ASPJ–Afrique et Francophonie 4e Trimestre 2017

ASPJ–Africa and Francophonie 4th Quarter 2017

ASPJ Afrique et Francophonie

4e trimestre 2017 Volume 8, No. 4

Briser le mythe de la cause unique d'une insurrection
Daniel G. Cox, PhD
Alex Ryan, PhD

L'irrationnelle rationalité du terrorisme
Robert Nalbandov, PhD

Interagir avec les prestataires non étatiques des services de sécurité
Où va l'état de droit?
Timothy Donais, PhD

La stratégie des « Trois guerres » de la Chine ou comment atténuer les retombées du cyberespionnage
Emilio Iasiello

L'opérationnalisation de la protection des civils dans les opérations de l'OTAN
Marla B. Keenan
Alexander Beadle

AIR & SPACE POWER JOURNAL

VISER HAUT . . . VOLER, COMBATTRE ET GAGNER

Air and Space Power Journal (ISSN 1931-728X) est publié trimestriellement. Cette revue est conçue pour servir de forum ouvert à la présentation et à la stimulation de réflexions innovatrices sur la doctrine militaire, la stratégie, la tactique, la structure de force, la préparation et d'autres sujets de la défense nationale. Les points de vue et les opinions exprimés ou implicites dans cette revue sont ceux des auteurs et ne devraient pas être interprétés comme portant la sanction officielle du département de la Défense, de l'armée de l'Air, du Commandement de l'éducation et de la formation des forces aériennes, de l'*Air University*, ou d'autres agences ou départements du gouvernement des États-Unis.

http://www.af.mil

http://www.aetc.randolph.af.mil

http://www.au.af.mil

ASPJ–Afrique et Francophonie
600 Chennault Circle
Maxwell AFB AL 36112-6026
USA
Télécopieur : 1 (334) 953-1645
courriel aspj.french@us.af.mil

Visitez *Air and Space Power Journal* en ligne à http://www.airuniversity.af.mil/ASPJ/

ASPJ Afrique et Francophonie

4e trimestre 2017 Volume 8, No. 4

Choix de l'éditeur

La stratégie des « Trois guerres » de la Chine ou comment atténuer les retombées du cyberespionnage, Briser le mythe de la cause unique d'une insurrection, Interagir avec les prestataires non étatiques des services de la sécurité : Où va l'état de droit ?, L'irrationnelle rationalité du terrorisme, et L'opérationnalisation de la protection des civils dans les opérations de l'OTAN 2
Rémy M. Mauduit

Articles

Briser le mythe de la cause unique d'une insurrection. 5
Daniel G. Cox, PhD
Alex Ryan, PhD

L'irrationnelle rationalité du terrorisme 25
Robert Nalbandov, PhD

Interagir avec les prestataires non étatiques des services de sécurité Où va l'état de droit ? 40
Timothy Donais, PhD

La stratégie des « Trois guerres » de la Chine ou comment atténuer les retombées du cyberespionnage 57
Emilio Iasiello

L'opérationnalisation de la protection des civils dans les opérations de l'OTAN. 81
Marla B. Keenan
Alexander Beadle

Choix de l'éditeur

La stratégie des « Trois guerres » de la Chine ou comment atténuer les retombées du cyberespionnage, Briser le mythe de la cause unique d'une insurrection, Interagir avec les prestataires non étatiques des services de la sécurité : Où va l'état de droit ?, L'irrationnelle rationalité du terrorisme, et L'opérationnalisation de la protection des civils dans les opérations de l'OTAN

Une insurrection peut naître d'une seule cause. Les insurgés s'identifient à cette cause unitaire, la communiquent à la population, si bien que leur conviction reste inébranlable même quand la contre-insurrection neutralise leurs activités et répond aux motifs d'insatisfaction. Tel est le postulat de Daniel Cox et Alex Ryan dans *Briser le mythe de la cause unique d'une insurrection*. Car bien souvent la cause n'est pas unique. Plusieurs motivations sous-tendent le soulèvement du peuple. Et avant même que les forces contre-insurrectionnelles n'aient résolu l'objet initial des griefs, les meneurs avancent de nouvelles justifications pour continuer à bénéficier d'un large appui populaire. Un scénario qu'il serait sage de prendre en compte dans toute stratégie de contre-insurrection, étant donné les compétences et la grande capacité d'adaptation des chefs contestataires. Même si cette théorie est reconnue dans la littérature sur la guerre contre-insurrectionnelle, elle passe sous silence la façon dont elle influe sur l'approche opérationnelle. Les auteurs comblent cette lacune en offrant une trame afin de cartographier avec précision, de comprendre, d'anticiper et de résoudre les différentes causes de l'insurrection et de sa persistance.

Dans l'article *L'irrationnelle rationalité du terrorisme,* Robert Nalbandov examine le problème ontologique que pose l'application d'un cadre de choix rationnels à l'étude du terrorisme. L'auteur examine les itérations « anciennes » (antérieures à la fin de la guerre froide) et « nouvelles » (postérieures à la fin de la guerre froide) du terrorisme par le prisme de la rationalité. Après en avoir analysé les principes fondamentaux, il examine la rationalité à deux niveaux différents, l'individu (les acteurs) et le groupe (le collectif), et sous deux perspectives, la tactique (à court terme) et la stratégie (à long terme). L'article explique

en somme que, si les itérations passées du terrorisme s'expliquent par la théorie du choix rationnel, les nouvelles itérations s'écartent considérablement de la rationalité.

La primauté de l'état de droit est de longue date considérée comme un principe essentiel dans la programmation de la réforme du secteur de la sécurité (RSS). Du reste, le discours global sur la RSS souligne que la redevabilité des prestataires de services de sécurité est mieux garantie en intégrant la gouvernance de la sécurité dans un cadre d'état de droit. Dans *Interagir avec les prestataires non étatiques des services de sécurité : Où va l'état de droit ?*, Timothy Donais explique que reconnaître l'existence d'une prestation non étatique dans le secteur de la sécurité remet en question la vision selon laquelle la RSS n'est que le prolongement de l'état de droit dans le domaine de la sécurité. En effet, quelle que soit la légitimité des prestataires de services de sécurité, elle tire son origine dans des fondements *extrajuridiques*. En proposant une analyse plus conceptuelle qu'empirique, l'article envisage les implications des formes hybrides de gouvernance de la sécurité pour définir les contours de la relation entre RSS et promotion de l'état de droit. L'auteur explique que l'état de droit fournit des axes stratégiques utiles pour élaborer le plan d'action de la RSS.

Dans l'article *La stratégie des « Trois guerres » de la Chine ou comment atténuer les retombées du cyberespionnage*, Emilio Iasiello affirme que la Chine s'est engagée, de longue date, dans des activités de cyber espionnage contre les États-Unis et d'autres nations. Cette stratégie vise à collecter, dans les secteurs public et privé, des informations sensibles afin de réaliser les objectifs nationaux définis par le douxième plan quinquennal. Les gouvernements étrangers ont tancé le régime chinois sur ses activités délictueuses, des accusations énergiquement démenties par Pékin. La Chine riposte par les « Trois guerres », une stratégie militaire de contrôle de l'information à trois dimensions, médiatique, juridique et psychologique, dans le but de tromper la communauté internationale. Si les États-Unis ont brandi la menace d'imposer des sanctions économiques, Pékin a pu parer le coup en arrêtant des hackers identifiés par le gouvernement américain, comme gage de la volonté du régime chinois à maintenir un cyberespace stable et pacifique. Par ses disciplines imbriquées, la stratégie des « Trois guerres » cible le processus cognitif du leadership américain et vise à donner de la Chine l'image d'une menace à l'échelle internationale. C'est ainsi que le régime chinois évite l'application de toutes mesures effectives de rétorsion ou de dissuasion économique, voire de cyber sanctions.

Dans *L'opérationnalisation de la protection des civils dans les opérations de l'OTAN,* Marla Keenan et Alexander Beadle affirment que si l'OTAN et les autres forces armées admettent de plus en plus que la protection des civils est un objectif clé de leurs opérations, sa mise en œuvre reste compliquée. Pour assurer une protection effective, la force militaire doit comprendre les menaces spécifiques existantes et adapter les moyens destinés à les contrer. Selon les auteurs, les planificateurs militaires doivent s'appuyer sur une structure plus formelle afin de conceptualiser la protection physique. Ils proposent « l'échelle de la protection » comme outil permettant aux planificateurs et aux chefs militaires d'expliquer les obligations légales

et de déterminer les capacités opérationnelles nécessaires à la protection des civils. L'article formule des suggestions pratiques sur la façon dont la protection des civils peut être assurée efficacement avant, pendant et après les opérations militaires. L'OTAN devrait accroître ses capacités de protection, car le succès des missions futures en dépend.

Rémy M. Mauduit, Éditeur
Air and Space Power Journal–Afrique et Francophonie
Maxwell AFB, Alabama

Briser le mythe de la cause unique d'une insurrection

Daniel G. Cox, PhD*
Alex Ryan, PhD**

Tant de choses ont déjà été écrites sur l'importance de conquérir « le cœur et l'esprit » lors d'une insurrection et sur le rapport de cette approche à la cause des insurgés[1]. Il convient cependant d'admettre que la plupart des articles analysant les causes de l'insurrection tendent à se concentrer sur ses éléments déclencheurs, en dressant la liste des problématiques, des griefs ou des invectives qui ont suffisamment interpellé les cœurs et les esprits de la population pour la motiver à se rebeller. Si les événements de crise et les griefs initiaux peuvent servir de catalyseur pour la mobilisation d'un mouvement insurrectionnel, on constate souvent rétrospectivement que les tensions sociales sous-jacentes ont fomenté la rébellion avant et après l'étincelle apparemment critique. Ainsi, les mouvements d'insurrection continuent d'identifier les tensions sous-jacentes dans une société et d'en tirer parti pour faire avancer le mouvement et accroître la participation. Dans de nombreux cas, les multiples tensions et propensions qui nourrissent l'insurrection se chevauchent et s'entremêlent, tissant une toile complexe qui suscite confusion et incompréhension au sein de la communauté académique et militaire désireuse de trouver des moyens efficaces pour désamorcer les causes de l'insurrection.

Une insurrection peut en effet se développer à partir d'une cause unique, que les insurgés peuvent identifier et communiquer à la population dans le but de rester fermement unis autour de ce qui les rassemble, même lorsque les mouvements contre-insurrectionnels minent leur organisation et rectifient la cause du problème. Mais souvent, la cause n'est pas unique et le soutien populaire est mobilisé sur la base de

*Daniel G. Cox est professeur agrégé de sciences politiques à la School of Advanced Military Studies et professeur auxiliaire au sein de l'American Military University. Dr. Cox a publié plusieurs ouvrages ainsi que des articles dans plusieurs scientifiques à comité de lecture. Il collabore également à un projet de plus grande envergure sur l'avenir de la guerre.

**Alex Ryan est conseiller principal en conception de systèmes auprès du gouvernement de la province canadienne d'Alberta. Il est le cofondateur de l'Alberta CoLab et du Systemic Design Research Network. Il co-préside le *Relating Systems Thinking and Design Symposium*.

COX, Daniel G., et RYAN, Alex, « Countering Insurgency and the Myth of "The Cause" », *Journal of Strategic Security* 8, n° 1, 2015, pp 43-62. DOI: http://dx.doi.org/10.5038/1944-0472.8.1.1419. Accessible à l'adresse : http://scholarcommons.usf.edu/jss/vol8/iss1/4

motivations aux origines multiples. Au moment où les mouvements contre-insurrectionnels ont apporté une réponse aux griefs initiaux, l'insurrection a déjà trouvé d'autres justifications pour poursuivre la mobilisation du soutien populaire. Dans la mesure où le leadership de l'insurrection est souvent composé d'individus compétents et doués de bonnes facultés d'adaptation, il serait sage de tenir compte de ce scénario lors du choix de la stratégie contre-insurrectionnelle. Pourtant, même si elle est reconnue dans la littérature spécialisée, la théorie reste étonnamment silencieuse quant à la façon dont cela affecte le choix de l'approche opérationnelle. Nous devons donc nous aventurer en dehors des théories contre-insurrectionnelles (COIN) classiques présentées dans les revues spécialisées pour combler cette lacune.

Le présent article s'articule autour de la structure suivante. La prochaine section se penchera brièvement sur la façon dont les théories COIN abordent la question des tensions sous-jacentes et des causes de l'insurrection. Elle sera suivie de deux études de cas, aux Philippines et en Indonésie, qui illustrent la façon dont les propensions et les tensions au sein d'une société donnée suscitent et soutiennent la cause de l'insurrection. Les auteurs du présent article présenteront ensuite un cadre permettant d'analyser des insurrections ayant plus d'une cause potentielle. Ce cadre s'accompagne d'un certain nombre d'applications pratiques pour la stratégie COIN, que nous développerons dans la dernière section.

La notion de « cause » dans la théorie contre-insurrectionnelle.

Le lien établi très tôt par Roger Trinquier entre les tensions sous-jacentes dans une société et la formation des mouvements insurgés semble constituer un bon point de départ pour notre discussion. Trinquier note ainsi :

> La guerre est un système entrecroisé d'actions – politiques, économiques, psychologiques, militaires – qui vise *le renversement de l'autorité établie dans un pays et son remplacement par un autre régime*. Pour parvenir à ce but, les « agitateurs » essaieraient d'exploiter les tensions internes du pays attaqué – idéologiques, sociales, religieuses, économiques – et tout conflit susceptible d'avoir une influence profonde sur la population à conquérir [italique dans l'original][2].

Trinquier identifie quatre grandes catégories de tensions dans la citation susmentionnée : idéologique, sociale, religieuse et économique. Ces dernières ensemble couvrirent la plupart des griefs spécifiques qui pourraient émaner d'un groupe sociétal est utilisé par un mouvement insurrectionnel opportuniste ou un groupe d'insurgés afin de développer une cause qui peut être utilisée pour rallier le soutien du plus grand nombre. Trinquier souligne également que les tensions pouvant être à l'origine d'une insurrection ne connaissent pas de limites, même en 1964. Il observe ainsi que : « d'un conflit localisé à l'origine est d'importance secondaire, ils s'efforceront toujours, dans des délais plus ou moins long, de faire un conflit généralisé[3] ».

Il est cependant assez paradoxal de voir Trinquier considérer les tensions sous-jacentes comme un élément fondamental de l'émergence et au maintien d'une insurrection, et de le voir ensuite consacrer le reste de son ouvrage à expliquer comment le contrôle des populations et des ressources – par l'intermédiaire de recensements précis, d'opérations de renseignement et visant à limiter et contrôler les mouvements – constitue la clé de la victoire. Ses observations initiales sur les tensions semblent s'être évaporées ensuite, et il nous donne presque l'impression d'avoir tenu pour acquis qu'une fois l'insurrection lancée, il convient d'y faire face en usant de méthodes quasiment similaires à celles employées par les insurgés : la répression de la population plutôt que la résolution des causes du mouvement.

Galula met davantage l'accent sur la nécessité de la cause et note que « les problèmes de toutes natures sont exploitables pour une insurrection[4] ». Mais il ne parle pas de ces problèmes en termes de tensions ou même de griefs au niveau local, mais se concentre plutôt sur les facteurs qui rendent une cause juste et durable. Tandis que Trinquier explique bien le rôle des tensions dans la genèse des causes, Galula formule, de façon beaucoup plus opportune, des moyens permettant de s'attaquer aux tensions sous-jacentes et de saper ainsi la cause des insurgés. Galula soutient que même après le déclenchement de la violence armée par l'insurrection, une bonne stratégie COIN consisterait à faire des recherches sur les revendications des insurgés et à dresser une liste que les mouvements contre-insurrectionnels utiliseront immédiatement pour identifier les griefs faciles à résoudre. Si cette approche porte ses fruits, l'insurrection dans son ensemble peut être contrecarrée grâce à la résolution des principaux griefs ou tensions que les insurgés ont à mis à profit à l'origine pour favoriser l'émergence de l'insurrection[5].

Propensions et tensions qui alimentent la cause des insurgés

Pour comprendre la dynamique des insurrections, il est particulièrement important de tenir compte du contexte historique et culturel. L'histoire et la culture d'un état-nation, d'un groupe identitaire ou d'une région constituent une source importante de tensions sous-jacentes. La mémoire collective des acteurs, entretenue par les récits historiques qui remontent souvent à plusieurs centaines de milliers d'années, joue un rôle prépondérant, en guidant et en limitant les actions à venir.

Lorsqu'elle fait référence à la propension d'une situation, la présente étude fait référence à l'influence des événements, des idées et des émotions du passé sur les événements futurs. Il ne s'agit pas d'une relation déterministe entre les états passés et futurs, mais plutôt un conditionnement des possibilités de l'avenir en fonction du passé. Par exemple, l'exploitation par les états-nations occidentaux des anciennes colonies pourrait placer un groupe de contre-insurgés dans la position peu enviable de devoir « combattre » l'histoire, ou à tout le moins la perception historique, simplement

pour être accepté comme un acteur légitime par la population locale. Cette société est susceptible d'avoir une propension pour la xénophobie et la défiance vis-à-vis de toute intervention externe.

Il existe de multiples groupes d'insurgés qui ont mené des opérations, ou qui le font toujours, aux Philippines, dont le Groupe Abou Sayyaf (GAS), le Front Moro de Libération nationale (FMLN), et le Front Moro islamique de libération (FMIL). Ces différents groupes ont démontré une très faible synergie opérationnelle. En réalité, le GAS et le FMIL sont des groupes dissidents du FMLN. Cependant, il partage une propension commune majeure avec leurs partisans au sein de la société civile : ils considèrent le gouvernement national et tout intervenant militaire étranger agissant sur leur territoire au nom du gouvernement national comme une simple extension de la répression injuste et brutale contre les musulmans qui a commencé lors de la colonisation espagnole.

Le cas des Philippines

L'islam a été introduit aux Philippines au XIII^{e} siècle. À l'origine, il était isolé aux îles Sulu, mais il s'est ensuite propagé pour englober non seulement les îles Sulu, mais aussi la quasi-totalité de l'île méridionale de Mindanao. Les conquistadors espagnols sont arrivés peu après la propagation de l'islam en 1565 et un effort de colonisation brutal a été entrepris pendant trois cent trente-quatre ans[6]. Les Espagnols ont fini par céder le contrôle des Philippines aux États-Unis en 1898, mais cela a entraîné presque immédiatement des hostilités entre les États-Unis et les Philippines et, finalement, la guerre américano-philippine (1899-1902). Cette guerre sanglante fit plus de 7 000 victimes américaines et beaucoup plus encore du côté philippin. Elle coûta également aux États-Unis quelque 400 millions de dollars[7]. L'objectif des États-Unis était de permettre la mise en place d'un gouvernement autonome aux Philippines[8]. Bien que la loi sur l'indépendance des Philippines de 1934 ait été élaborée pour garantir la liberté et la souveraineté de l'État, les dommages causés pendant la guerre, conjugués à l'expérience coloniale espagnole, ont créé une profonde méfiance à l'égard de l'intervention militaire étrangère, en particulier chez les musulmans du Sud[9].

L'animosité de cet héritage historique et la méfiance des étrangers qui en résulte ne sont que l'un des nombreux aspects dont il faut tenir compte lorsqu'on intervient dans les régions des Philippines majoritairement musulmanes. Compte tenu de cet obstacle, la trajectoire réussie des forces spéciales américaines poursuivant l'opération des forces d'opérations spéciales interarmées des Philippines (JSOTF-P) mérite d'être soulignée. L'utilisation de l'approche indirecte par les forces spéciales américaines, qui s'est manifestée par des opérations menées par, avec et par l'intermédiaire de l'armée philippine, a peut-être permis aux forces spéciales américaines d'atténuer la propension négative décrite ci-dessus.

Malheureusement, les propensions ne sont pas la seule partie critique de l'environnement opérationnel qu'un contre-insurrectionnel doit identifier et affronter. Les tensions sous-jacentes sont également un aspect important qui nourrit la cause des insurgés. Des tensions existent chaque fois que deux ou plusieurs forces opposées coïncident. Pour ce qui est des insurrections, nous sommes particulièrement intéressés par les tensions découlant des conflits de valeurs, que ce soit au sein même des groupes concernés ou entre eux. La possible superposition de ces tensions induit un problème de transparence. Cette situation peut, à son tour, créer un problème de lien causal, par lequel le mouvement contre-insurrectionnel s'attaque aux tensions les plus récentes exploitées par les insurgés, sans s'attaquer aux tensions ou aux causes profondes qui ont d'abord ou plus fondamentalement alimenté la cause de l'insurrection. Inversement, de nouvelles tensions peuvent avoir remplacé les anciennes, créant une situation où le mouvement contre-insurrectionnel perd son temps et ses ressources à s'attaquer aux tensions initiales, qui ont certes été à l'origine du mouvement mais qui ne sont plus actives.

Le cas de l'Indonésie

La région de Banda Aceh, en Indonésie, située à la pointe nord de l'île de Sumatra, est un exemple des tensions multiples qui peuvent alimenter une insurrection. L'Indonésie est une mosaïque de peuples disparates, dont beaucoup n'ont en commun que l'expérience historique de la répression du colonialisme hollandais. Le régime dictatorial de Sukarno et de Suharto, bien que très brutal, a contribué à forger une identité nationale indonésienne forte. Mais même cette situation était fragile, et la situation économique et le traitement peu reluisant réservé à la population du Timor oriental a fini par conduire à la petite île méridionale à se détacher de l'état-nation indonésien. Les Papous de Papouasie occidentale et les Acehnais du nord de Sumatra ont eux aussi exprimé leur désir d'indépendance.

Le découpage en strates des tensions qui alimentent la rébellion contre le gouvernement indonésien est particulièrement évident dans le cas de l'Aceh ; il sera brièvement décrit ici. Le peuple de la province d'Aceh a beaucoup souffert de la fondation de la nation sous le règne du président Megawatti. Sous le Président Suharto, l'Indonésie a été témoin de nombreuses persécutions à l'encontre de groupes extérieurs. Développant sa vision dictatoriale du « Nouvel Ordre », Suharto a imposé un régime autoritaire pour poursuivre le développement économique. Il a d'abord visé les communistes, pour aboutir à l'interdiction de tous les partis de ce mouvement[10]. Après s'être chargé des communistes, Suharto s'est tourné vers les militants politiques musulmans, persécutant les principaux dirigeants et mouvements[11].

Il est compréhensible qu'un mouvement de résistance, connu sous le nom de Mouvement Aceh Libre, Gerakan Aceh Merdeka (GAM), se soit formé et qu'il ait rapidement attiré de violentes répressions du gouvernement indonésien. Ce mouve-

ment a été qualifié d'organisation terroriste par le gouvernement central, mais rien ne prouve que le GAM ait jamais perpétré une attaque contre des cibles civiles. Les auteurs actuels estiment qu'il serait plus judicieux de qualifier le GAM de mouvement insurrectionnel ou sécessionniste, bien que la plupart des actions entreprises par les membres du GAM relèvent du domaine de la protestation pacifique. Malgré ces éléments, le GAM constituait une menace pour le contrôle indonésien de la province d'Aceh et plusieurs affrontements violents notables ont eu lieu entre les membres du GAM et l'armée indonésienne.

Le tsunami de 2005, qui a fait plus de 160 000 victimes, a bouleversé le paysage et donné au gouvernement indonésien et aux États-Unis l'occasion d'intervenir et de fournir une aide d'urgence et une aide à plus long terme pour reconstruire la province sinistrée. Susilo Yudhayono n'avait que récemment remplacé Megawatti au poste de président, mais il a décidé de tendre la main à la population d'Aceh en offrant une participation aux bénéfices provenant des énormes réserves de gaz naturel au large de la côte d'Aceh, ainsi qu'une plus grande participation à la politique indonésienne[12]. La stabilité est vite revenue dans la région et le GAM est entré dans une période d'inactivité. Cela aurait été la fin de l'histoire, sauf qu'une nouvelle tension de fond s'était déjà développée, alimentée par les mêmes mauvais traitements que le peuple d'Aceh avait subis de la part du gouvernement national.

La propension à la méfiance à l'égard du gouvernement central, engendrée par une succession ininterrompue de présidents prêts à utiliser des tactiques militaires brutales contre les Acehnai, de Sukarno à Megawatti, est aujourd'hui en train de se mêler à une tension engendrée par le groupe terroriste régional Jemaah Islamiyah (JI), entre fondamentalisme religieux et laïcité. Par conséquent, en dépit de l'aide massive apportée à la province après le tsunami de 2005, et malgré les récentes concessions politiques et locales accordées par le gouvernement indonésien à la province d'Aceh, un mouvement islamique fondamental fort est en train de se former. Il convient de noter qu'il s'agit d'un développement nouveau dans l'histoire indonésienne[13]. En 2003, le premier tribunal de la charia d'Aceh a ouvert ses portes. Les chefs religieux locaux avaient initialement promis que l'application de la charia serait « modérée » et que les droits de l'homme ne seraient pas violés. Mais une bastonnade publique n'était, par exemple, pas exclue, comme punition pour ne pas avoir assisté à la prière du vendredi[14]. Toute prétention à la modération reste éphémère. À l'automne 2009, de nouvelles lois ont été adoptées. Elles stipulent que « les personnes mariées reconnues coupables d'adultère peuvent être condamnées à mort par lapidation. Les célibataires peuvent être condamnés à 100 coups de canne[15] ».

De même, une unité de police spécialisée, Wilayatul Hisbah, patrouille actuellement dans les rues d'Aceh, cherchant à perturber ou à arrêter « les couples non mariés, les femmes musulmanes sans foulard ou portant des vêtements moulants, et les personnes qui boivent de l'alcool ou jouent », ce qui semble viser à combattre l'influence

occidentale, en particulier l'influence qui s'est infiltrée dans la région lorsque les pays occidentaux ont fourni une aide après le tsunami[16]. Même si certains citoyens d'Aceh ont exprimé leur mécontentement à l'égard des lois religieuses de plus en plus sévères, la plupart craignent d'exprimer leurs inquiétudes par crainte d'être qualifiés de non religieux[17].

Cette tendance fondamentaliste s'accompagne d'une violence croissante autour des élections dans la province et d'une MOC de plus en plus active et violente. Alors qu'une période d'apaisement s'est installée après l'accord de paix de 2005, en cas de réapparition la violence vis-à-vis du gouvernement indonésien, une nouvelle tension créera une insurrection encore plus complexe à traiter que celle qui a jamais été présentée par le GAM, à savoir opposant fondamentalisme religieux et laïcité politique, sur fond de vieux griefs économiques et de droits de l'homme bafoués.

En résumé, même si l'on peut identifier la « cause » d'une insurrection, elle doit nécessairement émerger d'un tissu complexe de tensions et de propensions dynamiques. Au fur et à mesure que les tensions sous-jacentes évoluent, la cause peut elle aussi évoluer. Par conséquent, une définition unique et statique de la cause des insurgés n'est pas une base fiable pour la planification des opérations COIN. Bien que cet élément soit déjà largement reconnu dans la doctrine et les théories COIN, leurs implications logiques n'ont pas été entièrement résolues. Une analyse multi causale de l'insurrection nécessite de nouveaux outils conceptuels qui ne sont pas disponibles dans la théorie traditionnelle.

