013 envisage cette possibilité en cas d'attaques menées par des hackivistes relevant d'un niveau de gravité suffisant et causant un préjudice important. Reste à déterminer précisément le seuil permettant de qualifier l'action des hacktivistes d'acte suffisamment grave et préjudiciable.

Si l'on exclut l'hypothèse des pertes en vie humaine, a priori peu compatible avec les valeurs des hacktivistes qui associent régulièrement leurs actions avec des organismes humanitaires lors des conflits, les attaques menées contre les réseaux informatiques des armées seraient suffisamment graves pour justifier que les hacktivistes soient ciblés par les militaires et mis hors d'état de nuire. En revanche, l'attaque, par les hacktivistes, des réseaux informatiques civils, dans le but de porter atteinte aux intérêts économiques d'un État ennemi par exemple, ne relèverait pas d'un niveau de gravité suffisant pour considérer qu'ils participent activement aux hostilités. Il serait alors impossible pour les forces armées de les prendre pour cible dans cette hypothèse, sauf si les dommages causés aux hacktivistes civils ne sont pas excessifs par rapport à l'avantage militaire direct, concret et attendu selon l'article 51 (5) b du Protocole additionnel aux Conventions de Genève du 8 juin 1977.

Cette question est toujours discutée à l'heure actuelle, mais face à cette nouvelle menace que représente l'hacktivisme, certains organismes gouvernementaux, qui s'étaient cantonnés autrefois à un rôle de veille, d'alerte et de recueil de renseignements, utilisent désormais la loi nationale et internationale pénale pour sanctionner les agissements des hacktivistes, hors des conflits armés, en qualité de civils et d'acteurs non-étatiques du cyberespace. En effet, les intrusions informatiques, pratiquées par les hacktivistes, sont clairement réprimées par la plupart des législations criminelles de différents pays[13]. Pour assurer l'effectivité des poursuites et des condamnations, encore faut-il que le principe de la double incrimination s'applique entre les États. A ce titre, une coopération internationale a été mise en place pour harmoniser les législations nationales. Plusieurs initiatives ont vu le jour, de différents organismes, tels que le G8, l'O.C.D.E, l'O.N.U. ou l'Union Internationale des Télécommunications notamment. Mais le seul texte international ayant une réelle portée juridique à

[12] Bradley Manning , analyste pour l'armée américaine en Irak en 2010, accusé d'avoir téléchargé illégalement et diffusé par le biais du site Wikileaks, des documents confidentiels de l'armée américaine, risque la prison à perpétuité. Il était poursuivi pour 22 chefs d'accusation, mais s'il a été reconnu coupable d'espionnage, la « collusion avec l'ennemi » a été rejetée par le Tribunal militaire de Fort Meade le 30 juillet 2013

[13] En Europe, 36 pays sur 46 ont mis en place une législation spécifique, en Asie 23 sur 44, en Afrique 9 sur 52, en Amérique (Centrale, du Nord et du Sud) 10 sur 35 et en Asie 23 sur 44, selon M. Mohamed CHAWKI, Docteur en Droit, Fondateur de l'Association Internationale de lutte contre la cybercriminalité.

l'heure actuelle est la convention de Budapest de 2001[14] ratifiée par 39 pays membres du Conseil de l'Europe, mais également par les Etats-Unis, l'Australie et le Japon. Toutes les législations de ces pays répriment les intrusions informatiques[15], l'interception et la diffusion illégale de données personnelles et confidentielles, ainsi que la divulgation d'informations classifiées qui aurait pour effet de nuire à la défense nationale[16]. Par conséquent, la mise en ligne, par des hacktivistes, d'éléments pour discréditer une entreprise, un groupe politique ou religieux, rendre publiques les données confidentielles d'un ministère, dans le but de redonner l'information à la population, est illégale[17].

Par ailleurs, le fait de détenir ou de mettre à disposition d'autrui des outils pour commettre des intrusions informatiques, comme c'est le cas de certains groupes d'hacktivistes, pour redonner aux opposants le pouvoir sur les réseaux, est également sanctionné[18]. Les hacktivistes se regroupent souvent pour garantir une meilleure efficacité de leurs actions.