Un cadre conceptuel de l'insurrection multi causale

La présente section élabore un cadre multi causal pour comprendre l'insurrection. Premièrement, il convient d'établir une distinction entre causalité et les causes d'une insurrection. La causalité est l'inférence des relations de nécessité et de suffisance entre une cause et ses effets. La recherche sur les causes de la guerre cherche à découvrir ce type de relation causale. Dans la discussion précédente, la toile complexe des tensions et des propensions dynamiques lie les causes et les effets.

En revanche, selon le *Field Manual* (FM) 3-24, « une cause est un principe ou un mouvement défendu ou soutenu de façon militante[18] ». Galula explique comment une cause est liée à des tensions sous-jacentes :

> Qu'est-ce qu'un problème politique ? C'est une 'contradiction non résolue', affirme Mao Tse-tung. L'acceptation de cette définition revient à dire qu'une cause politique est la défense de l'un des deux pans de la contradiction[19].

Les causes des insurgés ne sont pas des causes matérielles qui produisent des effets de causalité ; ce sont plutôt les causes insurrectionnelles justifiant le recours à la violence. Bien que les deux concepts soient liés, ils sont tout à fait distincts et ne doivent être confondus. Le lien de causalité est généralement pertinent au niveau de

l'action tactique, tandis que les causes insurrectionnelles influencent l'insurrection au niveau stratégique. La causalité et les causes insurrectionnelles sont toutes deux pertinentes à la discussion que nous engageons ci-après.

Jusqu' à récemment, la plupart des explications scientifiques de la causalité se concentraient sur les relations de cause à effet. Ainsi, le *Guide for Understanding and Implementing Defense Experimentation*: *GUIDEx*, un rapport établi en collaboration entre des scientifiques de la défense représentant l'Australie, le Canada, le Royaume-Uni et les États-Unis, affirme que :

> Tout problème de capacité nationale ou de coalition peut être posé comme suit : A est-il la cause de B ? Une capacité ou un concept – un nouveau modèle commercial – est soumis à une expérimentation pour déterminer si la capacité A cause l'effet militaire B. L'hypothèse expérimentale énonce la relation de cause à effet entre la solution proposée et le problème[20].

Cela traduit bien la vision scientifique classique de l'expérimentation. Le GUIDEx poursuit en posant le postulat que l'un des critères importants d'une bonne expérience est la capacité d'isoler la raison du changement dans l'effet B[21]. Dans ce paradigme, l'expérimentation a pour but de répondre à la question de la causalité entre une variable indépendante et une variable dépendante. La méthode d'expérimentation consiste à créer un système fermé permettant d'éliminer les sources alternatives de variation qui pourraient biaiser le résultat expérimental. Dans ce paradigme, les connaissances accumulées à partir d'expériences multiples permettent de raisonner sur les chaînes causales : A provoque B, qui cause C, qui cause D.

Bien que les scientifiques puissent parfois approcher les conditions idéales d'un système fermé sur une durée suffisamment longue que pour isoler une seule variable indépendante, ce degré de contrôle est évidemment impossible dans toute société humaine. Les sociétés dans lesquelles les insurrections se multiplient sont des systèmes ouverts, caractérisés par une perpétuelle nouveauté et un nombre incalculable de variables indépendantes. Ici, la causalité est mise en réseau et ne peut être réduite à des relations de cause à effet uniques, ni même à des chaînes de causalité linéaires.

La science des systèmes complexes offre une perspective alternative qui semble en mesure de donner un sens à la causalité en réseau. Les réseaux distribués d'agents autonomes qui prennent des décisions locales à partir d'informations locales caractérisent des systèmes adaptatifs complexes. De ces choix locaux individuels émergent des schémas globaux qui se répercutent sur les décisions ultérieures des agents autonomes. En raison de ces cycles de rétroaction itératifs, la causalité est complexe, resautée et circulaire. La modification de A peut se répercuter sur B, C et D, ce qui à son tour affecte A. Ainsi, non seulement les causes ont des effets, mais ces effets peuvent aussi en avoir causé... la cause !

Si tout cela semble inutilement compliqué, il vaut la peine de considérer les effets très réels que ces boucles de rétroaction peuvent générer. Un exemple classique est

l'effet Pygmalion d'une panique bancaire. Une rumeur selon laquelle une banque est en difficulté financière, même si elle ne l'est pas, peut inciter les investisseurs prudents à retirer leur argent. Le fait de voir des clients faire la file en nombre pour retirer leurs économies poussera d'autres clients à en faire de même, créant ainsi un effet boule de neige. Avant la fin de la journée, la banque aura épuisé ses réserves de liquidités et sera insolvable. Les perceptions et les rumeurs peuvent avoir des effets similaires et non moins dramatiques pendant les révolutions et les insurrections. Galula cite l'utilisation efficace, par les communistes chinois, du slogan « Land to the Tiller » pour faire circuler l'idée, fausse, que la propriété foncière en Chine était concentrée dans les mains d'une petite minorité[22].

Systèmes complexes et options d'intervention

Les systèmes complexes présentent des mécanismes d'auto-organisation, d'émergence, d'hystérésis, de voies latentes et d'adaptation. La compréhension de chacun de ces concepts fournit d'importantes perspectives pour la théorie COIN et ouvre de nouvelles options d'intervention pour les mouvements contre-insurrectionnels.

Auto-organisation

L'auto-organisation est l'augmentation spontanée de l'ordre dans le temps dans un système ouvert. Il est spontané en ce sens qu'il n'est pas imposé de l'extérieur, mais qu'il s'accumule par des interactions entre les parties du système au fur et à mesure que l'énergie le traverse. Un modèle d'auto-organisation largement étudié démontre une augmentation spontanée de l'organisation lorsque les agents fixent leur couleur selon deux règles. La première règle, l'activation à courte portée, définit la préférence en fonction de la couleur des voisins les plus proches de l'agent. La deuxième règle, l'inhibition à longue portée, définit la préférence en fonction de la couleur opposée à celle des voisins les plus éloignés de l'agent. D'autres paramètres du modèle comprennent le rayon des voisins les plus proches, le rayon des voisins les plus éloignés et la pondération accordée à l'activation à courte distance par rapport à l'inhibition à longue portée. Les résultats de ce modèle sont présentés à la figure 1. En cinq étapes, un mélange aléatoire d'agents noirs et blancs s'est d'abord organisé en un motif à rayures noires et blanches. Avec des conditions initiales différentes, le modèle produira des rayures noires et blanches différentes à l'analyse détaillée, mais le même motif qualitatif restera identique. Avec différents réglages de paramètres, le même jeu de règles peut produire uniformément des agents noirs ou blancs, des taches noires sur fond blanc ou vice versa. Ce modèle très simple a été utilisé pour expliquer la croissance et la différenciation structurelle d'un organisme, la formation de structures

récurrentes dans la fourrure animale et le regroupement d'industries dans l'économie régionale[23].

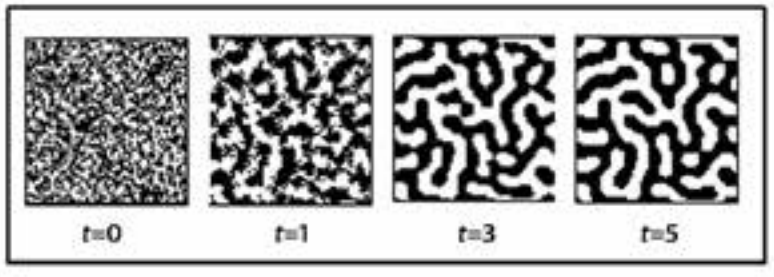

Figure 1 : formation de structures récurrentes comme exemple d'auto-organisation et d'émergence

Dans la littérature consacrée aux théories contre-insurrectionnelles, il est courant de diviser la population en trois catégories : les soutiens actifs du gouvernement, la majorité neutre et silencieuse, et les soutiens actifs à l'insurrection. En regardant la présente discussion à travers le spectre de ce postulat simplifié, la dynamique de l'auto-organisation aide à expliquer pourquoi un village peut être pro-gouvernemental, alors qu'un village voisin aux conditions sociales identiques soutient l'insurrection. Parce que le choix de l'état d'un acteur est conditionné par l'état des autres maillons de son réseau social, une population qui serait obligée de choisir entre les insurgés et les contre-insurgés aura tendance à se regrouper en modèles spatialement organisés au fil du temps.

La première conséquence de l'auto-organisation est que la répartition spatiale des populations pro-gouvernementales et pro-insurrectionnelles est plus importante que la proportion totale de la population de chaque catégorie. Les mesures d'efficacité agrégeant les données statistiques nationales peuvent nous induire en erreur ; une carte à codes de couleur montrant les tendances d'allégeance au fil du temps fournit un outil d'évaluation beaucoup plus riche. Dans les théories COIN, la situation locale peut être très différente de la situation locale voisine et de la situation régionale. Par conséquent, les décideurs aux niveaux inférieurs ont besoin d'une plus grande autonomie pour s'adapter à leur contexte local. Bien entendu, l'importance des flux de renseignements ascendants et du transfert des décisions aux niveaux les plus bas relève déjà d'un principe standard de la doctrine classique[24]. La doctrine contre-insurrectionnelle publiée conjointement par l'Armée de terre et le Corps des Marines des États-Unis décrit les théories COIN comme une « 'guerre mosaïque' mouvante difficile à envisager comme un tout cohérent par les mouvements anti-insurgés[25] ». Ce qui est nouveau ici, c'est que l'auto-organisation fournit une explication théorique de la « guerre mosaïque » observée dans la pratique, une justification pour l'exécution décentralisée des opérations COIN et une prescription pour l'évaluation des progrès.

La deuxième implication de l'auto-organisation est que les approches indirectes conduisent à des transformations plus radicales du modèle observé que l'intervention directe. Les modèles formés font office d'« attracteurs » dans un système dynamique, et ont tendance à résister aux perturbations locales. Pour la majorité des agents de la figure 1, le changement de couleur du noir au blanc n'a pas d'effet permanent sur le système. L'état inchangé de leurs voisins signifie simplement que l'agent reviendra à l'étape suivante. L'action directe ne fonctionnera que si un nombre critique d'agents est simultanément inversé. Même dans ce cas, tant que le calcul sous-jacent des agents demeure inchangé, l'action directe ne fera probablement que redistribuer l'emplacement des bandes noires et blanches, et n'aura aucun effet à long terme sur leur proportion relative. En revanche, un changement relativement faible de la pondération entre les règles d'activation à courte portée et d'inhibition à longue portée peut modifier qualitativement les tendances observées. Le changement traverse le système en utilisant exactement la même dynamique d'auto-organisation qui a perpétué le modèle original. Dans le cas des théories COIN, cela implique qu'en général, il est probable que les mesures indirectes visant à modifier le calcul de la population – en choisissant de soutenir les insurgés ou le gouvernement – seront plus efficaces à la transformation que la coercition.

Émergence

Les modèles produits par les systèmes auto-organisés sont émergents. L'émergence signifie que l'ensemble diffère de la somme de ses constituants[26]. En science, il existe une hiérarchie d'émergence entre physique, chimie, biologie et psychologie. Les lois de la chimie se réduisent aux lois de la physique, mais s'ajoutent à celles de la physique. La biologie se réduit aux lois de la chimie, et les produits chimiques sont les éléments constitutifs des cellules, mais la chimie introduit aussi de nouvelles théories pour expliquer la vie. La psychologie est limitée par la biologie, mais de nouveau, de nouvelles théories agissent au niveau de l'esprit. À chaque niveau, la théorie est limitée par les niveaux inférieurs, mais elle jouit également d'une certaine autonomie par rapport au niveau qui lui est directement inférieur. De nouveaux concepts et de nouvelles règles sont nécessaires pour expliquer les régularités au niveau supérieur. Dans la figure 1, on peut évoquer de façon sensée les rayures et les taches qui composent l'ensemble. Pourtant, au niveau des agents individuels, l'ensemble de règles ne fonctionne qu'à partir d'informations locales sur la couleur des voisins proches et éloignés. Les rayures et les taches sont des propriétés émergentes qui n'ont aucun sens au niveau individuel. Les modèles qui émergent d'un niveau fournissent les éléments de base des systèmes du niveau suivant.

De même, il existe une hiérarchie d'émergence dans la guerre contre-insurrectionnelle. Le niveau opérationnel de la guerre n'est pas simplement la somme des engagements tactiques qui la composent. Le niveau stratégique qui relie l'instru-

ment militaire à la politique est qualitativement différent du niveau opérationnel, qui planifie et exécute la mission sur le théâtre des opérations. Ainsi, différents niveaux de guerre requièrent différents concepts. Dans une étude détaillée des violences commises lors de guerres civiles, et en particulier lors de la guerre civile grecque, Stathis Kalyvas constate par exemple que les populations n'ont pas uniformément recours à la violence à cause de la peur, de l'idéologie ou de la polarisation sociale politique d'avant-guerre, mais qu'elles agissent de manière sélective pour des raisons sous-régionales, voire locales[27]. Kalyvas n'en conclut pas pour autant que toute la violence est locale, car les dirigeants politiques et les insurgés peuvent naturellement amener les gens et les groupes à la violence. Mais il tente néanmoins de faire la distinction entre les motifs des niveaux « macro » et « micro » qui poussent les gens à la violence dans tous les conflits. Comme le soutient Kalyvas,

> la violence aveugle est un raccourci informationnel qui peut se retourner contre ceux qui l'utilisent ; la violence sélective est produite conjointement par des acteurs politiques à la recherche d'informations et des individus cherchant à éviter le pire - mais aussi à saisir les opportunités que la situation leur offre[28].

Kalyvas note que les guerres civiles se distinguent des guerres interétatiques par leur niveau d'intimité. Les guerres interétatiques sont des affaires entre pays étrangers et donc manquent d'intimité, alors que les guerres civiles, et nous pourrions argumenter que les insurrections aussi, sont des guerres contre les compatriotes, les voisins, et même les parents[29]. Les voisins, les parents et les amis se dénonçaient régulièrement après d'autorités légitimes et illégitimes pour de multiples raisons, y compris la jalousie et les griefs personnels. Le passage de la dénonciation à la violence était alors aisément franchi, si l'occasion se présentait[30]. Si certains ont été véritablement guidés par les arguments politiques de leurs dirigeants, beaucoup d'autres nourrissent des motivations mesquines et extrêmement personnelles.

L'étude de Kalyvas et le présent travail révèlent qu'il est malavisé de lancer une campagne opérationnelle centrée sur la cause ou le centre de gravité. Comme Kalyvas le fait remarquer, beaucoup d'érudits et de praticiens définissent la cause de la violence comme impénétrable et brandissent alors « des explications de la violence mettant l'accent sur les émotions collectives, les idéologies et les cultures qui ont, à l'analyse, un faible potentiel explicatif[31] ». Par conséquent, le meilleur plan de campagne pourrait être d'accorder aux commandants de brigade et de bataillon une plus grande latitude pour gérer les motifs locaux de violence lors d'une opération de contre-insurrection, les motifs pouvant être macro, micro voire un mélange des deux.

Hystérésis

Le troisième concept de la science des systèmes complexes, l'hystérésis, est un comportement non linéaire rencontré dans une grande variété de processus, allant de

la ferroélectricité à la biologie, où les relations dynamiques intrants-sorties entre les variables impliquent des effets de mémoire[32]. L'hystérésis implique une dépendance au chemin emprunté. Lorsqu'un système revient à un état précédent, il peut se comporter différemment. De plus, des chemins différents vers le même état peuvent se traduire par un comportement différent. Par conséquent, dans les systèmes avec hystérésis, il n'est pas suffisant de connaître uniquement l'état actuel ; l'histoire du système est essentielle pour donner un sens aux futurs modèles de comportement possibles.

La dépendance au chemin emprunté et l'importance de l'histoire ne sont guère nouvelles pour les contre-insurgés. L'hystérésis s'avère importante dans l'identification des causes de l'insurrection. Lorsqu'un gouvernement perd sa légitimité, la résolution des griefs déclarés ne permet pas automatiquement de regagner le soutien populaire. Par exemple, en Égypte, la concession du président Moubarak en réponse à des protestations de masse est susceptible d'avoir encouragé les manifestants à formuler de nouvelles demandes et a ainsi suscité un soutien plus large. Une approche plus sophistiquée est nécessaire pour contrer les causes de l'insurrection.

Plutôt que de réagir directement aux causes, les contre-insurgés doivent comprendre la façon dont les causes se rattachent aux récits dominants dans une société donnée. Les récits ne se résument pas à une chronologie désintéressée des événements. Le choix de la perspective à partir de laquelle l'histoire est racontée, des acteurs auxquels on donne la parole et ceux qu'on ignore, des événements sur lesquels on insiste et ceux qui sont omis, ainsi que la délimitation du récit dans le temps et l'espace, ont tous une incidence sur la morale implicite de l'histoire. L'enchaînement des événements, des sentiments et des actions peut être utilisé pour suggérer des relations entre les effets et leurs causes. Les causes de l'insurrection pouvant être liées aux récits existants sont davantage susceptibles de trouver un écho au sein d'une société, et élargir par corollaire la base du soutien de façon considérable.

Une fois que les causes des insurgés sont associées à un récit, le fait de s'opposer directement au récit peut le renforcer par inadvertance. George Lakoff utilise un exemple simple pour illustrer ce point. L'effet de l'instruction « Ne pense pas à un éléphant » produira invariablement l'effet contraire de son intention apparente. Elinor Ochs et Lisa Capps font remarquer que

> les contre-récits n'impliquent pas nécessairement une référence manifeste à une vision narrative dominante du monde. C'est l'expression de la réalité disjonctive qui constitue elle-même le contrepoint. Un compte-rendu alternatif peut ainsi s'avérer plus efficace pour démanteler la perspective du statu quo que des critiques manifestes. En s'y référant, les critiques perpétuent la prépondérance des discours dominants qu'elles visent justement à déraciner[33].

Pour lutter efficacement contre les causes de l'insurrection, il faut promouvoir de nouvelles identités et un récit qui parle d'une « réalité disjonctive », comme en témoigne le changement d'usage du terme « États-Unis » utilisé avant la guerre de

Sécession au pluriel et devenant ensuite un nom singulier après la guerre, symbolisant la transformation de « l'Union » en « nation ».

Les discours de guerre de Lincoln ont marqué cette transition. Dans son premier discours d'investiture, il a utilisé vingt fois le mot « Union » et pas une seule fois le mot « nation »... Dans sa lettre à Horace Greeley sur le rapport de l'esclavage à la guerre, le 22 août 1862, Lincoln utilisait huit fois le terme union et jamais celui de nation. Un peu plus d'un an plus tard, dans son discours de Gettysburg, le président n'a fait aucune allusion à l'« Union », mais a utilisé le mot « nation » cinq fois en référence à la renaissance de la liberté et du nationalisme aux États-Unis[34]. Et dans son deuxième discours inaugural, qui revient sur les événements des quatre dernières années, Lincoln a parlé d'un camp cherchant à dissoudre l'Union en 1861 et d'un autre acceptant le défi de la guerre pour préserver la nation[35].

Lincoln a utilisé le langage pour forger de nouvelles identités et façonner des récits à mesure que l'Amérique émergeait de la guerre civile. Un récit mettant l'accent sur le nationalisme a recadré le discours politique loin de la terminologie de l'Union et des Confédérés, qui était une source de division.

Voies latentes

Les systèmes complexes sont hautement interconnectés. C'est ainsi que naît le quatrième concept issu de la science des systèmes complexes : l'énergie, la matière et l'information circulent sur de multiples canaux. L'observation du comportement actuel ne fournit que des informations sur les voies actives ; les voies latentes peuvent rester invisibles. Par conséquent, les systèmes complexes présentent généralement une dégradation. Lorsqu'une voie est bloquée, les passages latents sont activés pour préserver la fonctionnalité du système. L'effet dit de ballon est un bon exemple de voies multiples d'un système complexe. Pour contrer les opérations de contrebande de drogues du cartel de Medellin entre la Colombie et les États-Unis, le *South Florida Drug Task Force* a mené une opération qui a permis de réduire considérablement le volume de drogues entrant en Floride via les Caraïbes. Cela n'a toutefois pas empêché le trafic de drogues vers les États-Unis. En réponse, les cartels colombiens ont établi des relations avec les cartels mexicains de la marijuana pour faire passer en contrebande des stupéfiants sur les quelque 3 200 kilomètres de frontière avec les États-Unis. Les violences qui caractérisent actuellement la guerre mexicaine contre la drogue sont une conséquence indirecte de la fermeture réussie d'une voie dans un système complexe.

Le concept de voies multiples est lié aux causes de l'insurrection. Il faut s'attendre à ce que le fait de s'attaquer efficacement à une cause active de nouvelles voies pour mobiliser les insurgés. Cela renforce les dangers de se focaliser sur une seule cause insurrectionnelle. Même si les voies latentes d'un système complexe ne sont pas évidentes d'après l'observation du modèle de comportement actuel, il est possible d'anticiper les voies alternatives avant qu'elles ne soient activées. C'est là qu'il est essentiel

de comprendre les tensions et la propension sous-jacentes au sein de la société, car ces éléments éclairent les contradictions que les insurgés peuvent chercher à exploiter. L'identification de groupes externes potentiels, tels que la population chiite de Bahreïn, permet également au contre-insurgés d'anticiper le type de griefs que les insurgés peuvent utiliser pour mobiliser ces groupes externes, puis de prendre des mesures pour atténuer ces voies latentes avant qu'elles ne soient activées.

Adaptation

L'adaptation est le concept final de systèmes complexes que nous évoquons dans le présent ouvrage. Les théoriciens des approches COIN mettent souvent le doigt sur la capacité d'adaptation des insurgés. Le FM 3-24 affirme que les insurgés compétents sont dotés d'une bonne capacité d'adaptation[36]. Mais paradoxalement, c'est la faiblesse relative des forces insurgées qui leur donne un avantage en matière d'adaptabilité. Les experts des systèmes complexes se sont inspirés de la théorie de l'évolution de Charles Darwin pour étudier les raisons expliquant pourquoi les insurgés s'adaptent plus rapidement et plus efficacement[37]. L'adaptation exige la présence de variations, de sélections et de réplications. Dans un conflit asymétrique, le camp faible se caractérise généralement par une plus grande diversité, et est soumis à une pression de sélection plus forte que la pression qu'ils exercent sur le camp fort. Il est aussi exposé au combat plus longtemps, ce qui décuple l'expérience de combat[38]. Cette théorie est étayée quantitativement par des données provenant à la fois de l'Irak et de l'Afghanistan, qui montrent que l'intervalle de temps moyen entre les attaques mortelles par engins explosifs improvisés augmente logarithmiquement pendant la durée de la guerre[39]. Pour paraphraser encore la paraphrase de Megginson sur Darwin, ce ne sont pas les insurrections les plus fortes qui survivent, ni les plus intelligentes, mais celle qui ont la meilleure capacité d'adaptation au changement.

Compte tenu de l'importance centrale de l'adaptation dans la stratégie COIN, les contre-insurgés doivent à la fois améliorer leur propre capacité d'adaptation et contrer l'adaptabilité des insurgés. Cela exige une plus grande variation de nos propres forces, une pression de sélection plus forte et une réplication plus rapide des innovations réussies. La contre-adaptation nécessite d'affaiblir ou de fausser la pression évolutive exercée sur les insurgés. Le lieutenant-colonel Michael Ryan, de l'armée australienne, a délibérément utilisé la contre-adaptation contre les talibans lorsqu'il était commandant de la 1re Force opérationnelle de reconstruction dans la province d'Oruzgan, en Afghanistan.

Les récents progrès de la théorie évolutionniste nous apportent de nouvelles idées sur la façon d'exploiter au mieux le pouvoir de l'adaptation. L'évolution de l'évolutivité, l'adaptation de second ordre, applique l'évolution au processus d'évolution lui-même. Par exemple, la façon dont la variation est générée est loin d'être aléatoire, car elle s'est adaptée pour produire une variation génotypique dans les zones corrélées

avec le plus grand flux environnemental, tandis que les codes correcteurs d'erreurs protègent les régions associées à la fonctionnalité critique d'une trop grande variation. L'adaptation de second ordre permet aux contre-insurgés d'accélérer leur rythme d'adaptation. À titre d'exemple simple, l'utilisation des analyses après action (AAA) aide les unités à apprendre et à s'adapter. L'adaptation de la façon dont les AAA sont menées pour améliorer leur efficacité est une adaptation de second ordre.

Les biologistes évolutionnistes admettent aujourd'hui que la pression sélective s'applique non seulement au niveau du gène, mais aussi aux organismes et même aux groupes d'organismes. Bien que les pressions de sélection soient les plus rapides au plus bas niveau de sélection et les plus fortes en magnitude, les effets subtils de la sélection du groupe peuvent dominer sur des échelles de temps plus longues. Une vue à plusieurs niveaux induit un avantage clé potentiel pour les contre-insurgés. Même si les insurgés ont un avantage sur le plan de l'adaptation tactique en raison de leur structure très variable et décentralisée, les contre-insurgés peuvent néanmoins s'adapter davantage aux niveaux opérationnel et stratégique en raison de leur meilleure intégration. Les adaptations plus lentes, mais plus stratégiques, de la contre-insurrection peuvent pousser les insurgés dans une situation où une adaptation tactique plus rapide devient en grande partie inutile. Cela exige toutefois que les contre-insurgés améliorent leurs mécanismes d'adaptation de niveau supérieur.

Conclusions : Implications des approches COIN

Compte tenu des arguments avancés jusqu'ici, il est important de développer l'intelligence historique et culturelle du dirigeant et des membres du groupe. Quels facteurs ont poussé ces individus à passer d'un grief politique pacifique à une rébellion violente ? Il ne s'agit là que d'un exemple de question à laquelle il convient de répondre avant de pouvoir comprendre pleinement la cause d'une insurrection et de pouvoir y répondre. Ce degré d'intelligence culturelle et historique implique l'acquisition de connaissances approfondies sur le ou les groupes identitaires des insurgés ; mais c'est là une évolution positive, car elle limite la portée de l'étude. Ainsi, en termes d'opérations et de tactiques, il est primordial de savoir que les citoyens irakiens ont un profond dégoût pour les chiens. Si l'on fait bien sûr abstraction du fait que l'emploi de tactiques culturellement insensibles ne fait qu'alimenter la cause des insurgés, ces informations sont cependant peu utiles pour élaborer un plan de lutte contre la cause de l'insurrection.

Ce qu'il faut discerner, ce sont les antécédents historiques, politiques et culturels de l'insurrection. Nous devons comprendre les propensions historiques à prendre en compte lorsqu'on élabore une campagne de lutte contre l'insurrection. Mais il faut aussi connaître les tensions individuelles présentes dans la société, telles que la discrimination à l'encontre de certaines minorités, l'exploitation économique historique

d'une région, la discrimination religieuse, etc. qui sont utilisées actuellement par les insurgés pour développer leur cause et élargir leur potentiel de ralliement. Une nécessité analogue s'impose pour les tensions qui pourraient être exploitées à l'avenir pour étendre la rébellion ou qui pourraient évoluer si la contre-insurrection réussit à combattre une ou plusieurs des tensions initiales qui ont alimenté la rébellion.

Le mouvement contre-insurrectionnel tiendrait compte de tous ces éléments en élaborant une liste « galulesque » plus élaborée de revendications des insurgés, mais aussi des tensions et des propensions sous-jacentes qui alimentent ces revendications.

Galula suggère de répondre immédiatement aux revendications auxquelles le gouvernement national légitime peut répondre et d'ignorer le reste[40]. Les auteurs du présent article ne suggèrent cependant pas cette ligne de conduite. Avant de répondre à une seule revendication ou de s'attaquer à une seule tension sous-jacente dans la société, il faut essayer de réfléchir à la façon dont l'apport d'énergie dans le système affectera ce dernier dans son ensemble. Par exemple, la lutte contre la pauvreté sous-jacente dans une société favorise-t-elle l'émergence d'une tension d'ordre religieux qui alimente l'insurrection ? Existe-t-il d'autres tensions que les insurgés n'utilisent pas et qui pourraient être cooptées une fois que la pauvreté aura été combattue ? Lorsque l'on ne considère la cause que sous l'angle de la complexité, il est évident que s'engager dans la contre-insurrection est une entreprise extrêmement désordonnée.

De plus, à partir de cette analyse, il doit être clair que les opérations de COIN doivent s'accompagner d'une grande fluidité et faire l'objet d'un processus de révision constante au fur et à mesure que l'on constate des changements dans le cadre environnemental. Une telle approche devrait également aider à catégoriser le type d'insurrection présenté. Bard O'Neill tente vaillamment de désagréger les types d'insurrection en notant que chaque type exige des approches COIN différentes[41]. Cela implique que certaines stratégies peuvent fonctionner avec certaines insurrections alors qu'elles en alimentent involontairement d'autres, ce qui rend l'identification des tensions et de la cause encore plus importante.

La situation actuelle au Pakistan peut nous servir d'exemple pour étayer notre propos. Le gouvernement pakistanais a toujours eu beaucoup de difficulté à pénétrer dans la région du Baloutchistan et dans la province frontalière du Nord-Ouest (PFNO) et à les contrôler. Ce problème est devenu particulièrement aigu à l'ère post-Musharraf et les talibans pakistanais ont connu le succès en exploitant ce manque de contrôle historique, conjugué au chaos créé par la chute de Musharraf. Le gouvernement a d'abord tenté d'accorder des conciliations aux talibans pakistanais en leur offrant une plus grande autonomie locale et des normes religieuses plus strictes en matière d'éducation et d'application de la loi. Mais cette approche s'est vite retournée contre lui : les talibans, au lieu d'entrer dans une période d'inactivité, ont au contraire été encouragés à intensifier l'insurrection et à remettre en question avec plus de force encore le pouvoir du gouvernement national. Une campagne malsaine et violente de

lutte contre l'insurrection s'en est suivie et l'issue de cette campagne est encore incertaine.

Notant tout ce qui précède, les conciliations données aux insurgés ont été utilisées à bon escient comme stratégie contre-insurrectionnelle dans les insurrections passées, mais selon l'étude *How Insurgencies End*, menée en 2010 par la RAND Corporation, cette issue est rare et se produit dans moins d'un tiers des insurrections modernes. Parmi les exemples notables du XX[e] siècle, citons El Salvador, le Guatemala, l'Afrique du Sud et l'Irlande du Nord[42]. La clé est de comprendre le système, les propensions et les tensions qui alimentent et encadrent la cause avant de s'attaquer à cette dernière.

En dernière analyse, si l'on se fie à la thèse de Kalyvas, selon laquelle toute violence est initiée au niveau local, et que l'on reconnaît simultanément la complexité des interactions sociales, il faut aussi admettre que les causes seront très personnalisées. Un individu pourrait se joindre à l'insurrection par haine pour le gouvernement central. Un autre pourrait s'y joindre pour des raisons sociales. D'autres encore pourraient être attirés pour des raisons religieuses ou même par la perspective criminelle. Non seulement différentes personnes et différents groupes se joindront à l'initiative pour des raisons différentes, mais la cause principale changera probablement avec le temps.

Le présent article a pour but d'amorcer une réflexion sur cette question et de faire évoluer la mentalité des experts en recherche contre-insurrectionnelle. Sans une approche plus sophistiquée nous permettant de comprendre les causes des insurrections, il nous sera impossible de les contrer.

Notes

1. GALULA, David, « Counterinsurgency Warfare: Theory and Practice », New York : Praeger, 1964 ; RECORD, Jeffrey, « Beating Goliath: Why Insurgencies Win », Dulles, Virginie : Potomac Books, 2007 ; KITSON, Frank, « *Low Intensity Operations: Subversion, Insurgency, and Peacekeeping* », Saint Petersburg, Floride : Hailer, 1973 ; O'NEILL, Bard, « Insurgency and Terrorism: From Revolution to Apocalypse », 2[e] éd., Washington, D.C. : Potomac Books, 2005 ; JAMES, Anthony, « Resisting Rebellion: The History and Politics of Counterinsurgency », Lexington : University of Kentucky Press, 2004.

2. TRINQUIER, Roger, « *Modern Warfare: A French View of Counterinsurgency* », Fort Leavenworth : Combat Studies Institute, 1964, pp. 20, 22.

3. *Id.*, p, 6.

4. GALULA, « Counterinsurgency Warfare », p. 22.

5. *Id.*, p.103.

6. WILSON, Thomas G., Jr., « Extending the Autonomous Region in Muslim Mindanao to the Moro Islamic Liberation Front: A Catalyst for Peace », *U.S. Army School of Advanced Military Studies MMAS Monograph series*, 2009, pp. 13-14.

7. BIRTLE, Andrew J., « U. S. Army Counterinsurgency and Contingency Operations Doctrine 1860-1941 », Washington D.C. : U. S. Army Center of Military History, 2004, p. 108.

8. *Id*, 119.

9. Également connu sous le nom de *Tydings-Mcduffie Act*.

10. SUNDHAUSSEN, Ulf , « Indonesia: Past and Present Encounters with Democracy », in *Democracy in Developing Nations, Volume Three: Asia*, DIAMOND, Larry, LINZ, Juan, et LIPSET, Seymour Martin, éd., Londres, Angleterre : Adamantine Press Limited, 1989, p. 440.

11. LIDDLE, William R., « The Islamic Turn in Indonesia », *The Journal of Asian Studies* 55, n° 3, 1996, p. 614.

12. VATIKIOTIS, Michael, « Southeast Asia in 2005: Strength in the Face of Adversity », in *Southeast Asian Affairs,* Dajit Singh et Lorraine Carlos Salazar, éd., Singapore : Institute of Southeast Asian Studies, 2006, p. 6.

13. VATIKIOTIS, Michael, *Indonesian Politics Under Suharto: The Rise and Fall of the New Order*, 3e éd., New York : Routledge, 1993, p. 119.

14. « Aceh's Sharia Court », *BBC News Online*, 4 mars 2003, http://news.bbc.co.uk/go/em/fr/-/2/hi/asia-pacific/2816785.stm.

15. « Aceh Passes Adultery Stoning Law », *BBC News Online*, 14 septembre 2009, http://news.bbc.co.uk/go/em/fr/-/2/hi/asia-pacific/8254631.stm.

16. « Islamic Police Tighten Grip on Indonesia's Aceh », *The Malaysian Insider*, 14 janvier 2010, http://themalaysianinsider.com/index.php/world/49530-islamicpolice-tighten-grip-on-indonesias-aceh.

17. HAMANN, Katie, « Aceh's Sharia Law Still Controversial in Indonesia », *VOA News*, 29 décembre 2009, www.voanews.com/english/news/religion/Acehs-Sharia-Law-Still-Controversial-in-Indonesia-80257482.html.

18. U.S. Department of the Army, « Field Manual 3-24*:Counterinsurgency* », Washington, D.C. : HQDA, 15 décembre 2006, pp. 1-10.

19. GALULA, *Counterinsurgency Warfare*, p. 10.

20. The Technical Cooperation Program, Guide for Understanding and Implementing Defense Experimentation, Ottawa, Canada, Canadian Forces Experimentation Centre, février 2006, www.acq.osd.mil/ttcp/reference/docs/GUIDExBookFeb2006.pdf.

21. *Id*, p. 13.

22. GALULA, *Counterinsurgency Warfare*, p. 17.

23. TURING, Alan M., « The Chemical Basis of Morphogenesis », *Philosophical Transactions of the Royal Society of London, Series B, Biological Sciences* 237, n° 641, 1952, pp. 37-72 ; NAGORCKA, BN, et MOONEY, JR, « From stripes to spots: prepatterns which can be produced in the skin by a reaction-diffusion system », *IMA Journal of Mathematics Applied in Medicine and Biology* 9, n° 4, 1992, pp. 249-67 ; KRUGMAN, Paul, « A Dynamic Spatial Model », document de travail n° 4219, National Bureau Of Economic Research, Cambridge, MA, novembre 1992.

24. Department of the Army, *Field Manual 3-24*, *1-26* et *3-31*.

25. *Id*., pp. 1-8.

26. ANDERSON, P.W., « More is Different », *Science* 177, n° 4047, 4 août 1972, pp. 393-396.

27. KALYVAS, Stathis N., *The Logic of Violence in Civil War*, Cambridge : Cambridge University Press, 2006, p. 328.

28. *Id*., p. 388.

29. *Id*., pp. 330-33.

30. *Id*., pp. 333-34.

31. *Id*., p. 388.

32. IKHIOUANE, Fayçal, et RODELLAR, José, Systems With Hysteresis: Analysis, Identification and Co*ntrol Using the Bouc-Wen Model*, Chichester, West Sussex : Wiley-Interscience, 2007, p. xi.

33. OPCHS, Elinor, et CAPPS, Lisa, « Narrating the Self », *Annual Review of Anthropology* 25, 1996, p. 37.

34. LINCOLN, Abraham, lettre à Horace Greeley, 22 août 1862, www.abrahamlincolnonline .org/lincoln/speeches/greeley.htm.

35. LINCOLN, Abraham, deuxième discours d'investiture, 4 mars 1865, www.abrahamlincolnonline.org/lincoln/speeches/inaug2.htm.

36. Department of the Army, *Field Manual 3-24*, pp. 1-28.

37. JOHNSON, Dominic, « Darwinian Selection in Asymmetric Warfare: The Natural Advantage of Insurgents and Terrorists », *Journal of the Washington Academy of Sciences* 95, 2009, pp. 89-112.

38. *Id*., p. 89.

39. JOHNSON, Neil, et al, « Dynamic Red Queen explains patterns in fatal insurgent attacks », *arXiv*, janvier 2011, 1101.0987.

40. GALULA, *Counterinsurgency Warfare*, p. 103.

41. BARD, *Insurgency and Terrorism*, chapitre 3.

42. CONNABLE, Ben et LIBICKI, Martin C., *How Insurgencies End*, Santa Monica, CA : RAND, 2010, pp. 18-19.

L'irrationnelle rationalité du terrorisme

Robert Nalbandov, PhD*

La récente intensification de la recherche sur le terrorisme place les universitaires et les professionnels de la lutte antiterroriste devant un dilemme : l'absence d'une définition unique et largement acceptée du terrorisme[1]. Cette diversité ontologique découle de la volonté de faire entrer le terrorisme dans les cadres cognitifs de la rationalité. Selon une étude de l'organisation RAND : « le principal argument en faveur du modèle de choix rationnel réside dans le fait que, si les terroristes et les organisations terroristes se comportent de manière rationnelle, la connaissance de leurs croyances et préférences devrait nous permettre de les comprendre et de prévoir leur comportement[2] ». Plus le comportement des terroristes sera rationnel, ou prévisible, plus il sera facile d'identifier leurs véritables modèles et de lutter contre le terrorisme.

Différentes tentatives de catégorisation du terrorisme dans des cadres rationnels ont été entreprises : Bryan Caplan s'est penché sur des rationalités axées sur les acteurs ; Martha Crenshaw a exploré la rationalité des causes du terrorisme ; Andrew Kydd, Barbara Walter et Robert Pape ont introduit la rationalité dans les actions stratégiques des terroristes ; Anthony Oberschall s'est concentré sur la théorie de l'action collective, et Martin Libicki a étudié la réflexion rationnelle motivant l'action des terroristes[3]. Ces multiples approches dans l'étude du terrorisme révèlent l'absence remarquable d'une théorie cohérente et parcimonieuse de la rationalité, capable de réunir ses différentes formes dans un cadre théorique unique.

Le présent article s'attache à combler cette lacune en tentant d'appliquer le choix rationnel aux concepts de terrorisme « ancien » (avant la fin de la Guerre froide) et « nouveau » (après la Guerre froide). Cette distinction d'ordre chronologique est cependant bien plus fondamentale.

---

*Dr. Robert Nalbandov est professeur adjoint à la faculté de science politique de l'Utah State University. Titulaire d'un doctorat en science politique obtenu en 2008 à l'Université d'Europe centrale de Budapest, il est auteur de nombreux ouvrages et articles consacrés à la sécurité internationale et à la résolution des conflits.

Robert Nalbandov, « Irrational Rationality of Terrorism. » *Journal of Strategic Security* 6, no 4, 2013 : pp. 92-102, DOI : http://dx.doi.org/10.5038/1944-0472.6.4.5. Consultable à l'adresse : http://scholarcommons.usf.edu/jss/vol6/iss4/5

Le phénomène des « nouveaux » terroristes ne se limite pas aux attentats-suicides, qui existaient déjà bien avant la fin de la Guerre froide (chez les kamikazes japonais de la Seconde Guerre mondiale, les résistants juifs après la création de l'État d'Israël, les Tamouls qui ont modernisé les attentats-suicides au XX^{e} siècle, et bien d'autres encore). Les « nouveaux » terroristes radicalisés les plus récents, les frères Tsarnaïev, auteurs de l'attentat de Boston, n'avaient aucunement l'intention de mourir avec les victimes de leurs actes terroristes. La différence entre le terrorisme « ancien » et « nouveau » se reflète dans les catégories à plusieurs niveaux : leurs buts et objectifs, leurs cibles et les victimes qu'ils cherchent à détruire, les causes de leur radicalisation, leur zone d'action et les groupes qui les soutiennent.

Le présent article analyse tout d'abord les fondements de la théorie du choix rationnel, puis l'applique à deux niveaux, l'individu (acteur) et le groupe (collectif), dans deux perspectives : tactique (à court terme) et stratégique (à long terme). L'argument principal est le suivant : si la théorie du choix rationnel peut expliquer « l'ancien » terrorisme, sa « nouvelle » forme s'éloigne sensiblement de la rationalité. Il parvient à la conclusion qu'il est impossible de trouver une solution unique au terrorisme et propose quelques pistes nouvelles pour la lutte antiterroriste.

Le casse-tête rationnel du terrorisme

Théorie du comportement humain, le choix rationnel se focalise sur les individus et les groupes comme acteurs au sens « étroit » et au sens « large ». Selon Eric van Um, « la version étroite autorise uniquement une action qui maximise l'utilité personnelle de sorte que les individus agissent de façon purement égoïste, tandis que la version plus large autorise également la poursuite d'objectifs altruistes[4] ». Au niveau individuel, le choix rationnel « [...] suppose que l'individu est le mieux à même de juger ce qui lui convient le mieux [...]. L'individu a la liberté, mais aussi la responsabilité, de construire sa propre vie[5] ». Au niveau du groupe, le choix rationnel met l'accent sur « [...] la loyauté envers le groupe, avec la propension qui en découle à évaluer les actions à la lumière de leurs conséquences pour le groupe, sans prendre en compte leurs conséquences sur les personnes n'appartenant pas au groupe [...][6] ». Le choix rationnel postule à ces deux niveaux que tous les acteurs cherchent à maximiser l'utilité et poursuivent de manière cohérente des objectifs basés sur des préférences stables délibérément choisies[7]. Les acteurs sont guidés par la logique des conséquences attendues : ils sont en possession d'informations crédibles sur les options dont ils disposent et choisissent les meilleures en fonction de leur calcul de l'utilité espérée[8].

La difficulté liée à l'application de la théorie du choix rationnel au phénomène du terrorisme est de trois ordres. Tout d'abord, elle s'appuie sur une approche holistique unique pour déterminer l'existence ou non de la rationalité, qui ne tient pas compte des variables autres que les schémas cognitifs qui existent objectivement. La rationalité est appliquée en termes absolus et les acteurs sont considérés comme des

personnages statiques qui finissent toujours par choisir les actions promettant la plus grande valeur utilitaire[9]. En réalité, le comportement rationnel d'un acteur avec des systèmes de valeurs définis peut paraître, dans les mêmes circonstances, irrationnel aux yeux d'autres acteurs, en raison de l'incompatibilité de leurs systèmes de valeurs. Il est universellement reconnu que « les acteurs savent ce qu'ils veulent et peuvent commander leurs désirs de manière transitive[10] ». La difficulté de cette approche réside dans le fait qu'un résultat rationnel avec une valeur utilitaire accrue peut survenir seul ou résulter des interceptions multiples de choix pas toujours rationnels. Les acteurs rationnels peuvent choisir des options irrationnelles susceptibles de maximiser l'utilité espérée et inversement.

Le suicide altruiste est la parfaite illustration de ce dilemme théorique. L'aboutissement des actions est rationnel s'il est en adéquation avec les cadres cognitifs spécifiques : mourir pour le bien commun peut apparaître comme une cause noble. Par ailleurs, comme le signale Ludwig von Mises, « personne n'est en mesure de dire ce qui rendrait une autre personne plus heureuse ou moins mécontente », autrement dit, la rationalité est de nature fondamentalement subjective[11]. Au niveau individuel, le soldat qui combat l'ennemie au quotidien sur le champ de bataille pour survivre, et soudain décide de commettre un acte héroïque mais suicidaire pour sauver ses compagnons d'armes, est un autre exemple de suicide pour le bien commun. Ici, le terrorisme rationnel prédirait une forte recrudescence de soldats désireux de se suicider parce que leurs préférences établies les incitent à sauver la vie des autres en sacrifiant la leur. Ce n'est cependant pas le cas et les raisons qui motivent le suicide prémédité demeurent au sein des cadres cognitifs de l'individu et de ses uniques préférences personnelles.

L'autre difficulté de l'approche rationnelle holistique du terrorisme est liée aux niveaux multiples des schémas comportementaux cognitifs. Dans un monde idéal, les acteurs seraient capables de prévoir clairement et de calculer facilement l'utilité espérée résultant de chaque option. Cependant, comme l'indiquent Monroe et Maher, « [...] les personnes réelles ne fonctionnent pas toujours de cette manière, et ne sont pas censées le faire. Nous savons que chacun de nous dispose d'une capacité limitée à percevoir, se souvenir, interpréter et calculer [...][12] ». La rationalité est restreinte par les imperfections humaines, par l'inhérente incapacité des hommes à « effectuer les calculs nécessaires, même pour un nombre réduit d'options, en situation de prise de décision » et, au final, par les déficiences absolues et objectives imposées par les « limitations cognitives de leurs esprits[13] ».

L'identité, qui varie en fonction des acteurs, est une explication possible de leur comportement irrationnel. Des constructions identitaires spécifiques les poussent à choisir différentes options, non pas fondées sur des calculs d'utilité objectifs, mais sur leur évaluation subjective de la réalité objective. La « logique du comportement approprié » fondée sur l'identité limite le pouvoir du raisonnement rationnel des acteurs

et les pousse à « dériver leurs actions d'identités données » et à agir « conformément aux pratiques institutionnalisées d'une collectivité, sur la base de conceptions mutuelles, souvent tacites, de ce qui est vrai, raisonnable, naturel, juste et bon[14] ». Malheureusement, nous ne disposons d'aucune donnée sur la multiplicité des niveaux des schémas comportementaux cognitifs qui pourrait expliquer l'héroïsme du soldat de l'exemple précédent. La décision d'agir de manière héroïque peut découler de son désir d'apporter la victoire à son groupe à partir de son identité spécifique, ou de suivre la doctrine chrétienne du sacrifice personnel pour le bien commun. En revanche, un soldat avec une identité différente, qui croirait par exemple profondément en une autre doctrine chrétienne considérant le suicide comme un péché, en fonction de sa lecture individuelle des Écritures, pourrait vouloir s'abstenir de commettre un tel acte.

Enfin, la « faible » rationalité échoue quand les acteurs sont confrontés à des contraintes d'ordre temporel. La rationalité est susceptible d'être présente, ou pas, dans la prise de décision immédiate : ce qui apparaît comme rationnel à un instant donné peut se révéler irrationnel par la suite, et inversement, si les acteurs prennent le temps de reconsidérer leurs actions d'un point de vue rationnel. Toute action rationnelle immédiate perd sa rationalité sous l'influence des variables supplémentaires extrinsèques aux cadres du choix rationnel. Certains facteurs externes peuvent accroître l'utilité d'une option qui avait auparavant une faible utilité espérée, supposée ne pas évoluer. De la même manière, un acte qui semblait irrationnel dans l'immédiat peut acquérir une base rationnelle à condition de disposer du temps nécessaire à son réexamen. Le soldat de l'exemple précédent pourrait changer d'avis et s'abstenir de commettre un acte héroïque suicidaire s'il a suffisamment de temps pour peser avec soin (c'est-à-dire rationnellement) les avantages et inconvénients d'une action impulsive immédiate. De même, si sa réaction spontanée consiste à éviter de sacrifier sa vie, il peut ultérieurement et dans des conditions similaires choisir de mourir héroïquement pour sauver les autres. Dans tous les exemples mentionnés ci-dessus, les préférences ne sont pas déterminées : elles sont multiples et versatiles, en fonction des cas individuels.

La rationalité au niveau individuel

Quand on applique la théorie du choix rationnel aux actes de terroristes individuels, il convient de faire la distinction entre les formes de terreur suicidaire et non suicidaire. Le terrorisme non suicidaire, ou « survivaliste », caractérise essentiellement « l'ancien » terrorisme, représenté avant la fin de la Guerre froide par l'organisation basque ETA (Eucadi ta Askatasuna), l'Armée républicaine irlandaise véritable (IRA-Véritable), l'Armée secrète arménienne de libération de l'Arménie (ASALA), le Parti des travailleurs du Kurdistan (PKK), le Front Farabundo Marti de Libération nationale (FMLN), le mouvement des Tigres de libération de l'Îlam Tamoul (LTTE),

ainsi que le mouvement Narodnaya Volya et le Parti socialiste révolutionnaire en Russie (Esers). La plupart des « anciens » terroristes étaient des acteurs rationnels souhaitant survivre à leur combat afin de constater les résultats de leurs actions et d'en partager les bénéfices avec l'ensemble du groupe qu'ils représentaient. La notion de sacrifice pour le bien commun était absente de la rationalité égoïste des « anciens » terroristes. Outre leurs motifs survivalistes, ils cherchaient à obtenir des avantages concrets : au minimum une plus grande autonomie pour leurs proches ou au maximum la souveraineté et l'indépendance. Ces objectifs avaient une portée et une couverture géographique limitées et concernaient généralement les terroristes eux-mêmes.

De leur côté, les « nouveaux » terroristes, apparus au début des années 1990 suite à l'effondrement du système bipolaire, poursuivent des objectifs d'une portée transnationale avec des effets limités à long terme. Au niveau individuel, le terroriste qui sacrifie sa vie « espère obtenir le bonheur éternel au paradis[15] ». À première vue, il peut être considéré comme « un agent qui accepte une mort certaine dans le but de tuer avec une probabilité élevée[16] ». Tout comme les terroristes traditionnels, il effectuerait un calcul de coût relatif, qui selon Sandler « [...] doit démontrer que l'utilité associée à la mission suicidaire est au moins aussi grande que l'utilité du *statu quo*[17] ». Cette conclusion est possible, comme l'indique très justement Caplan, « [...] si vous croyez sincèrement que mourir pour le djihad vous apportera une récompense éternelle », ce qui peut laisser penser que le « nouveau » terrorisme est rationnel[18].

L'approche rationnelle de la prise de décision présuppose une utilité supérieure après l'action, ou tout au moins non inférieure à l'utilité avant l'action. Il est essentiel que ces deux utilités soient faciles à calculer en termes concrets. L'idée de troquer des vies humaines pour un plus grand bien commun est assez difficile à accepter, car sacrifier sa vie pour un résultat inconnu et, par conséquent non quantifiable, est loin d'être rationnel. Même si la personne croit que l'utilité après l'action d'un attentat-suicide sera supérieure, elle ne peut en calculer la véritable valeur. Au niveau tactique, les terroristes qui commettent des attentats-suicides ne sont plus présents pour constater les résultats de leurs actions. Ils meurent sans pouvoir comparer (en termes rationnels) leur utilité avant et après l'action. En définitive, personne n'est jamais revenu de « l'autre monde » pour confirmer que la vie après la mort est meilleure ou pire que la vie elle-même. En somme, il n'est pas possible de quantifier de manière crédible l'utilité individuelle de la vie et de la mort : les auteurs d'attentats-suicides peuvent « aller tout droit au paradis en compagnie de soixante-douze vierges » ou terminer en enfer (à supposer que la première option est sans conteste « meilleure » que la seconde)[19].

La rationalité religieuse mérite une attention particulière. Tout d'abord, la religion est un motif important des actions humaines. Les personnes qui se considèrent comme de véritables croyants ont des systèmes de valeurs différents de ceux des athées. Nous sommes donc en présence de deux cadres cognitifs de référence diffé-

rents : ce qui est rationnel pour un croyant (c'est-à-dire justifiable du point de vue de l'utilité post-action) peut être tout aussi irrationnel pour un non-croyant. De nombreuses religions intègrent des cadres de choix rationnels à leurs systèmes de croyances. Les notions opposées de « paradis » et « d'enfer » sont plus ou moins présentes dans la plupart des religions, et la voie qui mène à l'un ou à l'autre dépend de la manière dont les fidèles ont vécu leur vie. Se conformer au dogme garantit une meilleure existence après la mort, et inversement : le pécheur est condamné à un avenir plus sombre dans l'au-delà. Le choix de la vie après la mort est rationnel dans la mesure où la personne « choisit » de vivre dans le péché ou dans la vertu, selon les différentes normes religieuses.

Ce phénomène ne fait cependant pas ici de la religion la variable indépendante ou intermédiaire. Par leurs vertus propres, de nombreuses religions sont discriminatoires « vers l'extérieur » et non discriminatoires « vers l'intérieur ». Autrement dit, elles opèrent une discrimination entre leurs fidèles et ceux des autres religions, entre ce qui est considéré comme le « bien » ou le « mal », mais pas au sein de leur communauté de fidèles ou de celle des non-croyants. Les préférences religieuses sont les mêmes pour tous les adeptes d'une religion : tous les « justes » sont promis à une vie après la mort qui correspond à leurs actes sur Terre, et il en va de même pour les pécheurs. Le même raisonnement s'applique aux fidèles des différentes religions.

Accepter la religion comme un facteur variable soulève la difficulté suivante : le cadre du choix rationnel qui en découle supposerait que tous les acteurs croyants tendent tous vers le même but, « le paradis » pour les chrétiens, le « nirvana » pour les bouddhistes, « shamayim » pour les hébreux ou « jennah » pour les musulmans. Si l'on considère la religion comme la principale force motrice des « nouveaux » terroristes, une autre hypothèse devrait également se vérifier : tous les autres croyants commettraient des actes de violence suicidaire ou non suicidaire en masse, convaincus qu'ils doivent prendre la vie de tous les non-croyants. Si tel était le cas, l'argument de Miese selon lequel il est impossible de prescrire le bonheur universel ne tiendrait pas. Si tous les acteurs avaient prétendument les mêmes préférences au sein des cadres de leur religion respective, leur mode de fonctionnement serait prédéterminé : l'assassinat des hérétiques/des infidèles serait omniprésent chez tous les acteurs religieux. Cette position ne résiste toutefois pas au test de la robustesse scientifique et de la généralisabilité[20]. Les actes suicidaires sont toujours assez rares et toutes les personnes qui croient sincèrement au paradis n'attaquent pas aveuglément les fidèles d'autres religions : les événements tels que le massacre de la Saint-Barthélemy restent des cas particuliers.