Or, la seule participation à un groupement formé ou à une entente établie, en vue de préparer des intrusions informatiques, est réprimée par la loi[19]. On comprend mieux la volonté d'anonymat de certains collectifs d'hacktivistes pour ne pas rendre possible l'identification de leurs membres. Certes, les peines encourues varient d'un pays à l'autre, mais le fait que ces infractions soient prévues par les lois pénales permet les poursuites. Dans le cadre des enquêtes, les pays sont tenus de s'accorder l'entraide la plus large possible. Concrètement, les États doivent divulguer rapidement les données de connexion conservées pour identifier les hacktivistes, lorsqu'il est avéré que le fournisseur d'accès d'un État a participé à la transmission de communications, au profit des hacktivistes. Ainsi, si les agissements des hacktivistes dépassent les frontières et rendent les poursuites pénales difficiles, leur condamnation n'est pas impossible, comme l'a prouvé l'arrestation par Interpol en juillet 2012[20] et la condamnation de certains Anonymous à des peines de prison ferme le 22 janvier 2013 au Royaume-Unis[21]. Les peines prononcées contre les hacktivistes tiennent bien évidemment compte de l'importance des attaques informatiques réalisées, mais surtout du degré de classification des données divulguées. Par ailleurs, si l'hacktiviste appartient au personnel militaire, comme c'est le cas de Bradley Manning, analyste du renseignement américain en Irak, la condamnation sollicitée sera bien évidemment beaucoup plus lourde, eu égard aux qualifications d'espionnage et de collusion avec l'ennemi. La sanction est également proportionnelle à la menace que représente le phénomène hacktiviste pour les États. Ainsi, les États-Unis prennent-ils très au sérieux la menace hacktiviste.
Par conséquent, les intrusions informatiques sont considérées comme un crime fédéral et les peines encourues sont de 5 ans d'emprisonnement et de 250.000,00 $ d'amende. Les condamnations prononcées devant les tribunaux sont sévères[22], contrairement aux décisions de justice rendues par les juridictions européennes, qui sont le plus souvent des peines de quelques mois de prison avec sursis[23].

Cela s'explique car les États-Unis ont connu les plus importantes divulgations de données protégées par le secret de défense nationale, qui ont pu être livrées à des puissances étrangères et donner un avantage certain à leurs adversaires. Face à cette lutte législative engagée contre les hacktivistes, ces derniers peuvent-ils compter sur le soutien de certains États ? En effet, les États sont tenus de

[14] Conventions.coe.int/treaty/fr/Treaties/Html/185.htm
[15] Réprimées en France par 2 ans d'emprisonnement et 30.000 € d'amende et 5 ans d'emprisonnement et 75.000€ d'amende (Articles 323- et suivants du Code Pénal).
[16] Puni de 5 ans d'emprisonnement et 75.000 € d'amende par l'article 413-11 alinéa 3 du Code Pénal.
[17] Publications de données personnelles de policiers et de gendarmes (photos, profils facebook) sur le site CopWatch et Fafwatch dont l'accès a été bloqué en France par décision de justice en 2011.
[18] Par l'article 323-3-1 du Code Pénal.
[19] Article 323-4 du Code Pénal.
[20] lexpansion.lexpress.fr/.../arrestation-de-25-hackers-lies-a-anonymous
[21] http://zataz.com/news/22658/jugement-prison-anonymous.html
[22] Kevin Mitnick arrêté par le FBI et condamné à 5 ans de prison en 1995 pour intrusions informatiques.
[23] Un hacktiviste français condamné à 4 mois de prison avec sursis et à 300 € pour avoir défacé le site du Front National par le Tribunal Correctionnel en 2008 – www.legalis.net/spip.php?page=jurisprudencedecision&id_article=2539

s'accorder l'entraide judiciaire la plus large possible pour lutter contre le phénomène hacktiviste, mais quelle est la limite apportée à cette coopération internationale ? Si un État considère que la demande d'investigation porte sur une infraction de nature politique ou s'il estime que son concours aurait pour effet de porter atteinte à sa sécurité, son ordre public ou d'autres intérêts essentiels, cet État peut refuser de coopérer. Ainsi, certains États peuvent-ils s'abstenir d'apporter leur aide pour permettre l'identification et l'arrestation de certains hacktivistes, s'ils estiment que les agissements de ces derniers sont légitimes, notamment face à la répression exercée par certains régimes dictatoriaux.