L'économie du nouveau terrorisme

D'un point de vue purement économique, les preuves de l'efficacité létale du « nouveau » terrorisme sont contradictoires. Dans l'absolu, le terrorisme suicidaire s'avère plus efficace que sa forme survivaliste : selon Caplan, « un attentat-suicide fait

en moyenne entre quatre et treize fois plus de victimes qu'un attentat sans suicide[21] ». Pape note également que, bien que rares, les attentats-suicides sont responsables de près de la moitié des pertes humaines sur la même période[22]. Les coûts imposés aux gouvernements visés par tous les terroristes sont toutefois sensiblement inférieurs à ceux de la guerre conventionnelle. L'étude de Mueller et Stewart étaye cette affirmation : « [...] les risques de décès annuels liés au terrorisme [...] sont de moins d'un sur un million et se situent par conséquent généralement dans la plage que les législateurs considèrent comme sûre ou acceptable, ne requérant pas de réglementations supplémentaires, surtout celles qui peuvent s'avérer onéreuses[23] ». Charkavorti souligne également que « [...] le terrorisme seul n'atteint nulle part l'ampleur des destructions causées par la guerre classique, les guérillas et les émeutes communautaires[24] ». Enfin, comme le montre l'analyse statistique d'Asthappan pour la période 1951-2006, « [...] les attentats-suicides tuent moins de personnes, même si les incidents se sont multipliés[25] ».

En termes relatifs, toutefois, les morts violentes de « cibles dures », fonctionnaires de haut rang, auraient un impact stratégique bien plus important sur les politiques intérieures et internationales que la mort de citoyens ordinaires[26]. Pourtant, la rationalité demeure relative, même dans ce cas : l'assassinat de l'archiduc François-Ferdinand d'Autriche en 1914 par Gavrilo Princip, un membre de l'organisation terroriste serbe « Main noire », a provoqué des bouleversements politiques bien plus importants que l'assassinat du Premier ministre indien Rajiv Gandhi en 1991 par le LTTE, qui n'a entraîné aucun changement politique international ou régional notoire.

La rationalité stratégique

Sur le plan stratégique, c'est-à-dire au vu des effets à long terme des actes terroristes, le terrorisme individuel peut prendre une apparence rationnelle. La rationalité stratégique suppose que les acteurs poursuivent des objectifs à long terme. Il convient ici de distinguer entre les véritables auteurs des attentats terroristes et leurs instigateurs. Comme le souligne Etzioni : « Il peut, en effet, être rationnel (dans le sens où il sert l'objectif) pour les organisations terroristes et leurs leaders d'envoyer leurs recrues mourir dans des attentats-suicides, cela ne rend toutefois pas cet acte rationnel du point de vue de l'individu recruté[27] ».

Par conséquent, la mort de l'auteur d'un attentat-suicide, qu'elle soit préméditée ou accidentelle, n'est pas la seule variable permettant de définir la rationalité globale de l'acte. L'intervention d'une tierce partie (organisateur des attentats et non leurs auteurs immédiats) est un facteur à prendre en compte.

Qu'ils soient suicidaires ou survivalistes, les actes terroristes ne mettent généralement pas en danger la vie de leurs instigateurs, mais seulement celle de leurs auteurs. Selon Cowen, les leaders des divers groupes et fractions terroristes « [...] peuvent avoir des motivations différentes de celles des troupes qui leur sont subordonnées. Ils

organisent souvent les attentats, mais ne les perpètrent pas eux-mêmes[28] ». Dans cette optique, le risque de périr dans un attentat est minime pour les leaders des groupes terroristes. D'après Pape, « si de nombreux auteurs d'attentats-suicides sont irrationnels ou fanatiques, ce n'est pas le cas des leaders qui les recrutent et les dirigent[29] ». Enfin, Neumayer et Plumper affirment que « les leaders de groupements terroristes sont en grande majorité rationnels et agissent de manière stratégique pour atteindre leur objectif qui consiste à exercer une influence politique sur le système politique de leur pays[30] ».

La rationalité au niveau du groupe

Le terrorisme est généralement une entreprise collective, mises à part quelques rares exceptions comme le double attentat du marathon de Boston en 2013. Le terrorisme individuel demeure une « agrégation de décisions individuelles et le comportement d'un groupe peut être expliqué à partir des comportements individuels[31] ». Les terroristes solidaires peuvent revendiquer leur affiliation identitaire aux organisations terroristes établies, ils n'en demeurent pas moins de simples criminels poursuivant leurs propres objectifs. Cela ne veut évidemment pas dire que la radicalisation ne peut survenir au niveau individuel. Le cas des frères Tsarnaïev est un parfait exemple d'identité terroriste fondée sur des « communautés imaginées[32] ». Ces terroristes avaient peu, sinon aucun contact avec les organisations centrales et ont même attaqué le pays qui n'avait rien à se reprocher vis-à-vis de leur terre natale, la Tchétchénie.

Ceci nous amène à la conclusion suivante : la radicalisation et les motivations politiques sont deux formes de terrorisme distinctes. Pour être véritablement politique, la violence doit en quelque sorte être institutionnellement approuvée par un groupe spécifique. Sans quoi les efforts de la lutte antiterroriste se heurtent au problème de l'irréfutabilité. Si chaque loup solitaire choisit l'identité qui le force à commettre des actes de violence prémédités, il n'y a pas d'autre motivation politique qu'un phénomène isolé. Le discours des frères Tsarnaïev sur leurs motivations politiques est vain : non seulement il ne permet pas de comprendre les motifs des attentats, mais il détourne également l'attention de la lutte antiterroriste, en l'aiguillant vers un terrorisme organisationnel plutôt qu'individuel.

Dans la perspective du choix rationnel, l'objectif au niveau du groupe consiste à augmenter l'utilité agrégée espérée pour l'ensemble du groupe. La différence entre « l'ancien » et le « nouveau » concepts de terrorisme réside dans le degré de rationalité entrant dans la poursuite des objectifs. La plupart des « anciennes » organisations terroristes représentaient des cercles ethniques ou idéologiques limités de partisans au sein desquels elles recrutaient, et luttaient uniquement au profit de ces groupes. Ce qui était essentiellement dû à la spécificité de leurs objectifs stratégiques. Comme la plupart d'entre elles défendaient la justice sociale dans leurs groupes respectifs, leurs partisans appartenaient naturellement à ces communautés.

Parfaite incarnation du terrorisme traditionnel, l'ETA était presque exclusivement composé de nationalistes basques actifs en Espagne. De la même manière, l'IRA-Véritable recrutait uniquement des Irlandais : « des jeunes hommes célibataires sans possession issus de la classe moyenne, dominés de manière de plus en plus disproportionnée par des activistes urbains, qualifiés et socialement mobiles » à travers le monde. L'ASALA grossissait également ses rangs avec de jeunes Arméniens. Il en va de même du PKK : selon Kalyvas, en effet, « [...] il serait difficile de trouver des combattants d'origine turque luttant aux côtés du PKK[33] ». Le « Narodnaya Volya » tout comme « l'Esers » étaient également composés de Russes et étaient uniquement actifs au sein de l'empire de Russie.

D'un point de vue tactique, « l'ancien » terrorisme visait à imposer des coûts humains et économiques insurmontables à la partie adverse dans le but de forcer cette dernière à entreprendre les changements politiques souhaités[34]. Il cherchait, selon Pape, à atteindre ces objectifs en « infligeant suffisamment de souffrance à la société pour vaincre sa volonté de s'opposer aux exigences des terroristes, obligeant ainsi le gouvernement à céder ou la population à se révolter contre le gouvernement [...][35] ». Ceci dit, « l'ancien » terrorisme avait des objectifs limités : « contraindre un gouvernement donné à changer de politique, mobiliser des recrues supplémentaires et des soutiens financiers, ou les deux » ou « [...] inciter la cible à réagir de manière disproportionnée, radicaliser les modérés et rallier des soutiens pour ses objectifs ambitieux sur le long terme[36] ». Ainsi, l'ASALA faisait pression sur la Turquie pour qu'elle reconnaisse le génocide arménien dans le but ultime « [...] de créer un État arménien indépendant et entièrement souverain, incluant la République socialiste soviétique d'Arménie et l'Arménie turque », sans chercher à détruire complètement la République turque per se[37]. L'IRA-Véritable et l'ETA militaient pour la souveraineté de leurs groupes ethniques respectifs (les Irlandais et les Basques) au Royaume-Uni et en Espagne, sans viser l'anéantissement total de l'État de leurs adversaires ni la gouvernance supranationale de l'Union européenne. Les actions du PKK avaient une visée tout aussi circonscrite : obtenir davantage de droits politiques pour leur groupe et « former un État kurde indépendant[38] ». De tels objectifs étaient, en principe, rationnellement réalisables, et démontraient que le « comportement qui bénéficiait non seulement à l'individu, mais également au groupe auquel l'individu était fidèle pouvait aussi être considéré comme rationnel[39] ».

Au niveau stratégique, les objectifs limités des « anciennes » organisations terroristes les poussaient à agir de manière très sélective et à viser essentiellement des « cibles dures ». Ce faisant, les terroristes envoyaient un message clairement rationnel aux successeurs de ces cibles : nous vous tuerons si vous continuez à résister. Plus de 60 pour cent des victimes de l'ETA étaient des membres de la police, de l'armée ou de la classe politique espagnoles, tandis que les civils étaient essentiellement des victimes collatérales ou « des informateurs, des trafiquants de drogue, des entrepreneurs

ne se pliant pas à l'extorsion financière, des adeptes de l'idéologie d'extrême droite ou des personnes impliquées dans la 'sale guerre' contre l'ETA[40] ». L'ASALA était également connue pour viser exclusivement des décideurs turcs et plus particulièrement des diplomates[41]. Pour ses attentats, l'IRA-Véritable a développé un schéma similaire[42]. Le FLMN s'attaquait également avant tout à l'armée et aux installations gouvernementales[43]. Le LTTE s'en prenait de préférence à l'armée, à la police, aux fonctionnaires de l'état et aux citoyens associés aux politiques du gouvernement sri lankais ou les soutenant[44]. Le « Narodnaya Volya » et « l'Esers » se concentraient uniquement sur les « gouverneurs généraux, les maires, les commandants de régiments militaires, les directeurs de prison, les gendarmes, les dirigeants de la police, les huissiers de justice, les gardiens de la paix, les juges et les procureurs [...] les membres de la Douma et même de la famille royale[45].

Le « nouveau » terrorisme est devenu une entreprise véritablement mondiale : à son avant-garde, Al-Qaïda recrute des musulmans et convertit des fidèles dans le monde entier. Ce mouvement ne dispose pas d'un « processus de recrutement unique et homogène pour un groupe, mais de multiples processus de recrutement différents en fonction des régions et des points nodaux dans lesquels le groupe est actif[46] ». L'apparition du « nouveau » terrorisme a, par ailleurs, transformé la stratégie globale de la violence politique, la rendant plus dangereuse que jamais. Cette évolution est le résultat du passage des attentats perpétrés pour des raisons politiques au spectacle orchestré de la violence totale inattendue aux niveaux organisationnel et individuel. Le « nouveau » terrorisme s'est détourné du privilège de « l'adhésion à un club exclusif » pour adopter des tactiques « franchisées » facilement accessibles pour les acteurs organisés ou individuels : toute personne de toute origine vivant en tout lieu peut se radicaliser et commettre des attentats terroristes au nom de toute organisation ou de toute cause.

La rationalité tactique

D'un point de vue tactique, les « nouveaux » terroristes ne sont pas engagés dans une guerre d'usure, mais dans une guerre pour une victoire totale, mais moins perceptible dans un jeu à somme nulle. Ils ne souhaitent pas simplement modifier le système dans lequel ils vivent ou mener leurs entrepreneurs politiques au pouvoir : ils veulent tout détruire pour créer un nouvel ordre mondial, le Califat mondial régi par la Charia. De nombreuses organisations terroristes tchétchènes actives en Russie ont repris cette idée à une échelle régionale de moindre ampleur sous la forme d'un « Imarat » caucasien, terme tchétchène désignant une entité politique islamique dans le Caucase[47].

La difficulté d'une telle approche, du point de vue du choix rationnel, apparaît au niveau des objectifs stratégiques. Les « nouveaux » terroristes n'ont aucun point de référence pour évaluer de manière crédible l'utilité espérée de l'état final visé de leur combat. Le Califat mondial proposé par Al-Qaïda s'inspire de ses diverses formes

historiques, telles que les califats Rashidun, Omeyyade et Abbaside et l'Empire ottoman. Toutefois, ces « mini-califats » souffraient déjà du constant désir de leur peuple de s'écarter de l'islam pur et de la charia pour plus de laïcité. Selon Arnason et Stauth, « l'histoire des états islamiques apparaît comme l'interminable recul de l'exercice du plein pouvoir religieux. Le premier califat [...] a été remplacé par une monarchie, qui [...] a tenté de remplacer l'autorité directe de la religion par un 'sentiment d'appartenance à un groupe et par le glaive' [...][48] ». La rationalité stratégique d'Al-Qaïda comme des organisations terroristes tchétchènes s'appuie sur l'éphémère promesse faite à leurs adeptes hors de tout cadre de référence rationnel qu'ils seront plus heureux dans le Califat mondial.

Du point de vue de la rationalité tactique, le « nouveau » terrorisme peut sembler passablement rationnel au vu de son mode d'action spécifique : la violence aveugle contre les civils. Considérant que tout acte de terrorisme, et en particulier dans sa nouvelle version, est avant tout un spectacle en quête d'un public, Stohl affirme que ses « [...] victimes et toutes les destructions ne sont pas aussi importantes aux yeux de leurs auteurs que le public spectateur de cette destruction dans le monde entier[49] ». Abondant dans le même sens, Crenshaw soutient que « les victimes ou objets d'un attentat terroriste ont peu de valeur intrinsèque pour le groupe terroriste. Elles captent cependant une bien plus vaste audience humaine, dont les terroristes attendent la réaction[50] ». Les données statistiques confirment cette évolution des tactiques asymétriques à travers le monde. Une étude menée par RAND en 2008 recense le décès de 3 827 civils et plus de 8 000 blessés contre seulement 110 soldats tués et 221 blessés dans les attentats perpétrés par Al-Qaïda entre 1994 et 2007[51].

Au lieu d'envoyer un message personnalisé à leurs cibles, en attaquant des acteurs inconnus essentiellement civils, les « nouveaux » terroristes visent indirectement les « cibles dures » en vue d'induire un changement politique. Cette approche diffère sensiblement de celle des « anciens » terroristes, pour qui les victimes se confondaient avec les cibles. Les exigences des « nouveaux » terroristes sont indirectement transmises par les personnes qui survivent aux attentats. Dans ces cas, et notamment quand les actes terroristes menacent de réduire à néant des perspectives de réélection, certains gouvernements sont tentés d'accéder à leurs demandes. Il n'y a rien de pire pour les gouvernements démocratiquement élus que d'assister à la mort d'électeurs innocents. De telles tactiques peuvent en effet, dans une certaine mesure, contribuer à la réussite des terroristes. Parmi les récents exemples de rationalité tactique figure le départ des soldats philippins d'Irak peu après l'enlèvement d'un chauffeur de camion par les extrémistes et le retrait des troupes espagnoles suite à la promesse électorale du Premier ministre Zapatero après les attentats de Madrid en 2004, suivi de près par le Honduras et la République dominicaine[52]. Ces décisions n'ont cependant pas eu les effets désirés sur la mission de lutte antiterroriste à long terme des forces de la coalition en Irak.

Conclusion

L'application du cadre du choix rationnel dans l'étude des motivations et des comportements des « anciens » et des « nouveaux » terroristes diffère sensiblement. L'approche fondée sur la rationalité présuppose que les efforts antiterroristes des acteurs publics luttant contre la terreur soient basés sur la rationalité.

Cette approche ne peut porter ses fruits que dans le cas des « anciens » terroristes affichant des objectifs clairs et tangibles. Cette démarche rendait leur comportement plus ou moins prévisible et facile à cibler, car les sources de menace étaient clairement identifiables. En revanche, les « nouveaux » terroristes sont imprévisibles en ce qui concerne leur portée mondiale, leurs formes changeantes et leurs objectifs flous. Les opérations de lutte antiterroriste mises en œuvre contre les « anciens » terroristes, missions à petite échelle, comme en Irlande et au Pays basque, ou vastes interventions militaires comme en Afghanistan, sont vouées à l'échec.

La « guerre mondiale contre le terrorisme » formulée par le président Bush suite aux attentats du 11 septembre est un terme extrêmement dangereux en l'absence d'une stratégie de désengagement. Les « nouveaux » terroristes ne luttent pas pour des objectifs spécifiques ou concrets. Leur combat est une fin en soi. Cette attitude qui distingue les « nouveaux » terroristes de leurs prédécesseurs représente un grave danger : l'absence d'états finaux clairement définis et réalisables pour les terroristes eux-mêmes. L'établissement de califats mondiaux ou régionaux et de la charia universelle est avant tout une utopie pour les terroristes eux-mêmes, ainsi que pour les cercles antiterroristes.

L'absence de rationalité fait du « nouveau » terrorisme un simple spectacle de la peur avec pour seul but de faire durer le spectacle en augmentant son public. Le succès d'un attentat terroriste ne doit pas être mesuré au nombre de ses victimes, comme indiqué plus haut, d'un point de vue purement rationnel, le taux de létalité du terrorisme est extrêmement bas comparé à d'autres menaces. Les troupes américaines peuvent se retirer d'Afghanistan, cela ne consacrera en aucun cas ni la défaite, ni la victoire des terroristes. La seule manière de mettre un terme au spectacle consiste pour le public à cesser d'acheter des billets. La doctrine philosophique de l'empirisme postule que le monde existe aussi longtemps que nous admettons son existence[53]. Le monde est, par essence, la combinaison des choses qui sont nées en raison du désir des acteurs de les reconnaître. De la même manière, le « nouveau » terrorisme demeurera une menace tant que les cercles antiterroristes continueront à le percevoir comme tel. Quand le public cessera de prêter attention aux multiples vidéos diffusées par des terroristes retranchés dans des grottes sur les réseaux de télévision mondiaux, quand il cessera de s'intéresser aux djihads éphémères lancés de manière sporadique dans différents pays par de nombreuses cellules terroristes et leurs affiliés, quand il commencera à les considérer comme des criminels ordinaires méritant un châtiment adéquat, la pandémie du terrorisme s'estompera progressivement.

Notes

1. Alex Schmid a relevé plus de 190 définitions du terrorisme entre les années 1930 et les années 1980 ; SCHMID, Alex P., et JONGMAN, A.J., *Political Terrorism: A Research Guide to Concepts, Theories, Data Bases and Literature,* New Brunswick, NJ : Transaction, 1983.

2. DAVIS, Paul K., et CRAGIN, Kim, éds., « Social Science for Counterterrorism. Putting the Pieces Together », *RAND : National Defense Research Institute,* 2009, p. 170, www.rand.org/pubs /monographs/2009/RAND_MG849.pdf.

3. CAPLAN, Bryan, « Terrorism: The Relevance of the Rational Choice Model », *The Political Economy of Terrorism* 128, no 1/2, 2006, pp. 91-107 ; CRENSHAW, Martha, « The Causes of Terrorism », *Comparative Politics* 13, no 4, 1981, pp. 379-399 ; KYDD, Andrew H., et WALTER, Barbara F., « The Strategies of Terrorism », *International Security* 31, no 1, 2006, pp. 49-80 ; PAPE, Robert A., « The Strategic Logic of Suicide Terrorism », *American Political Science Review* 97, no 3, 2003, pp. 1-19 ; OBERSCHALL, Anthony, « Explaining Terrorism: The Contribution of Collective Action Theory », *Sociological Theory* 22, no 4, 2006, pp. 26-37 ; LIBICKI, Martin C., CHALK, Peter, et SISSON, Melanie, « Exploring Terrorist Targeting Preferences », *RAND Corporation Monograph Series*, 2007, www.rand.org/pubs/monographs/2007/RAND_MG483.pdf.

4. VAN UM, Eric, « Discussing Concepts of Terrorist Rationality: Implications for Counter-Terrorism Policy », working paper 22, Economics of Security, 2009, p. 9.

5. RIKER, William H., « The Political Psychology of Rational Choice Theory », *Political Psychology* 16, no1, 1995, p. 37.

6. SIMON, Herbert A., « Rationality in Political Behavior », *Political Psychology* 16, no 1, 1995, p. 58.

7. JONES, Bryan D., « Bounded Rationality », *Annual Review of Political Science* 2, 1999, pp. 297–321 ; MONROE, Kristen R., et MAHER, Kristen H., « Psychology and Rational Actor Theory », *Political Psychology* 16, no 1, 1995, p. 2.

8. Pour des références complémentaires concernant le discours sur la logique du comportement approprié et des conséquences espérées, voir les travaux suivants : MARCH, James G., et OLSEN, Johan P., *Ambiguity and Choice in Organizations,* Bergen, Norvège : Universitetsforlaget, 1976 ; MARCH, James G., et OLSEN, Johan P., *Rediscovering Institutions,* New York : Free Press, 1989 ; MARCH, James G., et OLSEN, Johan P., *Democratic Governance,* New York : Free Press, 1995 ; MARCH, James G., et OLSEN, Johan P., « The Institutional Dynamics of International Political Order », *International Organization* 52, no 4, 1998, pp. 943-969.

9. ONEAL, John R., « The Rationality of Decision Making During International Crises », *Polity* 20, no 4, 1988, p. 601.

10. RIKER, William H., « The Political Psychology of Rational Choice Theory », p. 24.

11. VON MISES, Ludwig, *Human Action,* Chicago : Contemporary Books, Inc., 1966, p. 19.

12. MONROE et MAHER, « Psychology and Rational Actor Theory », pp. 1-21.

13. JONES, Bryan D., « Bounded Rationality », p. 306 ; SIMON, Herbert A., « Human Nature in Politics: The Dialogue of Psychology with Political Science », *The American Political Science Review* 79, no 2, 1985, pp. 293-304. Doi :10.2307/1956650.

14. GOLDMANN, Kjell, « Appropriateness and Consequences: The Logic of Neo-Institutionalism », *Governance: An International Journal of Policy, Administration, and Institutions* 18, no 1, 2005. p. 44 ; MARCH, James G., et OLSEN, Johan P., « The Logic of Appropriateness », in *The Oxford Handbook of Public Policy*, éd. GOODIN, Robert E. et al., Oxford : Oxford University Press, 2008, p. 4.

15. COWEN, Tyler, « Terrorism as Theater: Analysis and Policy Implications », *Public Choice* 128, no 1/2, 2006, p. 238.

16. HARRISON, Mark, « An Economist Looks at Suicide Terrorism », *World Economics* 7, no 4, 2006, p. 1.

17. SANDLER, Todd, « Collective Action and Transnational Terrorism », *World Economy* 26, no 6, 2003, p. 785.

18. CAPLAN, « Terrorism: The Relevance of the Rational Choice Model », p. 98.

19. *Id.*, p. 97.

20. SOLER, Lena, et al., éd., *Characterizing the Robustness of Science: After the Practice Turn in Philosophy of Science*, New York : Springer, 2012.

21. CAPLAN, « Terrorism: The Relevance of the Rational Choice Model », p. 94.

22. PAPE, « The Strategic Logic of Suicide Terrorism », pp. 1-19.

23. MUELLER, John, et STEWART, Mark G., « Hardly Existential: Thinking Rationally About Terrorism », *Foreign Policy,* 2 avril 2010, www.foreignaffairs.com/articles/66186/john-mueller-and-mark-g-stewart/hardlyexistential

24. CHAKRAVORTI, Robi, « Terrorism: Past, Present and Future », *Economic and Political Weekly* 29, 36, 1994, p. 2343.

25. ASTHAPPAN, Jibey, « The Effectiveness of Suicide Terrorism », *Journal of the Washington Institute of China Studies* 5, no 1, 2010, p. 22.

26. BERMAN, Eli, et LAITIN, David D., « Hard Targets: Theory and Evidence on Suicide Attacks », décembre 2006, http://econ.ucsd.edu/~elib/Hardtargets.pdf.

27. ETZIONI, Amitai, « Rational Actors: Neither Mad nor M.A.D.1: The Meanings of Rationality, Rogue States and Terrorists », *Defense & Security Analysis* 26, no 4, 2010, p. 434.

28. COWEN, « *Terrorism as Theater: Analysis and Policy Implications* », p. 237.

29. PAPE, « *The Strategic Logic of Suicide Terrorism* », p. 2.

30. NEUMAYER, Eric, et PLUMPER, Thomas, « International Terrorism and the Clash of Civilizations », *British Journal of Political Science* 39, no 4, 2009, p. 712.

31. UM, « *Discussing Concepts of Terrorist Rationality: Implications for Counter-Terrorism Policy* », p. 10.

32. ANDERSON, Benedict, *Imagined Communities: Reflections on the Origin and Spread of Nationalism,* Londres : Verso, 2006.

33. HART, Peter, « The Social Structure of the Irish Republican Army, 1916-1923 », *The Historical Journal* 42, 2009, p. 207 ; KALYVAS, Stathis N., « Ethnic Defection in Civil War », *Comparative Political Studies* 41, no 8, 2008, pp. 1043-1068.

34. MACK, Andrew, « Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict », *World Politics* 27, no 2, 1975, pp. 175-200.

35. PAPE, « *The Strategic Logic of Suicide Terrorism* », p. 4.

36. LIBICKI, CHALK et SISSON, « *Exploring Terrorist Targeting Preferences* » ; LAKE, David A., « Rational Extremism: Understanding Terrorism in the Twenty-first Century », *Dialog-IO,* 2002, p. 26.

37. WILKINSON, Paul, « Armenian Terrorism », *The World Today* 39, no 9, 1983, p. 346.

38. MUKHLIS, Hatem, « Voting Yes to Chaos », *The New York Times*, 18 octobre 2005, p. 27.

39. UM, « *Discussing Concepts of Terrorist Rationality: Implications for Counter-Terrorism Policy* », p. 9.

40. SÁNCHEZ-CUENCA, Ignacio, « The Persistence of Nationalist Terrorism: The Case of ETA », in *Violent Non-State Actors in Contemporary World Politics*, MULAJ, Kledja, éd., New York : Columbia University Press, 2010, p. 24.

41. « *Turkish Diplomats Killed by Armenian Terrorists* », Assembly of Turkish-American Associations, 2011, www.ataa.org/reference/diplomats.html.

42. « *Targets of the Irish Republican Army* », Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism, consulté le 27 septembre 2017, www.start.umd.edu/gtd/search/Results.aspx?chart=target&search=Irish republican army&count=100.

43. « *Targets of the Farabundo Marti National Liberation Front* », Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism, consulté le 27 septembre 2017, www.start.umd.edu/gtd/search/Results.aspx?charttype=pie&chart=target&search=FML.

44. « *Targets of the Tamil Tigers* », Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism, consulté le 27 septembre 2017, www.start.umd.edu/gtd/search/Results.aspx?charttype=pie&chart=target&search=Tamil%20Tigers.

45. « *History. Terrorism in Russia* », K.G. Razumovsky Moscow State University of Technology and Management, http://mgutm.ru/stopteror/histori.php.

46. GERWEHR, Scott, et DALY, Sara, « Al-Qaida: Terrorist Selection and Recruitment », in *McGraw-Hill Homeland Security Handbook*, David Kamien, éd., New York : McGraw-Hill Companies, 2006, p. 75.

47. Les groupes terroristes tchétchènes les plus connus sont les suivants : le Majlis-ul-Shura militaire suprême des Forces moudjahidines unies du Caucase ; le Congrès des peuples d'Itchkérie et du Daghestan ; le front caucasien des forces armées de la république tchétchène d'Itchkérie.

48. ARNASON, Johann P., et STAUTH, Georg, « Civilization and State Formation in the Islamic Context: Re-Reading Ibn Khaldun », *Thesis Eleven* 76, no 1, 2004, p. 39.

49. STOHL, Michael, « Old Myths, New Fantasies and the Enduring Realities of Terrorism », *Critical Studies on Terrorism* 1, no 1, 2008, p. 13.

50. CRENSHAW, « *The Causes of Terrorism* », p. 379.

51. JONES, Seth G., et LIBICKI, Martin C., « How Terrorist Groups End. Lessons for Countering Al Qa'ida », *RAND Corporation Monograph Series*, 2008, www.rand.org/pubs/monographs/2008/RAND_MG7 41-1.pdf.

52. GLANZ, James, « Hostage Is Freed after Philippine Troops Are Withdrawn from Iraq », *New York Times*, 21 juillet 2004, www.nytimes.com/2004/07/21/world/hostage-is-freed-after-philippinetroops-are-withdrawn-from-iraq.html.

53. LOCKE, John, *An Essay Concerning Human Understanding,* Nabu Press, 2010.

Interagir avec les prestataires non étatiques des services de sécurité

Où va l'état de droit ?

Timothy Donais, PhD*

L'état de droit est, de longue date, un élément central dans la programmation de la réforme du secteur de la sécurité (RSS). Dans la mesure où la RSS cherche à garantir que les forces de sécurité sont non seulement efficaces, mais doivent aussi rendre des comptes à l'état et aux citoyens, la vision selon laquelle cette redevabilité est mieux garantie en incorporant la gouvernance de la sécurité dans le cadre de l'état de droit a été relativement peu contestée, à quelques exceptions notables près, malgré les résultats inégaux de la RSS. Dans le contexte des transitions post-conflit en particulier, le discours classique sur la RSS soutient que la (re)consolidation du pouvoir coercitif aux mains de l'état (au sens wébérien du terme) est à la fois justifiée et légitimée par l'instauration parallèle d'un cadre juridique et d'un cadre institutionnel destinés à contraindre et à limiter les bonnes et mauvaises utilisations de ce pouvoir. De même que la RSS est au cœur de l'agenda contemporain du renforcement de l'état, partie intégrante d'un effort plus important tendant à créer des états capables, redevables et à l'écoute, l'état de droit, en tant qu'ensemble de principes et de pratiques cherchant à replacer les relations politiques et socio-économiques dans un cadre transparent et prévisible de règles applicables, occupe encore et toujours une place primordiale dans l'agenda contemporain de la RSS[1].

Or, si ce discours est incontestable du point de vue de sa logique interne et de la façon dont la plupart des acteurs de la RSS distinguent les secteurs de sécurité efficaces des secteurs inefficaces, l'embarras suscité au sein de la communauté élargie de la RSS par l'intérêt croissant porté à la prestation des acteurs non étatiques dans le

*Le professeur Timothy Donais a rejoint Laurier en 2008, après avoir enseigné pendant quatre ans au département de science politique de l'université de Windsor. Ses recherches portent sur la consolidation de la paix après un conflit. Il contribue actuellement à un projet de recherches de plusieurs années, financé par le Conseil de recherches en sciences humaines du Canada, en examinant les questions de « maîtrise locale » dans les processus de consolidation de la paix. Le professeur Donais a écrit *The Political Economy of Peacebuilding in Post-Dayton Bosnia* (Routledge, 2005) et dirigé la publication de *Local Ownership and Security Sector Reform* (Lit Verlag, 2008).

DONAIS, Timothy, « Engaging Non-State Security Providers: Whither the Rule of Law? », *Stability International Journal of Security and Development*, 6, no 1, 2017, DOI : http://doi.org/10.5334/sta.553.

domaine de la sécurité reste difficile à expliquer. Les prestataires non étatiques de services de sécurité, dans ce contexte, incluent les acteurs, des milices aux groupes de surveillance de voisinage en passant par les chefs traditionnels, exerçant un pouvoir coercitif et assurant la sécurité et la protection de communautés particulières ou de territoires spécifiques, en dehors des services formels de sécurité fournis par l'état lui-même. L'existence de formes hybrides de prestation de sécurité, où les acteurs étatiques et non étatiques coexistent et se superposent, est progressivement admise dans bon nombre d'états fragiles et en conflit. Toutefois, ces « ordres » de sécurité, souvent très désordonnés et intrinsèquement instables, voire violents, engendrent une multitude de frictions là où les compétences revendiquées et contestées des différents prestataires de sécurité s'imbriquent les unes dans les autres. Pourtant, si ces mesures hybrides de sécurité sont reconnues, elles sont rarement considérées comme des solutions viables face aux approches classiques de la RSS. Elles sont tout au mieux vues comme des traits éphémères du paysage transitionnel et tolérées tant que l'État peut exercer son monopole réglementaire de l'usage de la force.

Il est certes difficile d'envisager la RSS en dehors de ces hypothèses statocentrées. Mais les formes hybrides de gouvernance de la sécurité se montrent peu à peu plus durables, plus efficaces et moins facilement supplantées que l'on pensait. S'il est probablement prématuré de déclarer, comme Bruce Baker, que « le futur c'est le non-état », l'idée selon laquelle l'hybridité devrait être incorporée dans la programmation de la RSS gagne du terrain. Elle repose notamment sur des considérations très pragmatiques[2]. Comme l'a souligné Kate Meagher, la volonté d'envisager l'hybridité comme modèle viable de gouvernance de la sécurité procède de l'aspiration à des formes de gouvernance moins sophistiquées et moins coûteuses et de la nécessité progressivement admise de juger les systèmes en place pour ce qu'ils sont, et non pour ce que les étrangers aimeraient qu'ils soient[3]. Conformément aux critiques plus générales portées sur la consolidation de la paix libérale, cette ouverture à l'hybridité est aussi une réponse au triomphalisme et au « managérialisme arrogant » de nombreuses interventions en matière de RSS, animées d'ambitions sociales irréalistes et irréalisables et d'efforts permanents visant à étendre la réalité complexe des pays fragiles et en conflit « sur un lit de Procuste de modèles prédéfinis d'état de droit[4] ».

Ce document étudie le rôle des prestataires non étatiques de services de sécurité dans les contextes de la RSS avec, pour toile de fond, un engagement normatif et politique constant des donateurs en faveur d'une intégration de la RSS dans le cadre de l'état de droit. Pour ce faire, il envisage les possibilités d'un agenda « post-libéral » (si ce n'est post-état de droit) de la RSS, qui se distingue de son précurseur libéral par le souci de façonner des stratégies de RSS basées sur les réalités sociopolitiques existant au sein de la société concernée, plutôt que sur des objectifs idéalisés (et sans doute inatteignables). La prise en compte des conditions de départ au lieu (ou du moins en plus) du résultat final mobilise considérablement les intervenants extérieurs

pour comprendre le contexte local dans toute sa complexité dynamique. D'ailleurs, comme l'explique Amitai Etzioni, vu les limites de l'influence internationale, il est plus judicieux de se baser sur les structures et les tendances existantes « que de chercher à en créer de toutes pièces[5] ». En somme, il convient d'aborder la RSS par le biais d'une analyse des systèmes, basée sur une lecture attentive des acteurs concernés, des structures d'incitation qui s'offrent à eux, des dynamiques institutionnelles et relationnelles qui les relient, et des facteurs possibles de changement. Cela conduit presque inévitablement à une forme de RSS basée sur l'équilibre des forces politiques existantes et leurs interconnexions plutôt que sur des monopoles wébériens délimités et contraints par un cadre de lois capables de régler la vie politique tout en siégeant en dehors de la sphère politique. Du reste, il est illusoire et sans doute inutile d'attendre des donateurs qu'ils mettent de côté leurs engagements traditionnels en faveur de l'état de droit dans leurs interventions en matière de RSS. Ce document explique en effet que si l'on envisage l'état de droit comme l'élément, à développer au fur et à mesure, d'un cadre complexe et évolutif de redevabilité pour la prestation de services de sécurité, il reste la pierre angulaire d'une entreprise plus globale de RSS.

La suite du document s'articule comme suit. La première partie analyse les principes fondamentaux de la RSS classique, en examinant plus particulièrement la prééminence du monopole et de la responsabilité, ainsi que l'immense difficulté à les atteindre l'un ou l'autre, et plus encore l'un et l'autre, dans les délais standard de la plupart des interventions internationales contemporaines. Dans la deuxième partie, le document étudie les relations délicates entre les prestataires non étatiques de services de sécurité et l'état de droit, tout en soulignant pourquoi les mesures de sécurité hybrides, c'est-à-dire associant des acteurs étatiques et non étatiques, sont plus vraisemblablement conflictuelles que collaboratives. La troisième partie expose à grands traits une vision à plus long terme de l'évolution du secteur de la sécurité fondée sur un cadre réglementaire, en mettant en exergue la capacité émergente des institutions d'état à régir, plutôt que monopoliser, la prestation de services de sécurité. La conclusion passe en revue cette analyse dans son ensemble en suggérant que, dans la mesure où la RSS est, au fond, une question de transformation systémique de la prestation de services de sécurité, l'état de droit continue de fournir un référentiel de repères stratégiques afin de guider le processus.

La RSS conventionnelle : une fusion du monopole et de la redevabilité

Louise Andersen constate que le prétendu modèle dominant de la RSS, pivot du projet d'établissement d'une paix libérale dans les états fragiles, « n'implique pas simplement d'apprivoiser le Léviathan de Hobbes, mais d'établir le Léviathan[6] ». Cette caractérisation souligne subtilement l'imbrication des principes de monopole et de

redevabilité à la base de la RSS conventionnelle, tout en évoquant l'immensité de la tâche. Il est clair, depuis un certain temps, que les piètres performances de la RSS sont étroitement liées au fossé séparant à la fois les nobles principes des réalités du terrain, et à l'écart entre d'un côté l'ambition générale de l'agenda de la RSS et de l'autre le temps, les ressources et le capital politique requis pour faire de cette ambition une réalité.

Au sujet du monopole, la programmation de la RSS a mis au jour au court du dernier quart de siècle les attributions limitées de l'état et de son appareil judiciaire et de sécurité dans un grand nombre d'environnements fragiles et en conflit. Selon les chiffres généralement avancés et communément admis (quoique difficiles à vérifier), plus de 80 pour cent des prestations de justice et de sécurité dans les états bénéficiant de la programmation de la RSS sont assurés par des acteurs non étatiques[7]. En effet, l'essence même de la faiblesse ou fragilité d'un état tient en partie à l'incapacité du gouvernement à exercer un contrôle effectif sur le territoire, tandis que le conflit aggrave la fragmentation de la prestation des services de sécurité. Partant, la programmation de la RSS s'est efforcée le plus souvent de surmonter le défi du transfert du pouvoir des acteurs non étatiques, qui pour la plupart se sont montrés récalcitrants à la collaboration, aux acteurs étatiques.

Comme Ken Menkhaus le fait remarquer dans le cas de la Somalie, les efforts consentis pour renforcer le secteur formel de la sécurité dans ce pays « affrontent de puissants courants contraires » : les prestataires non étatiques de services de sécurité sont non seulement plus capables que les acteurs étatiques dans une grande partie du pays, mais ils ont également d'importants intérêts économiques à maintenir le statu quo[8]. La Somalie fournit certes un exemple extrême d'une prestation fragmentée des services de sécurité. Mais l'échec du modèle du monopole de la RSS à appliquer son principe de base s'observe dans bon nombre de situations post-conflit.

La RSS conventionnelle n'a sans doute pas été plus effective quant à la mise en œuvre de son deuxième principe de base : s'assurer que ceux qui exercent une force coercitive se comportent de manière responsable et rendent compte de leurs actions. C'est sur ce point que l'état de droit s'imbrique plus directement dans la gouvernance de la sécurité ; selon la typologie de Thomas Carothers, cela représente la réforme du « troisième type », d'ordre juridique, consistant à renforcer la conformité du gouvernement à la loi et, plus généralement, à mettre en place des mécanismes robustes contraignant le pouvoir exécutif[9]. Dans les environnements instables et incertains en particulier, il n'est pas surprenant que les acteurs dominants voient peu d'intérêt à limiter leur pouvoir en le soumettant, ainsi qu'eux-mêmes, à l'état de droit. En effet, comme Agnès Hurwitz le fait remarquer de façon plus générale, « les programmes cherchant à renforcer ou à ré-établir l'état de droit dans des contextes de consolidation de la paix ont rarement rempli leur objectif minimal de garantie des droits de l'homme, de sécurité ou de développement[10] ». Cela est dû en grande partie au fait

que l'état de droit n'est pas tant une question d'établissement des institutions que de changement des normes. Or un changement normatif s'inscrit presque invariablement dans la durée[11]. En matière de respect et d'observation de principes abstraits comme la justice, la responsabilité et la transparence par les élites nationales en particulier, il y a loin de la coupe aux lèvres : l'analyse coût-avantages et, plus prosaïquement encore, la poursuite de l'intérêt politique et économique individuel pèsent lourd dans la balance. De plus, comme l'a démontré Alex Berg, dans les environnements en conflit, l'état de droit émerge rarement d'une « illumination » des élites. Il résulte plutôt de schémas spécifiques et relativement peu courants des relations entre société et état (notamment dans les régimes ancrés dans des coalitions larges ou fragmentées aux sources de revenus insuffisantes), modifiant les structures d'incitation qui se présentent aux élites, de sorte qu'elles sont plus enclines à accepter les contraintes juridiques et institutionnelles[12].

Vu la difficulté à réaliser l'ambition démesurée sous-tendant le paradigme de la RSS conventionnelle, à savoir d'un côté restaurer les monopoles sur l'usage légitime de la force et, de l'autre, inscrire la gouvernance de la sécurité dans un cadre juridique robuste, l'impérieuse nécessité de se doter de modèles plus réalistes s'est fait sentir. En ce sens, les reproches formulés contre la RSS conventionnelle trouvent un écho chez Marina Ottaway qui, dans une critique plus globale, juge le modèle de reconstruction démocratique attrayant en théorie, mais inenvisageable dans la pratique, du fait de l'immense gouffre séparant les réalités sur le terrain et les objectifs idéalisés[13]. Comme Ottaway, les partisans d'une RSS de deuxième génération aspirent à des analyses plus réalistes et moins présomptueuses qui garantissent cependant un engagement fondamental en faveur de l'amélioration de la sécurité de l'état et de la sécurité humaine dans les pays fragiles et en conflit. Certes les approches hybrides gagnent en réalisme en évitant de recourir aux modèles formels pour renforcer les mécanismes existants de prestation de services de sécurité. Mais l'hybridité implique également, et pour ainsi dire par définition, de réconcilier des pratiques et des principes radicalement différents. Reconnaître la prestation non étatique de services de sécurité tout en affirmant un engagement indéfectible en faveur de l'état de droit, tel est le paradoxe.

Les prestataires non étatiques des services de sécurité et l'état de droit : une relation compliquée

Alors que, ces dernières années, les failles de la consolidation de la paix libérale comme de la RSS conventionnelle se sont fait jour, notamment du fait de l'incapacité de chaque cadre à combler le fossé entre les promesses et les résultats, l'état de droit continue à jouir d'une légitimité forte et incontestée d'une façon quelque peu remarquable. Sans compter que l'état de droit peut être considéré comme un *primus inter pares* parmi tous les grands principes sous-tendant les interventions libérales dans les

états fragiles et en conflit. Autrement dit, l'état de droit est une condition essentielle à la réalisation des principaux biens publics associée au paradigme moderne de la bonne gouvernance, du développement économique aux droits de l'homme, en passant par la démocratisation.

Si la littérature traitant de sa signification et de sa teneur substantielle abonde, l'état de droit peut se définir essentiellement, selon les termes de Thomas Carothers, « comme un système dans lequel les lois sont connues de tous, ont un sens clair et s'appliquent de façon égale à tout le monde[14] ». Comme le souligne également Carothers, l'état de droit est foncièrement dépendant de l'impartialité, de la compétence et de l'efficacité des principales institutions juridiques comme les tribunaux, les procureurs et la police, et plus généralement de l'intégration du gouvernement et de la gouvernance à un cadre juridique global[15].

Deux aspects de cette définition semblent tout particulièrement pertinents pour la réflexion sur la relation entre l'état de droit et la prestation non étatique de services de sécurité dans des contextes transitionnels. Le premier se rapporte à la définition du pouvoir de l'état : tandis que la plupart des visions de l'état de droit incluent des articulations du droit des citoyens à une procédure régulière *et* à l'égalité devant la loi, la principale énigme que les réformateurs juridiques doivent résoudre dans les états fragiles et en conflit est de savoir comment confier le pouvoir à l'état et, en même temps, le contraindre, conformément au principe général selon lequel il n'y a « pas de pouvoir sans responsabilité[16] ». Toutefois, comme Lisa Denney le suggère, les termes « non étatique » et « informel » restent utiles du point de vue analytique lorsque l'on fait référence aux dispositions de sécurité hybride, *précisément* parce qu'ils « témoignent du large éventail d'arrangements qui, d'une certaine façon, opèrent au-delà du filet de responsabilités de l'état[17] ». Autrement dit, admettre la réalité de la prestation *non étatique* de services de sécurité reste un défi si l'on envisage la RSS comme le simple prolongement de l'état de droit dans la sphère de la sécurité, surtout parce que la légitimité des prestataires non étatiques de services de sécurité s'appuie plutôt sur des fondements *extrajuridiques*.

Le deuxième aspect de la définition de Carothers qu'il convient de souligner à cet égard est sa nature apolitique en apparence, avec des lois et des gardiens agissant comme des arbitres neutres de la vie sociale et politique[18]. Mais un tel cadrage de l'état de droit dissimule la réalité autant qu'il la révèle. Étant donné que les lois elles-mêmes, n'étant guère plus que des mots couchés sur le papier, n'ont pas d'autorité intrinsèque, un état de droit (*rule of law*) authentique, par opposition à la règle par le droit (*rule by law*), exige que les éléments composant la société quelle qu'elle soit, et tout particulièrement ceux qui détiennent le pouvoir, consentent de manière intersubjective à se soumettre à l'autorité de la loi abstraite. En ce sens, l'acceptation de l'état de droit de la part des régulateurs et des régulés constitue, du moins dans les contextes démocratiques libéraux, un élément central du contrat social qui gouverne les rela-

tions entre la société et l'état. Historiquement, le consensus social sur le caractère central de l'état de droit comme base de la gouvernance a émergé d'une longue lutte politique, parfois violente (rappelons-nous le long chemin parcouru par l'Angleterre de la Magna Carta à la monarchie constitutionnelle moderne), dont l'issue n'est en aucun cas connue à l'avance. Le principal défi de ceux qui cherchent à intégrer l'état de droit dans les états en confit est, par conséquent, qu'il existe trop peu de bons modèles passant outre les dynamiques violentes et désordonnées de la contestation politique pour construire un consensus entre acteurs sociaux aux pouvoirs différents (et méfiants les uns envers les autres) sur la sagesse, l'attrait et la légitimité de l'état de droit comme principe de gouvernance globale. En définitive, comme l'ont suggéré Janice Stromseth et al., « rares sont les théoriciens de l'état de droit à s'être colletés avec le problème de savoir *comment* des cultures de l'état de droit peuvent être créées[19] ».

Malgré une forte conviction selon laquelle l'état de droit offre le seul cadre viable et durable à une gouvernance de la sécurité responsable et redevable, les modèles classiques de réforme du secteur de la sécurité n'ont jamais véritablement proposé de vision probante sur la façon d'amener le changement. Ils n'ont pas non plus complètement accepté la réalité selon laquelle, dans la plupart des cas, les services étatiques et non étatiques continueront de coexister pendant une période indéterminée, en s'appuyant sur des sources de légitimité très diverses, offrant ainsi des niveaux variables de sécurité ou d'insécurité, et obligeant les citoyens, en tant que consommateurs de la sécurité, à évoluer sur des terrains exceptionnellement complexes[20]. Pour les réformateurs extérieurs, ces terrains ne sont pas moins difficiles à gérer (même s'ils sont moins menaçants du point de vue existentiel), notamment en raison de la difficulté à distinguer les bons acteurs des mauvais et des limites inhérentes à l'effet de levier extérieur. Par conséquent, les donateurs restent focalisés sur la réforme au niveau de l'État des systèmes de sécurité et de justice et négligent la majorité des mécanismes assurant au quotidien des services de sécurité et de justice[21]. À l'inverse, une réflexion sur les « arrangements intérimaires de sécurité », même si la période intérimaire dans ce contexte peut se mesurer non pas en années, mais en décennies, voire en générations, exigerait de s'engager dans la confusion des dispositions existantes en matière de sécurité, plutôt que de les contourner ou de ne pas en tenir compte.

En 2011, le Comité d'aide au développement de l'OCDE a été l'un des premiers acteurs à vouloir fournir un cadre politique à ce type d'engagement. Soulignant le rôle central de la légitimité dans le cadre de débats plus larges sur la gouvernance, le CAD-OCDE a expliqué que les efforts de reconstruction des états fragiles ou en conflit devraient avoir pour fil rouge la « légitimité fondée », recherchée à travers des « stratégies volontaristes consistant à allier les institutions de gouvernance autochtones indigènes, coutumières et communautaires de gouvernance avec des institutions introduites, similaires à celles des états occidentaux, dans le but de créer une interac-

tion constructive et des ajustements mutuels positifs[22] ». Si l'idée de greffer des normes et des institutions occidentales sur des systèmes préexistants ayant une résonnance sociale et culturelle auprès des populations locales est intéressante, dans la sphère particulière de la prestation de services de sécurité, ces « alliances » entre acteurs étatiques et non étatiques risquent d'être particulièrement tendues. Mais souligner ces tensions n'est pas nier la possibilité ni l'existence de dispositions collaboratives en matière de sécurité entre acteurs étatiques et non étatiques, indépendamment de toute intervention extérieure ; Baker a par exemple décrit ce type précis de collaboration entre les autorités étatiques et les structures coutumières au Somaliland[23]. Il convient de noter que de tels arrangements devraient être exceptionnels et non habituels, en raison justement de la multitude et de la variété des acteurs composant les systèmes de sécurité dans les environnements en conflit, de la nature particulière des relations de puissance dans ces contextes, et des tensions inhérentes à la prestation privée de services de sécurité publique.

Premièrement, l'univers des acteurs non étatiques de sécurité, remarquablement varié, s'étend des chefs traditionnels aux sociétés secrètes, et des groupes de surveillance de voisinage aux gangs, en passant par les milices et les seigneurs de guerre. Ces acteurs peuvent entretenir parfois des liens ancestraux de réciprocité avec leurs communautés clientes, ou bien être nés dans des contextes de conflit, sans grands liens directs et historiques avec des communautés particulières. William Reno, par exemple, a fait la distinction entre les milices protectrices et les milices prédatrices. Les premières dépendent des communautés locales sur le plan des ressources et leur sont liées par un maillage dense de valeurs, de croyances et d'identités[24]. Mais la réalité est plus compliquée, car des acteurs donnés peuvent être simultanément perçus comme prédateurs et protecteurs par différents segments des communautés avec lesquelles ils interagissent, avec une perception évoluant au fil du temps. Plus généralement, Baker et Scheye ont expliqué qu'il n'y a pas de raisons *a priori* de supposer que les acteurs non étatiques sont moins capables de faire respecter les droits de l'homme ou de rendre des comptes, car ils peuvent « refléter plus précisément les croyances et les besoins locaux et être considérés par les autochtones comme plus légitimes[25] ». Certes, les expériences variées de prestation non étatique de services de sécurité menées dans diverses situations montrent que l'état de droit n'est pas un prérequis de la redevabilité : malgré l'écart abyssal en termes de pouvoir entre les prestataires de services de sécurité et les bénéficiaires, des éléments laissent penser que des seigneurs de guerre sont « apprivoisés » par des liens avec des formes plus traditionnelles d'organisation et que des milices, notamment celles qui sont intégrées à des communautés spécifiques, sont « civilisées » sous l'effet de la pression sociale[26]. Toutefois, l'intégration sociale ne garantit pas que les « protégés » pourront demander des comptes en toute fiabilité à leurs « protecteurs », vu la nature changeante et imprévisible de la plupart des arrangements informels de gouvernance : autrement dit, la prestation non étatique de

services de sécurité peut aussi bien affaiblir que renforcer la sécurité de certaines communautés. Le contexte est, sans grande surprise, un paramètre essentiel.

Deuxièmement, comme la RSS a toujours fait partie d'un projet plus vaste axé sur la réorganisation du mode d'exercice et de contrôle du pouvoir dans des sociétés particulières, les arrangements de sécurité hybride peuvent générer une dynamique concurrentielle du pouvoir, tant entre les acteurs étatiques et non étatiques, qu'entre les acteurs non étatiques eux-mêmes, car ils doivent apporter une cohabitation respectueuse et mutuellement consolidante entre prestataires de niveaux différents. D'un côté, dans ces contextes, et étant donné les enjeux élevés et la conviction historique que la prestation de services de sécurité est au cœur même de la définition du statut d'état contemporain, il est peu probable que l'état adhère avec grand enthousiasme à une norme émergente de gouvernance hybride de la sécurité[27]. De l'autre, l'insécurité persistante du « moment » post-conflit et la politique économique de la prestation privée de services de sécurité (quand les ressources manquent, de nombreux prestataires de sécurité ont du mal à résister à la tentation de renforcer l'autorité coercitive, par intérêt politique ou économique) révèlent les risques réels de voir, en l'absence d'un quelconque cadre réglementaire, les luttes persistantes pour le pouvoir et l'autorité tourner très mal. Ce prisme de la dynamique de sécurité concurrentielle permet précisément de comprendre comment la situation post indépendance au Soudan du Sud a dégénéré en guerre.

Troisièmement, comme le font remarquer Baker et Scheye, la justice et la sécurité sont toutes deux, fondamentalement, des biens publics, une réalité dont les dispositions hybrides de sécurité s'accommodent mal[28]. S'il n'y a bien sûr aucune garantie que les prestataires de services de sécurité publique prendront au sérieux leurs responsabilités en matière de sécurité publique (en effet dans les environnements en conflit, une pléthore d'exemples illustre malheureusement l'exploitation des services publics pour servir un intérêt privé), il y a, à tout le moins, une aspiration normative à ce qu'au fil du temps, les forces de sécurité publique agiront au nom de la sécurité publique. À l'inverse, l'hybridité implique une prestation de services de sécurité imbriqués sur plusieurs niveaux où les acteurs non étatiques en particulier offrent des services de sécurité à des segments particuliers de la population, tandis qu'ils représentent pour d'autres des agents d'*insécurité*. Dans ces contextes, la fourniture de services de « sécurité publique » peut s'avérer au mieux inégale et incomplète, tandis que les perspectives d'encouragement d'une multiplicité de prestataires non étatiques adhérant à une philosophie de sécurité publique restent résolument incertaines.