Par ailleurs, un État peut également offrir l'asile politique à un hacktiviste dûment recherché, s'il estime son action utile ou servant ses intérêts, comme l'a accordé l'Équateur à Julian Assange, fondateur WikiLeaks et la Russie à Edward Snowden le 1er août 2013[24]. Enfin, en ultime recours, les États peuvent décider de ne pas employer la loi, mais le recours à la force ou à la loi du talion, pour lutter contre les agissements des hacktivistes. En effet, face à l'action offensive des hacktivistes, certains gouvernements vont utiliser les mêmes armes et les retourner contre les opposants pour brouiller leur message sur les réseaux sociaux. On reviendra alors à une classique guerre de l'information et de la désinformation. Ainsi, en Syrie, fort de l'expérience du renversement des gouvernements égyptien, tunisien et libyen, le gouvernement est parvenu à utiliser des logiciels espions pour s'immiscer dans les communications entre les hacktivistes et les opposants sur les réseaux sociaux et intercepter les échanges visant à coordonner leurs actions. De fausses pages Facebook ou Youtube ont également été créées pour recueillir les identifiants et les mots de passe des utilisateurs par le biais du phising, l'accès au réseau Tor utilisé par les hacktivistes pour anonymiser leurs échanges avec les dissidents a été bloqué et certains comptes Twitter des opposants ont été piratés[25].

Conclusion

Les hacktivistes se sont emparés d'Internet pour alerter et mobiliser l'opinion publique internationale. Face à leurs actions, les États ont adapté leur réponse législative et répressive contre les hacktivistes, quand ils estiment que leurs agissements présentent une menace importante, de nature à remettre en question leur sécurité nationale, notamment par la divulgation de données confidentielles de leurs armées. Certains États ont coordonné l'action de leurs services de renseignements pour mettre en œuvre une véritable politique de cyberdéfense, afin de neutraliser toute tentative de soutien à leurs opposants, quand ils sont en mesure d'anticiper l'action des hacktivistes.

D'autres États n'hésitent plus à poursuivre les hacktivistes devant la justice et à obtenir leur condamnation, pour toute action illégale relative aux intrusions informatiques et à la divulgation de données classifiées, s'ils considèrent que leurs agissements constituent une réelle menace contre leur sécurité. Le recours à la loi est un outil efficace, car il permet aux États de communiquer sur leur capacité technique à identifier les hacktivistes, malgré la connaissance des systèmes d'information de ces derniers.

Par ailleurs, le recours à la loi et la condamnation des hacktivistes jouent un rôle dissuasif quand les peines encourues sont sévères. A ce jour, les hacktivistes ont essentiellement la volonté de garantir la liberté d'expression et de soutenir les opposants à un régime dictatorial. Ils peuvent certes déstabiliser un régime qui cherche à tout prix à se maintenir en place et ils ont parfaitement compris que les systèmes d'information revêtent à ce titre un enjeu stratégique, mais si leur rôle est fort symboliquement, il n'est pas déterminant dans l'issue d'un conflit.

Les risques qu'ils prennent quand ils ont recours à des actes illégaux peuvent être importants et sont-ils conscients de leur possible instrumentalisation pour servir les intérêts géostratégiques, politiques et financiers des États dans la guerre de l'information ? En effet, on peut s'interroger sur la fourniture de

[24] Julian Assange, fondateur du site WikiLeaks, a publié des documents militaires et fait des révélations importantes dans le domaine nucléaire et sur les stocks d'armes. A ce titre, il risque une lourde peine. Il est sous la protection de l'Équateur depuis juin 2012.

[25] « nouvelles guerres de l'information » : le cas de la Syrie – C. Pigot et A.Durand CEIS novembre 2012

matériel informatique, par des sociétés américaines, à des hacktivistes, pour leur permettre de mener leurs actions en Syrie, lorsque l'on sait que la Chine et la Russie soutiennent le régime syrien en place. Face au comportement des États à leur égard, à la possibilité d'être pris pour cible par les forces armées lors des conflits quand ils participent directement aux hostilités, les hacktivistes souhaiteraient aujourd'hui créer de nouveaux modes d'action, tout aussi efficaces mais moins compromettants, pour pérenniser leur présence sur la scène internationale.