Pour ces raisons, une certaine prudence s'impose quant aux capacités à long terme des arrangements hybrides de sécurité à offrir, aux populations durement éprouvées des états en conflit, de meilleurs résultats en matière de sécurité humaine. En effet, en se référant au contexte spécifique de l'Afrique, Kate Meagher met en garde contre les dangers de l'inversion plutôt que de la maîtrise des tendances essen-

tialistes de la pensée antérieure sur la gouvernance de la sécurité. Comme elle le suggère, dans la mesure où « la condamnation de l'ordre non étatique comme étant institutionnellement destructeur a laissé place à sa célébration en tant que véhicule de formes intégrées de l'ordre et de l'autorité », l'on s'expose au risque de ne pas faire la distinction entre formes constructives et corrosives de l'ordre non étatique[29]. Dans le même temps, l'empressement à adhérer aux arrangements existants en matière de gouvernance de la sécurité, au lieu de s'efforcer de trouver une issue idéale, comporte un danger : celui de perdre de vue le fait que la RSS est foncièrement une question de changement systémique. En effet, la littérature sur la gouvernance des services non étatiques de sécurité a notamment souligné les améliorations tactiques des dispositions de sécurité sur le terrain aux dépens d'une attention plus soutenue sur la façon dont les systèmes de sécurité pourraient être transformés à plus long terme. Nous étudions cette question dans la partie suivante en suggérant que, même dans le contexte de l'hybridité de la sécurité, l'état de droit comme ensemble de principes essentiels de gouvernance peut continuer à offrir une série de repères permettant aux praticiens de la RSS de dépasser la reconnaissance du rôle joué par les prestataires non étatiques de services de sécurité dans les contextes de la RSS pour engager avec eux un dialogue constructif tourné vers l'avenir.

La quadrature du cercle — Une défense qualifiée de l'état de droit

Pour concilier un engagement continu en faveur de l'état de droit et la reconnaissance de la prestation non étatique de services de sécurité, il convient de comprendre que la plupart des partisans des stratégies non étatiques de sécurité ne sont pas aussi radicaux qu'ils en ont l'air à première vue. Implicitement ou explicitement, bon nombre d'entre eux continuent à admettre le rôle crucial, quoiqu'un peu transformé, de l'état au sein d'un cadre évolutif de gouvernance de la sécurité. De la même façon, ils reconnaissent souvent encore l'impératif d'une gouvernance de la sécurité enveloppante au sein d'un cadre fondé sur des règles applicables. Baker et Scheye, par exemple, partent du postulat selon lequel, quelle que soit l'identité spécifique des acteurs *fournissant* des services de sécurité :

> Une fonction de principe d'un état fragile se relevant d'un conflit pourrait être de surveiller, d'autoriser et de réguler les activités des prestataires non étatiques de services. Il ne s'agit plus d'un état défini en termes de monopole du contrôle de la violence et de la coercition, mais plutôt un d'état hautement limité et circonscrit, œuvrant par le biais de partenariats et d'associations uniques avec des acteurs et des organisations non étatiques de la société civile[30].

De même, dans le cadre d'une réflexion plus large sur la nécessité de développer des stratégies non étatiques de RSS, Michael Lawrence défend la notion de l'état régulateur, chargé de définir dans les grandes lignes la prestation de services de sécurité,

« en particulier des normes de droits de l'homme, d'accessibilité et de responsabilité[31] ». Même dans un contexte comme la Somalie, cas classique d'un « État négocié » où les autorités publiques affaiblies n'ont guère d'autre choix que de négocier avec de puissants acteurs non étatiques, Menkhaus conclut que la réglementation par l'état de la prestation privée de services de sécurité reste possible, bien qu'elle fasse partie d'un processus long et tortueux « par lequel les autorités étatiques jouissent finalement d'une primauté sur les prestataires non étatiques et infra étatiques de services de sécurité[32] ».

Par conséquent, il transparaît de ces exposés une théorie incrémentaliste à long terme de la transformation du secteur de la sécurité favorisant un glissement progressif du pouvoir des acteurs non étatiques vers les acteurs étatiques, et en parallèle le repositionnement de l'état comme autorité régulant la prestation des services de sécurité et non qui en détient le monopole. Au centre de cette vision du changement réside la capacité en développement (et la légitimité) de l'état à faire et à mettre en œuvre les règles, les lois et les réglementations. Certes, à court terme, l'état pourrait n'avoir guère d'autre choix que de s'en remettre à la capacité et à la légitimité des prestataires non étatiques de services de sécurité et, à moyen terme, de partager l'autorité avec ces mêmes acteurs. Mais à long terme, l'état souverain devrait affirmer sa primauté sur les acteurs non étatiques dans les affaires de gouvernance de la sécurité, à travers ce que Menkhaus décrit comme une combinaison de négociation, de confrontation et de coopération[33]. Bien sûr rien de cela n'est incompatible avec l'impératif à court terme d'améliorer la gouvernance de la sécurité « existant effectivement » par des efforts constants visant à mettre en place des partenariats, à faciliter la collaboration et à atténuer les frictions avec un large éventail de prestataires de services de sécurité.

Vu sous cet angle, une conception plus souple de la façon dont l'état de droit pourrait au fil du temps lier l'état et le non-état, les prestataires de services de sécurité et les consommateurs, ou encore différents types de prestataires entre eux, pourrait même offrir un cadre raisonnablement contraignant à un engagement international dans le secteur de la sécurité des états fragiles et en conflit. Tout en évitant de tomber dans l'écueil à la fois de l'« orientalisme juridique » et de l'ingénierie sociale conduite de l'extérieur, la force de cette vision peut résider dans sa capacité à combler le fossé entre l'impératif de baser la RSS sur les conditions réellement existantes et la maxime d'Alice au pays des merveilles selon laquelle il faut savoir où l'on va pour espérer y arriver[34]. En ce sens, conceptualiser la RSS sous l'angle d'une expansion graduelle de la capacité de l'état à inclure la prestation des services de sécurité dans un cadre commun de règles permet au moins d'offrir des lignes directrices pour collaborer avec les prestataires non étatiques de services de sécurité sans chercher outre mesure à en normaliser les résultats finals.

Il est important d'adhérer à la vision qu'ont les intervenants extérieurs du changement progressif des systèmes de sécurité, notamment en raison du fossé séparant le besoin de penser le changement en termes systémiques et l'incapacité chronique des

acteurs internationaux, malgré la reconnaissance habituelle de l'holisme comme principe clé de la RSS, à s'engager dans le secteur de la sécurité des états en conflit en tant que systèmes complexes. En effet, l'échec de la coopération, de la coordination et de la planification stratégique reste, à de nombreux égards, le talon d'Achille de l'entreprise de la RSS dans son ensemble. Trop souvent, cette dernière revêt la forme d'une suite de projets discrets, non connectés et limités dans le temps plutôt que d'un plan cohérent et intégré destiné à faire passer les sociétés en conflit de l'insécurité vers la sécurité. Aussi, quand, dans une réflexion du reste excellente sur la gouvernance, Michael Lawrence suggère de définir et de mettre en œuvre des stratégies non étatiques de RSS, il ne ressort pas clairement qui est appelé à les créer, à les superviser ou à les opérationnaliser (exception faite d'une référence générale à la « société civile locale », qui semble mal taillée pour endosser ce rôle)[35]. De même, selon Lawrence, « l'objectif clé de la stratégie non étatique de RSS est l'ouverture de nouveaux canaux de communication et de dialogue entre les prestataires de services de sécurité sur le terrain, les citoyens, la société civile, les acteurs internationaux et l'état[36] ». La proposition est aisément défendable, certes. Mais en l'absence d'un lien cohérent entre la fin et les moyens, elle risque de n'introduire dans la RSS qu'une version de l'hypothèse du contact selon laquelle en mettant les acteurs clés en relation, on suppose que de bonnes choses en résulteront.

Si elle peut s'avérer trop minimaliste pour collaborer effectivement avec des composantes interconnectées et variables de la gouvernance de la sécurité hybride, la stratégie alliant des efforts à l'appui de formes flexibles, larges et spécifiques de gouvernance de la sécurité à l'engagement renouvelé des intervenants de la RSS en faveur d'un « réseau d'action effective », pour reprendre les termes de Robert Ricigliano, semble être plus prometteuse[37]. Comme il le suggère, la pensée systèmes met en exergue les approches itératives, l'apprentissage par la pratique et le travail avec (et dans) le système afin d'identifier et de mettre à profit les occasions d'un changement positif, qui pourrait en fin de compte servir de base pour des changements plus significatifs[38]. Si une analyse et une compréhension minutieuses et nuancées de la dynamique des systèmes sont nécessaires, cela n'implique pas nécessairement une planification et une coordination centralisées et sophistiquées. En revanche, des réseaux de communications ouverts sont requis, ainsi qu'une compréhension commune des objectifs globaux et des règles générales, et la volonté de la part de tous les membres d'envisager les efforts individuels dans le cadre d'une dynamique de réforme plus ample[39]. Dans ce contexte plus général, des efforts continus afin de faire évoluer des systèmes fondés sur les règles pourraient constituer un repère commun vers lequel les actions des intervenants peuvent converger.

Des efforts importants consentis durablement en faveur de l'état de droit et du développement de la capacité de l'état permettraient également de diminuer la résistance des acteurs étatiques à mettre en place des accords externes avec des prestataires

non étatiques de services de sécurité. Comme le montre l'évolution du discours sur la maîtrise nationale, les gouvernements des états fragiles et en conflit (prétendument représentés par le g7+) sont de plus en plus sensibles au non-respect, réel ou perçu, par le donateur, de leurs prérogatives souveraines. Par conséquent, ils ont tenté ces dernières années d'utiliser les engagements internationaux à respecter la « maîtrise nationale » comme un moyen de réaffirmer leur contrôle sur des programmes de réformes post-conflit. Comme l'on pouvait s'y attendre, la sensibilité des élites dirigeantes est particulièrement prononcée dans le domaine de la gouvernance de la sécurité, à la fois parce que la prestation de services de sécurité est de longue date considérée comme l'apanage de l'état et en raison de la valeur intrinsèque des systèmes de sécurité comme moyens de maintenir le contrôle, d'établir la légitimité ou de générer des rentes politiques, sociales ou économiques[40]. Dans les environnements où les gouvernements voient les acteurs non étatiques comme des adversaires empiétant sur leur autorité ou leur légitimité, les stratégies non étatiques de RSS ne tenant pas compte de ces tensions risquent tout d'abord de s'aliéner les appuis essentiels à leur mise en œuvre. Selon les termes d'Erwin van Veen et de Maria Derks, « quand les initiatives de justice et de sécurité sont perçues par les élites comme des menaces potentielles pour leurs propres intérêts, elles sont quasiment sûres d'échouer[41] ».

Paradoxalement, une interaction effective avec les prestataires non étatiques de services de sécurité exige également des stratégies d'engagement, admises de part et d'autre, alignées sur les structures d'incitation se présentant aux élites gouvernantes. Au-delà des appels au pragmatisme, pressant les élites gouvernantes à soutenir toute stratégie améliorant la prestation de services de sécurité, surtout si elles peuvent en retirer un certain crédit, l'intégration des stratégies de RSS dans le cadre plus large du développement d'un état de droit centré sur l'état pourrait aider à compenser les calculs à somme nulle des acteurs aussi bien étatiques que non étatiques. Cela apporterait également aux élites étatiques l'assurance que, à long terme, les tendances favorisent la capacité de l'état à commander et à réguler (sans nécessairement monopoliser), le secteur de la sécurité au sens large. Dans ce contexte également, une politique attentive d'incrémentalisme pourrait être perçue comme un avantage plutôt qu'un inconvénient, surtout au vu de la difficulté à s'assurer que les efforts visant à amener les acteurs étatiques et leurs actions, et pas seulement les prestataires de services de sécurité, dans un cadre réglementaire, ne sont pas perçus comme une menace ouverte aux intérêts des élites.

Conclusion

La recherche constante de méthodes améliorées et viables de réforme du secteur de la sécurité reflète le consensus grandissant sur les inadéquations normatives du modèle du monopole dans la vaste majorité des contextes de réforme. Dans l'esprit du

proverbe « *you can't get there from here* » (Vous ne pouvez pas arriver là-bas d'ici), il y a fort à parier que la plupart des états entreprenant une RSS ne seront pas en mesure d'avoir le monopole de la prestation des services de sécurité sur leur territoire dans un délai réaliste. La solution d'une gouvernance de sécurité hybride, admettant la juxtaposition désordonnée, instable et imbriquée de services de sécurité étatiques et non étatiques dans de nombreux états fragiles et en conflit, semble à l'inverse pâtir d'un défaut de prescription. Autrement dit, si l'hybridité désigne souvent avec justesse une « gouvernance de la sécurité réellement existante », elle est bien moins utile comme feuille de route pour la transformation durable de la prestation de services de sécurité dans les états en conflit.

En mettant tout particulièrement l'accent sur les relations entre la RSS et la promotion de l'état de droit, ce document montre que l'état de droit, même vaguement défini, a un rôle important à jouer, celui d'émettre des lignes directrices stratégiques en matière de RSS. Il est pour cela primordial de séparer les concepts du monopole et de la redevabilité. Tandis que les premières analyses soulignaient la redevabilité *dans le contexte* du monopole de l'état sur l'usage de la force, l'idée soutenue ici, en cohérence avec les apports de la littérature sur les acteurs non étatiques de la sécurité, est double : d'un côté, la redevabilité est au moins aussi importante, si ce n'est plus, dans les situations de gouvernance de sécurité hybride ; de l'autre, l'état de droit offrira à long terme une base plus solide en matière de redevabilité. Le document souligne la capacité croissante de l'état à intégrer la prestation de services de sécurité dans un cadre commun et, *in fine,* applicable de règles. De plus, les réformateurs doivent accepter la réalité d'une période provisoire indéfinie, et l'éventualité de travailler pendant cette période, en comprenant que les normes sous-tendant l'état de droit évoluent lentement et admettant que les relations entre prestataires et consommateurs de services de sécurité seront, dans un avenir prévisible, définies par les différentes configurations de légitimité et de redevabilité.

Envisager la RSS de cette façon implique également et nécessairement de repenser les rapports des intervenants extérieurs avec les systèmes de sécurité et les acteurs de la sécurité dans un contexte de réforme. En premier lieu, comme l'a fait remarquer Lisa Denney, négocier avec les prestataires non étatiques de services de sécurité est « un terrain inconfortable pour les organisations engagées dans les droits de l'homme et les principes de bonne gouvernance[42] ». L'aversion du risque et la répugnance à négocier avec des acteurs qui pourraient par ailleurs être considérés comme peu recommandables représentent par conséquent un premier obstacle majeur à surmonter afin de faciliter la compréhension des prestataires non étatique de sécurité et de commencer à développer « un spectre de partenariats et d'associations uniques » entre les systèmes étatiques et non étatiques[43] ». Dans le même ordre d'idées, les intervenants extérieurs doivent de plus en plus s'envisager comme des facilitateurs plutôt que comme des ingénieurs, afin d'aider à la mise en place des processus, des rela-

tions et des dynamiques qui permettront aux systèmes complexes de sécurité d'évoluer sur des voies constructives, longtemps après que les acteurs extérieurs seront rentrés chez eux. Erwin van Veen et Maria Derks ont en effet clairement appelé la communauté des donateurs à adopter « une approche processus de la programmation », qui combine notamment un engagement à des résultats à court terme (en particulier en soutenant les dispositions existantes qui « fonctionnent » dans un contexte donné), des cadres de résultats flexibles appuyés par des outils sophistiqués de surveillance et d'évaluation, et une compréhension approfondie des structures d'incitation auxquelles les acteurs principaux font face, et des engagements mutuels à long terme (à réaliser sur plusieurs décennies)[44].

Si la RSS est, au fond, une question de réglementation, de gestion et de contrôle du pouvoir coercitif, l'intervention extérieure doit se concentrer non plus sur l'immense (voire irréalisable) défi d'une *nouvelle répartition* du pouvoir, mais sur un cadre réglementaire large et prévisible. En définitive, l'objectif devrait être de relier les initiatives à court terme (en particulier celles qui facilitent les interactions constructives entre les différentes catégories d'acteurs de la sécurité composant les ordres de sécurité hybride) à une stratégie de longue haleine de changement systémique, basée sur l'évolution des dispositions existantes plutôt que sur la superposition d'arrangements extérieurs.

Notes

1. BARNES, Catherine, « Renegotiating the Political Settlement in War-to-Peace Transitions », document commandité par le ministère britannique du Développement international, Londres, GB : Conciliation Services, 20 mars 2009, 3, www.c-r.org/sites/default/files/Renegotiating%20the%20Political%20Settlement_200903_ENG.pdf.

2. BAKER, Bruce, « The Future is Non-State », in *The Future of Security Sector Reform*, SEDRA, Mark, dir., Waterloo, Ontario : The Centre for International Governance Innovation, 2010, pp. 208–228, www.cigionline.org/sites/default/files/the_future_of_security_sector_reform.pdf.

3. MEAGHER, Kate, « The Strength of Weak States? Non-State Security Forces and Hybrid Governance in Africa », *Development and Change* 43, no 5, 2012, pp. 1073–1101, DOI: https://doi.org/10.1111/j.1467-7660.2012.01794.x

4. MEAGHER, « *The Strength of Weak States?* », p. 1076 ; RAEYMAEKERS, Timothy, MENKHAUS, Ken, VLASSENROOT, Koen, « State and Non-State Regulation in African Protracted Crises: Governance without Government? », *Afrika Focus* 21, no 2, 2008, p. 10.

5. ETZIONI, Amitai, « Bottom-up Nation-building », *Policy Review* 158, 2009-2010, p. 54.

6. ANDERSEN, Louise, « *Security Sector Reform and the Dilemmas of Liberal Peacebuilding* », document de travail 31, Danish Institute for International Studies (DIIS), 2011, p. 12, www.diis.dk/files/media/publications/import/extra/security_sector_reform_and_the_dilemmas_of_liberal_peacebuilding_1.pdf.

7. DENNEY, Lisa, *Non-state Security and Justice in Fragile States: Lessons from Sierra Leone*, document d'information No 73, Londres, GB : Overseas Development Institute, avril 2012, www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/7640.pdf ; ALBRECHT, Pe-

ter, KYED, Helene Maria, « Introduction : Non-state and Customary Actors in Development Programs », dans *Perspectives on Involving Non-state and Customary Actors in Justice and Security Reform*, Peter Albrecht, et al., Rome : IDLO/DIIS, 2011, pp. 3–22.

8. MENKHAUS, « Non-State Security Providers and Political Formation in Somalia », *CSG Papers* No 5, Waterloo : Centre for Security Governance, avril 2016, p. 6, http://secgovcentre.org/wp-content/uploads/2016/11/NSSPs_in_Somalia_April2016.pdf.

9. CAROTHERS, Thomas, « The Rule of Law Revival », *Foreign Affairs* 77, no 2, 1998, pp. 95-106, DOI:10.2307/20048791.

10. HURWITZ, Agnès, « Civil War and the Rule of Law: Toward Security, Development, and Human Rights », dans *Civil War and the Rule of Law: Security, Development, Human Rights*, HURWITZ, HUANG, Reyko, dir., Boulder, CO : Lynne Rienner, 2008, p. 2.

11. STROMSETH, Jane, WIPPMAN, David, BROOKS, Rosa, *Can Might Make Rights? Building the Rule of Law after Military Interventions*, New York : Cambridge University Press, 2006, p. 75, DOI: https://doi.org/10.1017/CBO9780511803086.

12. BERG, Louis-Alexandre, « Guns, Laws and Politics: The Political Foundations of Rule of Law and Security Sector Reform », *Hague Journal on the Rule of Law* 4, no 4, 2012, pp. 4–30, DOI: https://doi.org/10.1017/S1876404512000024.

13. OTTAWAY, Marina, « Promoting Democracy after Conflict: The Difficult Choices », *International Studies Perspectives* 4, no 3, 2003, pp. 314–322, DOI: https://doi.org/10.1111/1528-3577.403007.

14. CAROTHERS, « *The Rule of Law Revival* », p. 96.

15. *Id*.

16. GOWLLAND-DEBBAS, Vera, PERGANTIS, Vassillis, « Rule of Law », dans *Post-Conflict Peacebuilding: A Lexicon*, Vincent Chetail, dir., New York: Oxford University Press, 2009, p. 321.

17. DENNEY, *Non-state Security and Justice in Fragile States*, p. 1.

18. CAROTHERS, « The Rule of Law Revival », p. 96.

19. STROMSETH, WIPPMAN, BROOKS, *Can Might Make Rights?*, p. 77.

20. MENKHAUS, « *Non-State Security Providers and Political Formation in Somalia* ».

21. DENNEY, *Non-state Security and Justice in Fragile States*, p. 1.

22. Organisation de coopération et de développement économiques (OCDE), *Supporting Statebuilding in Situations of Conflict and Fragility: Policy Guidance*, Paris, France : OECD, 2011, http://dx.doi.org/10.1787/9789264074989-en.

23. BAKER, Bruce, « *Policing for Conflict Zones: What Have Local Policing Groups Taught Us?* », (document présenté dans le cadre du projet « Non-State Security Providers and Political Formation in Conflict-Affected States », Waterloo, Canada, Centre for Security Governance [CSG], mai 2016).

24. LAWRENCE, Michael, « Towards a Non-State Security Sector Reform Strategy », *SSR Issue Papers* No 8, Waterloo : Centre for International Governance Innovation, 2012, p. 15, www.cigionline.org/publications/2012/5/towards-non-state-security-sector-reform-strategy.

25. BAKER, Bruce, SCHEYE, Eric, « Multi-Layered Justice and Security Delivery in Post-Conflict and Fragile States », *Conflict, Security and Development* 7, no 4, 2007, p. 517, DOI: https://doi.org/10.1080/14678800701692944.

26. MEAGHER, « *The Strength of Weak States?* », pp. 1080–1181.

27. LAWRENCE, « *Towards a Non-State Security Sector Reform Strategy* », p. 18.

28. BAKER, SCHEYE, « *Multi-Layered Justice and Security Delivery* », p. 519.
29. MEAGHER, « *The Strength of Weak States?* », p. 1074.
30. BAKER, SCHEYE, « *Multi-Layered Justice and Security Delivery* », p. 519.
31. LAWRENCE, « *Towards a Non-State Security Sector Reform Strategy* », p. 10.
32. MENKHAUS, « *Non-State Security Providers and Political Formation in Somalia* », pp. 38-39.
33. *Id.*, p. 38.
34. HEUPEL, Monika, « Rule of Law Promotion and Security Sector Reform: Common Principles, Common Challenges », *Hague Journal on the Rule of Law* 4, 2012, p.168, DOI : https://doi.org/10.1017/S1876404512000097
35. LAWRENCE, « *Towards a Non-State Security Sector Reform Strategy* », p. 17.
36. *Id.*, p. 22.
37. RICIGLIANO, Robert, « Networks of Effective Action: Implementing an Integrated Approach to Peacebuilding », *Security Dialogue* 34, no 4, 2003, pp. 445–462, DOI : https://doi.org/10.1177/0967010603344005.
38. DONAIS, Timothy, *Towards Vertically Integrated Peace Building: Bridging Top-down and Bottom-up Approaches*, CIGI Workshop Report, Waterloo, ON : Centre for International Governance Innovation, 2013, www.cigionline.org/sites/default/files/donais_vertical_integration_workshop_report.pdf.
39. RICIGLIANO, « *Networks of Effective Action* », p. 446.
40. VAN VEEN, Erwin, DERKS, Maria, « The Deaf, the Blind and the Politician: The Troubles of Justice and Security Interventions in Fragile States », *Hague Journal on the Rule of Law* 4, 2012, p. 85, DOI : https://doi.org/10.1017/S187640451200005X.
41. *Id.*
42. DENNEY, *Non-state Security and Justice in Fragile States*, p. 1.
43. BAKER, SCHEYE, « *Multi-Layered Justice and Security Delivery* », p. 525.
44. VAN VEEN, DERKS, « *The Deaf, the Blind and the Politician* », p. 93.

La stratégie des « Trois guerres » de la Chine ou comment atténuer les retombées du cyberespionnage

Emilio Iasiello*

D'aucuns accusent la Chine d'avoir lancé, il y a quelque temps déjà, une campagne d'espionnage informatique à l'encontre d'une série de pays, dont les États-Unis. Le pays fait, à ce titre, l'objet de vives critiques. La mauvaise presse qui découle de ces activités alimente la perception selon laquelle la « montée en puissance » de la Chine à l'échelle mondiale repose sur la volonté de ses dirigeants de se faire une place parmi les grandes puissances mondiales en volant subrepticement la propriété intellectuelle de ses concurrents, et peut-être de pouvoir ainsi rivaliser avec les États-Unis sur le terrain militaire régional et mondial. Afin de combattre cette perception, le présent article pose le postulat que la Chine a mis à profit sa stratégie des « Trois guerres » – guerre de l'information à trois volets s'articulant autour de composantes médiatiques, juridiques et psychologiques afin d'influencer la communauté internationale, et les États-Unis en particulier – dans l'objectif d'empêcher l'élaboration et la mise en œuvre de toute contre-stratégie. Le résultat lui a, jusqu'à présent, été largement favorable, et a permis à la Chine d'atteindre les jalons énoncés dans ses plans nationaux de développement, tout en échappant aux sanctions diplomatiques et économiques de la part de la communauté internationale, y compris celles imposées par les États-Unis en matière de cyber-espionnage. Le présent article examine l'activité cybernétique de la Chine, les perceptions internationales de la menace cybernétique chinoise et la façon dont sa stratégie des « Trois guerres » s'applique aux cyber-opérations. Nous formulons, sur cette base, une série de conclusions.

---

*Fort de plus de 12 ans d'expérience en tant qu'analyste stratégique en renseignement cybernétique, Emilio Iasiello collabore avec divers organismes de renseignement civils et militaires du gouvernement américain, ainsi qu'avec le secteur privé. Il a donné plusieurs exposés sur la cyber-menace lors de congrès nationaux et internationaux et a publié de nombreux articles dans des revues évaluées par des pairs.

IASIELLO, Emilio, « China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities », *Journal of Strategic Security* 9, n° 2, 2016, pp. 45-69. DOI : http://dx.doi.org/10.5038/1944-0472.9.2.1489. Accessible à l'adresse : http://scholarcommons.usf.edu/jss/vol9/iss2/4

La cyberactivité chinoise

Le général Keith Alexander, ancien directeur de l'Agence nationale de sécurité (NSA) et commandant du sous-commandement interarmées de combat en charge de la sécurité de l'information (U.S. Cyber Command), estime les pertes encourues par les États-Unis en raison des activités de cyber-espionnage à quelque 338 milliards de dollars[1]. Si ces pertes ne sont certes pas toutes dues aux efforts chinois, il reste évident que la Chine, identifiée comme le principal acteur du cyber-espionnage à l'échelle mondiale, est soupçonnée d'être à l'origine d'une bonne partie de cette activité[2]. L'ampleur de ces activités de cyber-espionnage soulève la question suivante : en dépit des avantages découlant du vol d'informations sensibles et exclusives que dénonce la communauté internationale, quel est le plan stratégique de Pékin ?

La Chine a trois objectifs principaux en matière de sécurité nationale : assurer la survie du régime, défendre la souveraineté nationale et l'intégrité territoriale et s'élever au rang de puissance régionale et internationale[3]. La position de la Chine vis-à-vis des États-Unis traduit un prudent mélange de scepticisme, de volonté de collaborer et de rivalité. Les Chinois considèrent les États-Unis comme une puissance révisionniste cherchant à réduire leur influence politique et à nuire à leurs intérêts[4]. L'une des façons de contrer la suprématie américaine consiste, pour la Chine, à s'engager dans des opérations cybernétiques dans le but de soutirer des informations de nature « diplomatique, économique et industrielle qui soutienne les programmes de défense des États-Unis[5] ». Dans ce contexte, on peut considérer que les opérations cybernétiques visent davantage à renforcer le noyau dur de la Chine qu'à réduire le pouvoir américain. Se concentrant uniquement sur les États-Unis, les cyber-espions chinois ont notamment ciblé les industries suivantes au cours des deux dernières années : l'espace[6], les infrastructures[7], l'énergie[8], l'énergie nucléaire[9], les entreprises technologiques[10], l'énergie propre[11], la biotechnologie[12] et les soins de santé[13].

Le 12e Plan quinquennal de la Chine reflète les objectifs globaux du gouvernement afin de promouvoir la croissance économique. Il s'agit d'un outil d'une importance cruciale qui permet de tracer, par cycles de cinq ans, les progrès du pays au moyen de lignes directrices, de cadres stratégiques et d'objectifs pour les décideurs à tous les niveaux de gouvernement[14]. Dans son Plan quinquennal actuel, qui couvre la période 2011-2015, la Chine a identifié sept secteurs prioritaires à développer, dans lesquels les États-Unis ont, en général, été un innovateur et un chef de file. Ces « industries stratégiques émergentes » sont censées devenir l'épine dorsale de l'économie chinoise dans les décennies à venir[15]. Ces industries sont :

- Nouvelles énergies (nucléaire, éolienne, solaire)
- Conservation de l'énergie et protection de l'environnement (objectifs de réduction de la consommation d'énergie)
- Biotechnologie (médicaments et dispositifs médicaux)

- Nouveaux matériaux (terres rares et semi-conducteurs haut de gamme)
- Nouvelles technologies de l'information (réseaux à large bande, infrastructure de sécurité Internet, convergence des réseaux)
- Fabrication d'équipements haut de gamme (équipements aérospatiaux et de télécommunications)
- Véhicules à énergie propre[16]

Une corrélation peut être facilement établie entre les types d'industries ciblées aux États-Unis au cours des deux dernières années et les industries émergentes stratégiques mises en avant par la Chine. De plus, la Chine voit la cybernétique comme un outil idéal pour atteindre ces objectifs en raison du caractère peu coûteux de la technique et de la facilité qu'elle offre en permettant d'atteindre plusieurs cibles potentielles de renseignement à la fois. En février 2007, la revue *China National Defense News* a défini la cyber-guerre comme « l'utilisation de la technologie et des méthodes en réseau à des fins de collecte d'informations dans les domaines politique, économique, technologique et militaire[17] ». Le principal avantage est que la cyber-guerre est directement liée à l'« avantage de l'information » et non à l'avantage militaire, ce qui suggère que les cyber-activités en temps de paix visent davantage à soutenir le développement de la Chine dans des domaines stratégiques et moins à établir une supériorité militaire à travers la reconnaissance d'un futur champ de bataille.

La perception de la menace cybernétique chinoise

Si certains experts estiment que les États-Unis, ainsi que la Chine et la Russie, sont engagés dans une course aux armements cybernétique[18], la Chine n'a pas encore été impliquée dans un incident portant sur la destruction de systèmes d'information ou des informations qui s'y trouvent, ni suspectée de l'avoir été. De nombreux ouvrages militaires stratégiques chinois préconisent l'utilisation de la guerre de l'information comme arme préventive avant le début des engagements militaires[19]. Toutefois, si la Chine est bel et bien à l'origine du volume des activités de cyber-espionnage qui lui sont attribuées, elle préfère tirer parti des intrusions informatiques comme moyen de collecte d'informations et d'avantages commerciaux en temps de paix plutôt que comme arme de dissuasion.

Actuellement, plusieurs pays, dont l'Allemagne, l'Australie, le Canada, l'Allemagne, l'Inde, Taiwan et le Royaume-Uni, ont publiquement accusé la Chine d'intrusion sur les réseaux de leurs secteurs public et privé[20]. De façon plus spécifique, les États-Unis sont depuis une douzaine d'années la cible principale des cyber-opérations orchestrées ou dirigées par la Chine. Alors que le gouvernement américain a maintenu une position réservée pendant la plus grande partie de cette période, en 2012, il s'est prononcé plus ouvertement sur le volume des activités de cyber-espionnage visant ses secteurs public et privé. En octobre 2011, Mike Rogers, membre du Congrès des

États-Unis et du Comité permanent de la Chambre des représentants sur le renseignement, a accusé publiquement la Chine d'avoir volé des informations sensibles :

> L'espionnage économique de la Chine a atteint un niveau intolérable et je crois que les États-Unis et nos alliés en Europe et en Asie ont le devoir de faire obstacle à Pékin et d'exiger que le pays mette un terme à cette piraterie[21].

En 2013, la société de sécurité Mandiant a publié un rapport détaillé identifiant une unité militaire chinoise impliquée dans le cyber-espionnage[22]. Jamais auparavant les preuves et analyses techniques établissant un lien entre ce type d'activités et une entité gouvernementale n'avaient été rendues publiques. Le rapport Mandiant a été un tournant décisif pour les hauts responsables du gouvernement américain, et plusieurs d'entre eux, dont le président Obama, ont évoqué publiquement la question de l'espionnage informatique chinois. Peu après la publication du rapport, en mars 2013, le conseiller à la sécurité nationale des États-Unis, Thomas Donilon, a déclaré :

> ... les entreprises expriment leur plus grande préoccupation à l'égard du vol ciblé et organisé d'informations commerciales confidentielles et de renseignements propriétaires exclusifs opéré par l'intermédiaire d'intrusions cybernétiques provenant de la Chine[23].

Au cours du même mois, le président Obama a interpellé directement le président chinois Xi Jinping au sujet de la cyber-sécurité et des futures opportunités de collaboration[24]. Cet entretien s'est suivi d'un sommet en juin au cours duquel les deux dirigeants ont discuté plus longuement de la cyber-sécurité[25]. Cependant, aucun progrès n'a été réalisé en mai 2014 lorsque le département de la Justice des États-Unis a accusé cinq officiers militaires chinois de cyber-espionnage. Ce fut la première fois que le gouvernement américain accusait publiquement des membres d'un gouvernement étranger de crimes contre des entreprises américaines[26]. D'autres rapports portant le groupe Axiom, un autre groupe chinois soupçonné d'espionnage dont les pratiques étaient réputées plus élaborées que celles décrites dans le rapport Mandiant, dressent un portrait peu reluisant de la Chine en tant que cyber-espion coupable de vols incessants d'informations sensibles[27]. Compte tenu du grand nombre de cyber-incidents indiquant un certain degré d'implication du gouvernement chinois, Pékin tente de maintenir son image de « montée en puissance pacifique » au milieu de la bronca grandissante de la communauté internationale, les États-Unis en tête, qui menacent d'imposer des cyber-sanctions contre les auteurs d'activités d'espionnage commercial.

La stratégie des « Trois guerres »

Il semble contre-productif pour un pays si soucieux de son « image » de s'engager dans des activités aussi flagrantes, aussi agressives et aussi nuisibles à sa réputation. Le *guanxi* et le *mianzi* sont deux concepts essentiels de la culture chinoise. Le premier, le *guanxi*, a été défini comme le partage des faveurs entre les individus, les

connexions et les relations et la capacité à exercer une influence. Le second, le *mianzi*, signifie la « face », comme dans les expressions sauver la face, perdre la face, voire montrer son (vrai) visage[28]. Alors, pourquoi donc un pays imprégné de cet état d'esprit risquerait-il volontairement d'écorner son image, surtout à un moment où le pays est considéré comme une puissance économique mondiale en pleine expansion ? La mise en œuvre d'opérations non cinétiques, non violentes, mais néanmoins offensives est la meilleure solution, en temps de paix, pour la stratégie chinoise d'influencer les processus cognitifs des dirigeants et de la population d'un pays, ou ce que Sun Tzu décrit comme « maîtriser l'ennemi sans se battre[29] ». En 2003, le Comité central du Parti communiste chinois et la Commission militaire centrale ont approuvé le concept des « Trois guerres », un outil de guerre d'information non militaire destiné à être utilisé par l'Armée populaire de libération avant et pendant les hostilités[30]. À elles trois, ces guerres permettent à la Chine d'entrer dans n'importe quel conflit, que ce soit en temps de paix ou de guerre, en bénéficiant d'un avantage politique qui pourra utilisé pour influencer l'opinion publique ou internationale[31]. Ces trois guerres sont :

- *Guerre psychologique* — La guerre psychologique affaiblit la capacité d'un ennemi à mener des opérations de combat par l'intermédiaire d'opérations visant à dissuader, déstabiliser et démoraliser le personnel militaire ennemi et à soutenir les populations civiles[32].
- *Guerre de l'opinion publique/médiatique* — Influence l'opinion publique nationale et internationale pour obtenir le soutien des actions militaires de la Chine et dissuader un adversaire de mener des actions contraires aux intérêts de la Chine[33].
- *Guerre juridique* — Utilise le droit international et national pour revendiquer une position de supériorité juridique ou faire valoir les intérêts chinois. Elle peut être utilisée pour entraver la liberté opérationnelle d'un adversaire et agencer l'espace opérationnel. La guerre juridique a également pour but d'obtenir le soutien de la communauté internationale et de gérer les répercussions politiques possibles des actions militaires de la Chine[34].

La guerre médiatique intègre le mécanisme des messages à transmettre, tandis que la guerre juridique justifie la raison des actions menées. La guerre psychologique apporte les nuances nécessaires en tirant parti de la capacité de diffusion des médias et des mécanismes juridiques plus formels pour démontrer le bien-fondé des activités auprès des publics nationaux et internationaux. Étant donné que chacun de ces types de guerre repose sur le ciblage et l'influence d'un public cible spécifique, il est facile de comprendre pourquoi les analyses chinoises associent presque toujours ces trois types de « combat »[35].

Guerre de l'opinion publique/médiatique

La guerre de l'opinion publique renvoie à l'utilisation de divers canaux d'information, y compris Internet, la télévision, la radio, les journaux, les journaux, les films et d'autres formes de médias, conformément à un plan d'ensemble et à des objectifs définis. Elle vise à transmettre des informations minutieusement sélectionnées à un public cible[36]. Les objectifs sont de préserver le moral des troupes, d'obtenir l'appui du public de la population nationale et à l'étranger, d'affaiblir la volonté de l'ennemi de combattre et de modifier son appréciation de la situation. La guerre défensive de l'opinion publique est utilisée pour neutraliser les effets possibles sur la population chinoise[37]. Compte tenu des nombreuses allégations de piratage informatique portées contre la Chine, la guerre défensive de l'opinion publique est un contrepoids naturel. Selon Cheng, quatre thèmes sont inhérents aux écrits chinois sur l'opinion publique[38] :

- *Suivre une orientation descendante (top-down)* — La haute direction dictera les mesures à prendre en fonction des objectifs stratégiques.
- *Mettre l'accent sur la préemption* — Les analyses chinoises de la guerre de l'opinion publique soulignent que « le premier à se faire entendre s'empare du peuple, le premier à s'engager assoie sa domination (*xian sheng duoren, xianru weizhu*).
- *Souplesse et réactivité face à l'évolution des conditions* — Utilisation de différentes activités de propagande selon le public visé. « Il convient de faire la distinction entre les éléments les plus têtus et le reste de la population de façon générale ».
- *Exploiter toutes les ressources disponibles* — Les ressources civiles et commerciales telles que les agences de presse, les installations de radiodiffusion, les utilisateurs d'Internet, etc. sont considérées comme une ressource inestimable pour faire passer le message de la Chine auprès des publics nationaux et internationaux.

Les premières critiques à l'égard des intrusions soutenues par Pékin ont fait surface dans l'opinion publique dès 2005, lorsqu'il a été révélé que des intrusions présumées du gouvernement chinois, appelées « *Titan Rain* », visaient depuis 2003 des acteurs des secteurs public et privé américains[39]. Depuis lors, de nombreux gouvernements étrangers se sont exprimés publiquement pour dénoncer les activités intrusives du gouvernement chinois ou de ses agents[40]. De plus, les entités du gouvernement américain soupçonnent depuis longtemps les sociétés de télécommunications chinoises Huawei et ZTE d'être des instruments de l'état, et des intermédiaires utilisés par le gouvernement chinois pour collecter des renseignements[41]. Ce débat s'est invité dans les plus hautes sphères de l'état, comme en 2013 lors des rencontres entre le président chinois Xi Jinping et le président américain Barack Obama[42]. En 2014, le secrétaire d'état à la Défense Charles Hagel a révélé à la Chine la structure et les capacités des cyber-forces américaines dans un effort de transparence militaire[43].

Applications au cyberespace de la guerre de l'opinion publique et médiatique de la Chine

La réponse chinoise a évolué au cours de cette période, où elle a été présentée comme une présence cybernétique ennemie. La Chine a généralement réagi à ces accusations en adoptant une attitude défensive, niant les allégations et demandant des compléments d'informations dans le but d'aider à retrouver les auteurs. Ainsi, des déclarations officielles de haut niveau émanant du ministère chinois de la Défense[44], du ministère des Affaires étrangères[45] et de son Premier ministre[46] se sont inscrites dans la ligne de conduite du parti, soutenant que la Chine n'est pas derrière les attaques, que le pays était une victime et non l'auteur de ces activités cybercriminelles, et que les lois chinoises considèrent, sans restriction, le piratage informatique comme un acte comme illégal condamnable[47].

La Chine a toutefois adopté une position plus affirmée lorsque l'ancien entrepreneur de la NSA, Edward Snowden, a publié des documents présumés hautement confidentiels exposant les activités de surveillance des États-Unis à l'échelle mondiale. Au lieu d'essayer de détourner les accusations, la Chine pointe maintenant le gouvernement américain du doigt. Pékin a même exigé des explications aux États-Unis sur de possibles activités d'espionnage de la compagnie chinoise Huawei par la NSA[48]. Un comble compte tenu des soupçons du gouvernement américain à l'égard des activités d'espionnage commises par la société Huawei au nom du gouvernement chinois. Notons toutefois que la véracité des allégations américaines n'a pas été démontrée par l'enquête diligentée pour le compte des États-Unis par Mike Rogers, membre du Congrès et du Comité permanent de la Chambre des représentants sur le renseignement[49]. En dépit de la persistance des sceptiques, la Maison-Blanche a procédé à sa propre enquête de sécurité de Huawei en octobre 2012 et n'a trouvé aucune preuve démontrant que Huawei espionnait les États-Unis au nom du gouvernement chinois[50]. En mars 2014, l'équipe nationale chinoise d'intervention d'urgence informatique a identifié les États-Unis comme la principale source d'intrusion contre ses ordinateurs[51].

Les efforts déployés par les États-Unis pour gérer leur image publique n'ont pas été à la hauteur des attentes, les alliés et les adversaires ayant exprimé leur indignation face au scandale dévoilé par Snowden[52]. La nuance subtile sur laquelle le gouvernement américain fonde sa défense, à savoir que le pays mène ces activités pour assurer la sécurité nationale et non pour procurer un avantage concurrentiel aux sociétés américaines, semble éculée, surtout après avoir été pris la main dans le sac cybernétique. Plusieurs accusations ont été portées à la suite de fuites de documents indiquant que la NSA espionnait des entités de sécurité non nationales, dont la plus grande compagnie pétrolière brésilienne[53], le commissaire de l'Union européenne en charge d'une enquête sur les sociétés Google, Microsoft et Intel[54], le Fonds monétaire international

et la Banque mondiale[55]. Même sur le sol américain, les groupes d'intérêts publics et spéciaux qui défendent les libertés civiles ont condamné les activités de la NSA[56].

Alors que les États-Unis semblaient avoir l'avantage et le soutien de la communauté internationale à l'égard des soupçons d'espionnage cybernétique de la Chine, le pays a réussi à redorer son blason. Elle continue de se présenter comme une cyber-victime et un partenaire coopératif en matière de cyber-sécurité. En 2014, la Chine a exprimé son souhait d'une coopération cybernétique avec les États-Unis[57] et, depuis avril 2014, le Pentagone a engagé des échanges militaires avec la Chine dans un esprit de transparence militaire[58].

Malgré les allégations persistantes de malveillances cybernétiques à son égard, la Chine est donc parvenue à améliorer son image, au détriment des cyber-activités secrètes américaines. Peut-être en réaction à se revirement, le département de la Justice des États-Unis a inculpé pour cyber-espionnage en mai 2014 cinq pirates informatiques militaires chinois[59]. Bien que cette décision historique visât à démontrer l'implication directe du gouvernement chinois dans le cyber-espionnage, elle n'a pas davantage incriminé la Chine aux yeux du grand public. Après tout, de nombreuses organisations publiques et privées partent généralement du principe que le gouvernement chinois s'approprie des propriétés intellectuelles et collecte des informations sensibles. À l'inverse, la sortie massive de documents hautement sensibles révélant le rôle du gouvernement américain dans des activités similaires (contre les gouvernements alliés et ennemis) a été perçue comme une injustice bien plus grande et comme un comportement indigne de la part d'un gouvernement prônant les droits de l'homme et les libertés individuelles.

Guerre juridique

La guerre juridique est l'un des instruments clés de la guerre psychologique et de la guerre de l'opinion publique[60]. Souvent, elle est utilisée conjointement à l'un ou aux deux autres types de guerre : elle est plus efficace en association avec une autre. De cette façon, la guerre juridique fournit la base qui renforce la guerre de l'opinion publique et la guerre psychologique[61]. Par définition, la guerre juridique est destinée à justifier une ligne de conduite. Deux influences alimentent la guerre juridique menée par la Chine :

- *Position de la Chine sur le rôle et la primauté du droit* — Des considérations historiques et culturelles éclairent la perception du gouvernement chinois en matière de guerre juridique. Le confucianisme et les influences légalistes faisaient partie intégrante de la Chine impérialiste, mais au fur et à mesure du mandat de Mao et de l'évolution du gouvernement, les perspectives marxistes ont préconisé que « la loi devrait servir d'instrument idéologique à la poli-

tique[62] ». Aujourd'hui, l'accent est mis sur le droit commercial et le droit des contrats, tandis que le droit pénal reste en retrait[63].

- *Perception de la Chine de la guerre juridique en Occident* — La Chine tient compte de cette importance aux yeux des Occidentaux lorsqu'elle justifie ses actions par le droit. Lors de la première guerre du Golfe, les États-Unis ont obtenu l'autorisation de l'ONU de recourir à des sanctions et à la force en Irak, tandis qu'au Kosovo, ils ont soutenu que leurs actions étaient « conformes à la loi » parce qu'elles étaient prises sous les auspices de l'OTAN[64]. Cette capacité à utiliser la primauté du droit ou ses perceptions juridiques pour justifier ses actions est un puissant outil de la pensée chinoise.

Applications au cyberespace de la guerre juridique de la Chine

En tant que mode d'influence, la guerre juridique est généralement utilisée avant le déclenchement d'un conflit physique, et ne survient que dans le contexte d'une guerre réelle. Toutefois, depuis que les projecteurs internationaux se sont tournés vers les activités de cyber-espionnage et que la Chine a été accusée d'être l'auteur de vols de propriété intellectuelle, il semble que les Chinois se servent peut-être des principes de la guerre juridique pour défendre leurs intérêts stratégiques. Les événements suivants se sont produits après que plusieurs gouvernements ont publiquement blâmé la Chine pour avoir piraté leurs réseaux et volé des données :

- *2014 — Les États-Unis projettent d'abandonner le contrôle de l'Internet* — En décembre 2012, la Chine et la Russie ont obtenu un soutien international pour que tous les états jouissent de droits égaux sur la gouvernance de l'Internet. L'accord a revu les règles de télécommunications de l'ONU, dont la création remontait à 24 ans[65]. S'il n'est pas contraignant, 89 pays l'ont signé, 55 se réservant le droit de le signer à une date ultérieure[66], ce qui témoigne d'un large soutien. Cette initiative a poursuivi les mesures nécessaires pour que l'Union internationale des télécommunications (UIT) joue un rôle actif dans le modèle multipartite de l'Internet[67]. Ces efforts, conjugués à la fuite de documents sensibles concernant la prétendue surveillance mondiale de la National Security Agency, ont exercé une pression considérable sur les États-Unis pour qu'ils renoncent à soutenir l'Internet Corporation for Assigned Names and Numbers (ICANN) et son influence sur le contrôle du trafic Internet[68]. L'obtention d'un soutien international et l'utilisation de l'UIT en tant qu'organe autorisé ont conféré à ces efforts une évidente légitimité. En janvier 2016, les responsables américains ont réitéré leur volonté de renoncer au contrôle fédéral sur la gouvernance d'Internet d'ici septembre[69].
- *2011/2015 — Lettres de la Chine et de la Russie aux Nations Unies* — Comme il n'existe pas de lois internationales officielles ni même de définitions communes

régissant les activités cybernétiques, la Chine a été un fervent défenseur de la mise sur pied de bonnes pratiques pour les états nations. En 2011, la Chine s'est associée à la Russie, au Tadjikistan et à l'Ouzbékistan pour présenter un code de bonne conduite international sur la sécurité de l'information à l'ONU[70], qui a été mis à jour en janvier 2015[71]. En substance, le cœur des deux propositions mettait l'accent sur l'identification des droits et des responsabilités des états dans l'espace de l'information, ainsi que sur la promotion de comportements constructifs et responsables dans le but de renforcer leur coopération en matière de lutte contre les menaces et de défis communs à relever. Bien qu'au moment de la rédaction du présent article, la proposition soit toujours en cours d'examen par les états membres, la Chine a joué un rôle de premier plan à l'échelle internationale en essayant d'établir des normes de bonne conduite pour les états nations en faisant appel à un organisme international pour légitimer ses efforts.

- *2009 — Mise à jour de la législation chinoise sur la cybercriminalité* — La Chine soutient publiquement que le piratage informatique est contraire aux lois chinoises[72]. En 2009, la Chine a étendu les peines infligées aux personnes reconnues coupables d'activités cybercriminelles[73]. Lorsqu'elle est accusée de parrainage de piratage, la Chine est prompte à invoquer ses propres lois pour justifier légalement pourquoi elle ne se livre pas à cette activité[74].

La Chine fait appel à des organisations internationales comme l'ONU, dont l'autorisation est étayée par des arguments juridiques, pour légitimer ses efforts. Cette approche sert deux objectifs stratégiques majeurs : 1) Elle tempère l'image négative de la Chine en tant qu'état pirate en démontrant qu'elle cherche à travailler collectivement et dans le cadre des règles définies par les organisations internationales établies, et 2) elle aide la Chine à mettre en œuvre des moyens asymétriques non cinétiques pour poursuivre ses objectifs politiques et économiques, en évitant le besoin d'utiliser la force ou l'influence militaire, réduisant ainsi le risque d'escalade potentielle sur une question donnée.

La guerre psychologique de la Chine

La guerre psychologique est profondément enracinée dans la stratégie chinoise. Par exemple, « les positions chinoises affirment qu'en temps de paix, les opérations psychologiques cherchent à révéler et à exploiter les divisions de l'establishment politique ou de l'alliance interne de l'ennemi et à remettre en cause les valeurs de l'ennemi[75] ». Elle vise un degré de précision élevé dans le ciblage des points critiques afin d'obtenir des effets non linéaires.

Applications au cyberespace de la guerre psychologique de la Chine

Selon les spécialistes chinois, la guerre psychologique fait partie intégrante de la guerre de l'information[76]. Toutefois, il est plus difficile de définir la guerre de l'information dans un contexte chinois, car il n'existe pas de doctrine publiée sur la guerre de l'information et nous ne disposons que d'écrits chinois pour comprendre cette discipline complexe. Les premiers écrits sur le sujet ont été largement empruntés aux doctrines en vigueur aux États-Unis, en Russie, en France et en Allemagne[77]. Au fil du temps, la pensée chinoise en matière de guerre de l'information s'est développée, notamment à l'égard du concept de « domination de l'information », qui, selon James Mulvenon, cyber-expert chinois, est le principal objectif de la stratégie chinoise de guerre de l'information[78]. La domination de l'information a deux objectifs principaux : l'infrastructure de l'information physique et les données qui l'ont traversée et, de façon peut-être encore plus importante, les agents humains qui interagissent avec ces données, en particulier ceux qui prennent des décisions[79].

Selon les écrits chinois, il y a cinq grandes tâches associées à la guerre psychologique[80]. Compte tenu de la participation de la Chine à l'activité d'intrusion mondiale, ces composantes peuvent être appliquées à l'environnement actuel de la manière suivante :

1. *Souligner la légitimité de son propre camp* — La Chine est très soucieuse de son image publique, ce qui incite à s'interroger sur son ambivalence envers la publicité négative entourant ses activités de piratage. Toutes les tentatives visant « à blâmer et à faire honte » à la Chine se sont soldées par un échec retentissant, qui peut être attribué au fait que la Chine a établi et maintenu la même position officielle, quel que soit le gouvernement qui la pointe du doigt. Elle pare généralement ce type d'argument en réfutant systématiquement les allégations de piratage et en soulignant immédiatement qu'elle est elle-même victime du piratage[81]. Par ailleurs, comme nous l'avons déjà mentionné, Pékin n'hésite pas à rappeler que le piratage informatique est illégal en Chine, essayant ainsi de montrer qu'en tant que pays, elle mène aussi des actions par voie légale visant à mettre fin aux activités malveillantes dans le cyberespace[82]. Enfin, la Chine, en partenariat avec la Russie, le Tadjikistan et l'Ouzbékistan, a proposé aux Nations Unies un code de bonne conduite dans le cyberespace pour les états nations[83], qu'elle a mis à jour en février 2015 après avoir reçu la contribution des états membres[84]. Deux objectifs importants ont ainsi été atteints :
    i) Cela a montré que la Chine a été proactive dans sa tentative d'établir un ensemble international de normes de bonne conduite pour les états nations dans le cyberespace ; et
    ii) Cela a démontré la volonté de la Chine de collaborer avec les autres sur un pied d'égalité. La proposition soumise à l'ONU a également mis en exergue la volonté de la Chine d'obtenir un consensus au sein

de la communauté internationale. Pris collectivement, ces efforts peuvent être interprétés comme une tentative d'atténuation de la presse négative dont la Chine a fait l'objet en se présentant comme une nation responsable et coopérative en matière de cyber-sécurité. Ce désir de collaborer avec d'autres gouvernements sur ces questions a peut-être incité les États-Unis, en juin 2015, à accepter de négocier avec la Chine un « code de bonne conduite » dans le cyberespace[85].

2. *Exploiter ses avantages* — En 2014, la Chine est devenue la plus grande économie du monde. Son produit intérieur brut a connu une croissance exponentielle de 2003 à 2013, atteignant en moyenne annuelle plus de dix pour cent[86]. Bien que les États-Unis aient empêché les entreprises chinoises de s'implanter sur les marchés américains, la Chine ne s'est pas privée de conquérir d'autres marchés où les États-Unis jouissaient historiquement d'un avantage commercial. Récemment, la Chine a dépassé les États-Unis en devenant le premier partenaire commercial de l'Afrique et du Brésil[87]. Ce changement des rapports de force s'est traduit par des avantages économiques certains, qui n'ont donc en rien subi l'influence des allégations de piratage dont la Chine a fait l'objet. Ces pays ne se soucient tout simplement pas de la menace, estimant que l'activité économique et le développement accéléré de leurs infrastructures l'emportent sur toute conséquence potentielle. Le Brésil accueille de plus en plus de clients privés chinois et ces derniers jouent un rôle majeur dans la diversification de la coopération économique bilatérale[88]. En Afrique, la Chine est le premier fournisseur d'équipements de télécommunications[89]. Les accusations adressées à la société chinoise de télécommunications Huawei constituent un parfait exemple de la façon dont la Chine exploite ses points forts. Malgré les soupçons, exprimés en grande partie par le gouvernement américain, selon lesquels Huawei pourrait agir en tant qu'agent du gouvernement chinois, l'étude menée par la Chambre des représentants n'a fourni aucune preuve attestant d'une quelconque activité illicite d'espionnage. En outre, l'entreprise est « le deuxième plus grand fournisseur de télécommunications au monde, avec des produits et des solutions déployés dans plus de 140 pays, ce qui indique qu'un grand nombre de pays ne sont pas aussi préoccupés que ne semblent l'être les États-Unis par la menace que Huawei pose en matière de renseignement[90]. » Même les alliés américains, l'Australie et le Royaume-Uni, ne semblent pas s'inquiéter outre mesure. Le Conseil consultatif de Huawei au Royaume-Uni – une entité composée à la fois de membres du personnel du Quartier général des communications du gouvernement (GCHQ), de fonctionnaires, d'acteurs du secteur et de membre du personnel de Huawei – a conclu après un audit que les activités commerciales de Huawei au Royaume-Uni ne constituaient pas une menace de sécurité nationale[91]. En 2013, Huawei a soutenu la création d'un

centre de cyber-sécurité en Australie pour tester les systèmes d'identification des infrastructures critiques[92].

3. *Miner l'opposition* — Plusieurs articles ont été écrits sur la cyber-menace de la Chine par des experts civils et gouvernementaux, régionaux, culturels et fonctionnels, en plus des médias internationaux et des chaînes d'information de la presse écrite traitant du sujet. Dans chaque cas, deux messages retentissants sont transmis : 1) La menace cybernétique chinoise est massive et omniprésente, représentant le plus important transfert de richesses de l'histoire de l'humanité[93]. 2) La Chine cherche à accéder à des réseaux informatiques non seulement pour voler des informations sensibles, mais aussi pour asseoir sa « domination de l'information[94] ». Qu'elle soit sophistiquée, rudimentaire ou quelque part entre ces deux pôles, l'activité d'espionnage de la Chine a été constante et persistante. Même le terme « menace persistante avancée », qui lui aurait été attribué par l'U. S. Air Force en 2006 pour pouvoir en discuter avec des membres du personnel non tenu aux règles de confidentialité[95], décrit l'adversaire comme compétent, implacable et, compte tenu de son manque de couverture, intrépide. Le fait que les cyber-opérateurs chinois présumés n'aient subi que peu de conséquences de leurs actions renforce l'idée qu'ils ne peuvent pas être battus ou, à tout le moins, que leur activité effrontée ne peut être endiguée. Comme l'a dit Richard Clarke, « chaque grande entreprise aux États-Unis a déjà fait l'objet d'une intrusion chinoise[96] ». Venant d'un homme considéré comme le premier tsar cybernétique du gouvernement américain, de tels propos font passer la Chine comme un adversaire pratiquement imbattable.
4. *Encourager la dissension dans le camp de l'ennemi* — Cette tâche consiste à perturber les processus cognitifs des décideurs politiques et des décideurs, ce qui entrave leur capacité à élaborer un plan d'action. La théorie suggère que la meilleure stratégie est d'attaquer l'esprit de l'ennemi, le laissant incapable de planifier[97]. Compte tenu de l'historique des décideurs politiques américains de ne pas être en conformité avec les questions cybernétiques, cette stratégie en fait une cible de premier choix. Une chose est certaine : depuis l'apparition en 2003 des premiers soupçons d'espionnage[98], aucun plan d'action concret n'a été établi avant la mise sur pied par les États-Unis de sanctions cybernétiques ; un effort visant à décourager toutes les activités cybernétiques de façon générale, et en particulier celles qui seraient menées ou approuvées par la Chine[99]. Auparavant, les organismes apportaient leur appui à diverses mesures. Il y avait ainsi les partisans de la « cyber-défense active », comme le Cyber Command des États-Unis[100] et la Defense Advanced Research Projects Agency[101]. Il s'agit essentiellement d'un moyen de dissuasion. D'autres, cependant, à l'image de Mike Rogers, membre du Congrès, étaient davantage en faveur de la mise en place préalable d'une ligne de défense solide et viable[102]. D'autres encore,

comme le Government Accountability Office (GAO), ont dénoncé l'absence de rôles et de responsabilités clairement définis au sein des organismes fédéraux, indiquant qu'il s'agissait d'un obstacle sérieux à toute politique de cybersécurité efficace[103]. L'incapacité persistante à mettre en place une stratégie nationale solide en matière de cyber-sécurité empêche le gouvernement des États-Unis d'adopter une approche unifiée et cohérente, qui implique toutes les parties prenantes et où chacun comprend le rôle qui lui est attribué dans le processus. Même le décret de février 2013 sur l'amélioration de la cybersécurité des infrastructures critiques n'a pas pu rassembler le soutien nécessaire. Bien qu'il s'agisse d'une mesure positive, ce décret n'a pas permis d'instaurer des changements significatifs, obligeant l'état à ne compter que sur le bon vouloir des entreprises. Bien qu'il n'ait pas mentionné le décret de février, le GAO, dans un rapport publié en mars, a quand même fait état de la nécessité d'une stratégie nationale intégrée en matière de cyber-sécurité, avec des jalons, des mesures de rendement et un contrôle du Congrès[104]. Que ce soit intentionnellement ou non, les campagnes de cyber-espionnage de la Chine ont profité du climat d'indécision qui régnait au sein du gouvernement américain avant l'accord conclu en 2015 entre les deux gouvernements.

5. *Instaurer des défenses psychologiques* — La Chine a également recours à d'attaques psychologiques afin de démontrer l'inefficacité des efforts de ses adversaires[105]. Le pays a toujours maintenu sa position politique en affirmant qu'elle ne se livrait pas au cyber-espionnage. Même lorsqu'il a été interpellé directement au sujet des activités d'espionnage de son pays, le président chinois Xi Jinping a détourné l'accusation en évoquant la mauvaise sécurité du réseau. Ainsi, lorsque le programme de surveillance de la NSA a été dévoilé, la Chine a immédiatement saisi l'occasion de pointer le gouvernement américain du doigt[106]. Même le géant chinois des télécommunications, Huawei, pourtant tant critiqué, en a profité pour condamner l'espionnage de la NSA et promouvoir un dialogue mondial sur la cyber-sécurité[107].

En considérant ces cinq composantes de la guerre psychologique, on ne peut que conclure que la Chine est une force cybernétique dominante. En niant les accusations qui lui sont adressées, le pays s'appuie sur cette image sans devoir le dire publiquement ou divulguer dans la presse son implication dans un événement cybernétique majeur. En définitive, contrairement aux États-Unis, la Chine n'a pas éprouvé le désir ou la nécessité de renforcer son image en tant qu'acteur dominant du cyberespace par le biais d'annonces publiques ou de stratégies nationales. De son côté, Pékin a profité de l'attitude des autres pays spéculant sur ses capacités et sa force pour concentrer ses efforts sur l'amélioration de son image, tout en maintenant ses activités d'espionnage pour servir ses intérêts nationaux.

Éviter les cyber-sanctions américaines

Bien que l'activité chinoise de cyber-espionnage jouisse d'une relative liberté depuis un certain temps déjà, la visite d'état de 2015 a fait comprendre à la Chine que les États-Unis ne toléreraient pas le cyber-espionnage à des fins commerciales. Afin d'éviter des sanctions, Pékin est parvenu à un accord quelques jours avant la visite officielle du Président Xi aux États-Unis, dans lequel les deux parties ont convenu qu'« aucun des gouvernements de ces deux pays ne mènera ou soutiendra sciemment le vol cybernétique de propriété intellectuelle, en ce compris les secrets de fabrication et toute information commerciale jugée confidentielle, dans le but de procurer des avantages concurrentiels aux entreprises ou aux secteurs de leur pays respectif[108] ». À la suite de cet accord, la Chine a arrêté plusieurs pirates informatiques identifiés par les États-Unis[109], démontrant sa détermination à mettre un terme aux pratiques des criminels du cyberespace, même s'il s'agit de ses propres citoyens. Alors que les opinions divergent sur les véritables motifs de Pékin, la mesure n'est pas sans précédent. Ainsi, en 2010, selon un témoignage d'un fonctionnaire de la NASA au Congrès, les autorités chinoises ont arrêté un ressortissant chinois pour le piratage informatique de sept systèmes de la NASA (National Aeronautics and Space Administration)[110].

Alors que Washington attend de voir si Pékin poursuivra réellement ces pirates informatiques, nous retiendrons la volonté de la Chine de démontrer ses dispositions à travailler avec les États-Unis — et peut-être aussi, par extension, avec d'autres gouvernements — sur des questions cybernétiques similaires, ce qui n'avait pas été fait auparavant. La possibilité de voir des sanctions imposées reste cependant d'actualité si les soupçons de piratage informatique commandité par Pékin contre les intérêts commerciaux des États-Unis se confirment. Dans le cas contraire, la Chine en ressortira gagnante, en voyant sa réputation réhabilitée. Conformément aux principes de la guerre juridique et médiatique énoncés *supra*, l'assurance donnée par la Chine de « s'opposer aux cyber-attaques et à l'espionnage et de lutter contre les formes de piratage par toute voie de droit[111] », associée à des exemples publics de collaboration avec les parties prenantes, peut progressivement apaiser les craintes des opposants quant à la menace que représente le pays et dépeindre la Chine comme un partenaire coopératif plutôt que comme un ennemi.

Ajoutons encore que l'instauration d'une coopération accrue en matière de cyber-sécurité avec les gouvernements régionaux renforcera le message de la Chine, qui souhaite un Internet stable, à l'abri des activités criminelles et terroristes. La Chine s'est montrée active en la matière, en s'engageant dans des discussions sur la cyber-sécurité avec le Japon[112], la Malaisie[113] et la Corée du Sud[114], ainsi que dans une série de pactes de non-agression cybernétique menant à l'accord du G20 de novembre 2015[115]. On peut s'attendre à ce que la Chine poursuive dans cette logique dans le cadre de réunions bilatérales indépendantes ou par l'intermédiaire d'organisations internationales comme l'Organisation de Shanghai pour la coopération.

Conclusion

Bien qu'accusée de mener des campagnes de cyber-espionnage de longue date et substantielles contre les États-Unis et plusieurs autres pays, la Chine a échappé à toute répercussion punitive ou économique importante. La stratégie des « Trois guerres » de la Chine, une logique de guerre de l'information en trois volets, conçue pour influencer la communauté internationale, a joué un rôle majeur dans la prévention de toute réaction dissuasive importante, tout en permettant à la Chine de se présenter comme un partenaire fiable dans le cyberespace. La Chine a cherché à influencer la perception du grand public quant à la menace croissante que le pays représente en niant les accusations, tout en tirant parti des fuites de Snowden sur les activités de surveillance américaines à l'échelle mondiale pour ternir l'image des États-Unis. Parallèlement, la Chine a eu recours à des mécanismes juridiques visant à se positionner en tant que partenaire de confiance en matière de cyber-sécurité. Le soutien témoigné envers le droit dont jouit chaque état de participer à la gouvernance de l'Internet a gagné suffisamment d'influence que pour encourager les États-Unis à renoncer à leur rôle de chef de file. Le fait de fournir aux Nations Unies un « code de bonne conduite » a aussi démontré la volonté de la Chine de faire valoir les intérêts de la communauté mondiale afin d'assurer la stabilité du cyberespace dans tous les états. La révision de sa législation sur la cybercriminalité témoigne de l'engagement de Pékin à sanctionner les pirates informatiques. Cette impression a été renforcée par l'arrestation, en 2015, de pirates présumés à la demande des États-Unis[116]. Enfin, le recours à des opérations psychologiques (PSYOPS) a permis à la Chine de se présenter comme une partie prenante respectueuse de la loi dans le cyberespace, tout en profitant discrètement des écrits l'identifiant comme une puissance cybernétique majeure. Plus les experts mettent le doigt sur la puissance des cyber-capacités chinoises, plus la Chine est perçue comme un pays influent, sans même que Pékin n'ait à intervenir.

La confluence de ces trois stratégies a ainsi empêché l'Occident, pendant une très longue période, de dissuader la Chine d'exercer ses activités de cyber-espionnage présumées. La Chine a clairement tiré parti de cette période de flottement prolongée. Au moment où les États-Unis ont envisagé la possibilité d'imposer des sanctions à la Chine, Pékin a profité de sa rencontre avec des pays comme le Japon et la Corée du Sud[117]. Elle a aussi exploité une série de « pactes de non-agression cybernétique » conclus entre la Chine et la Russie[118], le Royaume-Uni[119] et les États-Unis[120], dans un effort qui a abouti à l'accord historique de novembre 2015, par lequel les membres du G20 ont convenu de ne pas exercer d'activités d'espionnage électronique à des fins commerciales à l'encontre de leurs partenaires[121].

La Chine a accompli ce tour de force tout en devenant, dans le même temps, la plus grande économie du monde, et en se positionnant comme chef de file régional lors des efforts menés en faveur de la mise en place d'une Route de la soie maritime

(un réseau de ports, de projets et de zones économiques spéciales interconnecté en Asie du Sud-Est et dans le nord de l'océan Indien[122]) et de la fondation de la Banque asiatique d'investissement pour les infrastructures (qui compte déjà 20 gouvernements à son bord)[123]. Le dessein de la Chine est peut-être simplement de se hisser d'abord au sommet de sa région avant de monter sur le trône mondial. Dans ce contexte, le cyber-espionnage dont elle s'est rendue coupable peut être davantage considéré comme un moyen d'accroître son influence à l'échelle mondiale et moins comme une volonté de réduire celle des États-Unis.

Notes

1. ROGIN, Josh, « NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History' », *Foreign Policy: The Cable*, 9 juillet 2012, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatesttransfer-of-wealth-in-history/.

2. Office of the Director of National Intelligence, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace,* Washington DC: Office of the National Counterintelligence Executive, É.-U., octobre 2011, www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

3. SPADE, Colonel Jayson M., *Information as Power: China's Cyber Power and America's National Security*, Carlisle, PA: U.S. Army War College, É.-U., mai 2012, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf ; Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2014*, Washington, DC: Rapport annuel au Congrès, É.-U., 2014, www.defense.gov/pubs/2014_DoD_China_Report.pdf ; Department of Defense, *Quadrennial Defense Review 2014*, Washington, D.C.: OSD, É.-U., 2014: V, www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

4. NATHAN, Andrew J. et SCOBELL, Andrew, « How China Sees America », *Foreign Affairs,* septembre/octobre 2012, www.foreignaffairs.com/articles/138009/andrew-j-nathan-and-andrewscobell/how-china-sees-america.

5. Office of the Secretary of Defense, *Military and Security Developments*.

6. WALCOTT, John, « Chinese Espionage Campaign Targets U.S. Space Technology », *Bloomberg*, 18 avril 2012, www.bloomberg.com/news/2012-04-18/chinese-espionage-campaign-targets-u-s-space-technology.html.

7. SIMMONITE, Tom, « Chinese Hacking Team Caught Taking Over Decoy Water Plant », *Technology Review*, 2 août 2013, www.technologyreview.com/news/517786/chinese-hacking-team-caughttaking-over-decoy-water-plant/.

8. *Id*.

9. LIBERTO, Jennifer, « New Chinese Hacker Group Targets Governments, Nuclear Facilities », *CNN Money,* 4 juin 2013, http://money.cnn.com/2013/06/04/technology/security/cyber-hackergroup/index.html.

10. MAGNUSON, Stew, « Stopping the Chinese Hacking Onslaught », *NDIA*, juillet 2012, www.nationaldefensemagazine.org/archive/2012/July/Pages/StoppingtheChineseHackingOnslaught.aspx.

11. HALL, Susan D., « Chinese Hackers Targeting the Healthcare Industry », *FierceHealthIT*, 20 mars 2013, www.fiercehealthit.com/story/chinese-hackerstargeting-healthcare-industry/2013-03-20.

12. TAYLOR, Nick Paul, « Chinese Trial Data Hackers Reportedly Active Again », *Fierce BioTechIT,* 27 mai 2013, www.fiercebiotechit.com/story/chinesetrial-data-hackers-reportedly-active-again/2013-05-27.

13. HALL, Susan D., « *Chinese Hackers Targeting the Healthcare Industry* ».

14. « *China's 12th Five Year Plan: How it Actually Works and What's in Store for the Next Five Years* », APCO, 10 décembre 2010, www.export.gov.il/UploadFiles/03_2012/Chinas12thFive-Year Plan.pdf.

15. *Id*.

16. « *China's 12th Five-Year Plan: Overview* », Pékin, Chine, KPMG, mars 2011, www.kpmg.com/cn/en/IssuesAndInsights/ArticlesPublications/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf.

17. FERGUSON, Robyn E., « Information Warfare with Chinese Characteristics: China's Future View of Information Warfare and Strategic Culture », (mémoire de maîtrise, US Army Command and General Staff College, 2002, p. 15.

18. WINDREM, Robert, « Expert: U.S. In Cyber Arms Race With China, Russia », *NBC News Investigations*, 20 février 2013, http://investigations.nbcnews.com/_news/2013/02/20/17022378-expert-us-incyberwar-arms-race-with-china-russia.

19. MULVENON, James, « *The People's Liberation Army in the Information Age* », Santa Monica: RAND, 1999, p. 183.

20. THOMAS, Timothy L., « Google Confronts China's Three Warfares », *Parameters* 40, n° 2, été 2010, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2010summer/Thomas.pdf.

21. « Lawmaker: China Engaging in Cyber Spying », *Fox News*, 4 octobre 2011, www.foxbusiness.com/technology/2011/10/04/lawmaker-china-engaging-incyber-spying/.

22. « APT 1: Exposing one of China's Espionage Units », *Mandiant*, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

23. Remarques de Tom Donilon, 11 mars 2013, « The United States and the Asia-Pacific in 2013 », *The Asia Society*, https://obamawhitehouse.archives.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisor-president-united-states-an.

24. HOWARD, Steve, « Obama, China's Xi Discuss Cybersecurity Dispute on Phone Call », *Reuters*, 14 mars 2013, www.reuters.com/article/2013/03/14/ususa-china-obama-call-idUSBRE92D11G20130314.

25. JOHNSON, M. Alex et DELUCA, Matthew, « Obama Takes Diplomatic Tack on Chinese Cyberespionage Charges », *NBC News*, 7 juin 2013, http://usnews.nbcnews.com/_news/2013/06/07/18804533-obama-takes-diplomatictack-on-chinese-cyberespionage-charges.

26. BARRETT, Devlin, et GORMAN, Siobhan, « U.S. Charges Five in Chinese Military of Hacking », *The Wall Street Journal,* 19 mai 2014, www.wsj.com/articles/SB10001424052702304422704579571604060696532.

27. SEGAL, Adam, « Axiom and the Deepening Divide in U.S.-China Relations », *Council on Foreign Relations* (blogue), 29 octobre 2014, http://blogs.cfr.org/cyber/2014/10/29/axiom-and-the-deepening-divide-in-u-s-chinacyber-relations/.

28. « *China* », Cultural Savvy, www.culturalsavvy.com/china.htm.

29. TZU, Sun, *The Art of War,* www.theartofwar.ws/The_Art_of_War.pdf.

30. Office of the Secretary of Defense, *Military and Security Developments*, p. 26.

31. THOMAS, « *Google Confronts China's Three Warfares* ».

32. Office of the Secretary of Defense, *Military and Security Developments*, p. 26.
33. *Id*.
34. *Id*.
35. CHENG, Dean, *Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response*, The Heritage Foundation report n° 2745, Washington, DC, É.-U., The Heritage Foundation, É.-U., 26 novembre 2012, www.heritage.org/asia/report/winning-without-fighting-chinese-public-opinion-warfare-and-the-need-robust-american.
36. *Id*.
37. *Id*.
38. *Id*.
39. THORNBURG, Nathan, « The Invasion of the Chinese Cyberspies », *Time*, 29 août 2005, http://content.time.com/time/magazine/article/0,9171,1098961-1,00.html.
40. KOUTSOUKIS, Jason, « Chinese Waging Online Spy War », *The Age*, 10 février 2008, www.theage.com.au/news/national/chinese-waging-online-spywar/2008/02/09/1202234232007.html ; BOYES, Roger, « China Accused of Hacking into Heart of Merkel Administration », *The Times*, 27 août 2007, www.thetimes.co.uk/tto/news/world/europe/article2595759.ece ; BUENAVENTURA, Donna, « China Tried to Hack Our Computers, Says India Security Chief M.K. Narayanan », *Donna's Security Flash* (blogue), 18 janvier 2010, https://blogs.msmvps.com/donna/2010/01/18/china-tried-to-hack-our-computers-says-india-s-security-chief-m-k-narayanan/.
41. INGRAHAM, Nathan, « US Government Claims Huawei and ZTE Pose a Risk to National Security: the Accusations, Responses, and Fallout », *The Verge,* 11 octobre 2012, www.theverge.com/2012/10/11/3488584/huawei-zte-us-governmentsecurity-investigation.
42. « Admit Nothing and Deny Everything », *The Economist*, 6 juin 2013, www.economist.com/news/china/21579044-barack-obama-says-he-ready-talkxi-jinping-about-chinese-cyber-attacks-makes-one.
43. McREYNOLDS, Joe, « Cyber Transparency for Thee, But Not for Me », *The Jamestown Foundation China Brief*, 14, n° 8, www.jamestown.org/single/?tx_ttnews[tt_news]=42246&no_cache=1#.VTfXNBdSxdY.
44. RILEY, Charles, « China's Military Denies Hacking Allegations », *CNNMoney,* 20 février 2013, http://money.cnn.com/2013/02/20/technology/china-cyberhacking-denial/.
45. BARBOZA, David, « China Says Army Is Not Behind Attacks in Report », *The New York Times*, 21 février 2013, www.nytimes.com/2013/02/21/business/global/china-says-army-not-behindattacks-in-report.html?_r=0.
46. « Espionage Report: Merkel's China Visit Marred by Hacking Allegations », *Spiegel Online*, 27 août 2007, www.spiegel.de/international/world/espionage-report-merkel-s-china-visitmarred-by-hacking-allegations-a-502169.html.
47. « M Trends 2014: Beyond the Breach », *Mandiant*, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.
48. PEEK, Liz, « U.S. and China in a Lethal Game of Cyber Chess », *The Fiscal Times*, 9 avril 2014, www.thefiscaltimes.com/Blogs/Peek-POV/2014/04/09/USand-China-Lethal-Game-Cyber-Chess.
49. House, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei Technologies and ZTE*, 112th Congress, 8 octobre 2012, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf.

50. « Huawei: Leaked Report Shows No Evidence of Spying », *BBC News*, 18 octobre 2012, www.bbc.com/news/technology-19988919.

51. BLANCHARD, Ben, HUI, Li, et CARSTEN, Paul, « China Blames U.S. for Rise in Hacking Attacks », *The Fiscal Times*, 28 mars 2014, www.thefiscaltimes.com/Articles/2014/03/28/China-Blames-US-Rise-Hacking-Attacks.

52. WILDER, Charly, « Out of Hand: Europe Furious over U.S. Spying Scandal », *Spiegel Online*, 24 octobre 2013, www.spiegel.de/international/world/angry-european-and-german-reactionsto-merkel-us-phone-spying-scandal-a-929725.html.

53. WATTS, Jonathan, « NSA Accused of Spying on Brazilian Oil Company Petrobas », *The Guardian*, 9 septembre 2013, www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

54. MOYER, Edward, « NSA Spied on EU Antitrust Official Who Sparred With U.S. Tech Giants », *Cnet*, 20 décembre 2013, www.cnet.com/news/nsa-spiedon-eu-antitrust-official-who-sparred-with-us-tech-giants/.

55. HOSENBALL, Mark, « Obama Halted NSA Spying on IMF and World Bank Headquarters », *Reuters*, 31 octobre 2013, www.reuters.com/article/us-usasecurity-imf-idUSBRE99U1EQ20131031.

56. SAVAGE, Charlie, « Watchdog Report Says NSA Is Illegal and Should End », *The New York Times*, 23 janvier 2014, www.nytimes.com/2014/01/23/us/politics/watchdog-report-says-nsa-program-is-illegal-and-should-end.html?partner=rss&emc=rss&smid=twnytimes&_r=1.

57. « U.S., China Agree to Work Together on Cyber Issues », *Reuters*, 13 avril 2013, www.reuters.com/article/2013/04/13/us-china-us-cyberidUSBRE93C05T20130413.

58. PEEK, « *U.S. and China in a Lethal Game of Cyber Chess* ».

59. Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage*, Washington, DC, U.S. Department of Justice, É.-U., 19 mai 2014, www.justice.gov/opa/pr/us-charges-fivechinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

60. CHENG, *Winning Without Fighting*.

61. KEXIN, L., *Study Volume on Legal Warfare,* Washington, DC, É.-U., National Defense University Press, 2006, p. 18, 34-37.

62. ORTS, Eric W., « The Rule of Law in China », *Vanderbilt Journal of Transnational Law*, 1 janvier 2001, www.highbeam.com/doc/1G1-72733959.html.

63. CHENG, *Winning Without Fighting*.

64. *Id*.

65. THOMSON, Amy, « UN Telecom Treaty Approved Amid U.S. Web-Censorship Concerns », *Bloomberg*, 14 décembre 2012, www.bloomberg.com/news/articles/2012-12-13/u-s-and-u-k-refuse-to-sign-unagreement-on-telecommunications.

66. « U.S. and UK Refuse to Sign UN's Communications Treaty », *BBC News,* 14 décembre 2012, www.bbc.co.uk/news/technology-20717774.

67. Ibid.

68. TIMBERG, Craig, « U.S. to Relinquish Last Control Over the Internet », *The New York Times*, 14 mars 2014, www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html.

69. RRN Prasad, « Towards Freedom of the Internet », *The Financial Express*, 4 janvier 2016, www.financialexpress.com/article/fe-columnist/towardsfreedom-of-the-internet/187447/.

70. Assemblée générale des Nations Unies, A/66/359, « Courrier daté au 12 septembre 2011 et adressé au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, du Tadjikistan et de l'Ouzbékistan auprès de l'Organisation des Nations Unies », 12 septembre 2011, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

71. Assemblée générale des Nations Unies, A/69/723, « Courrier daté au 9 janvier 2015 et adressé au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, du Tadjikistan et de l'Ouzbékistan auprès de l'Organisation des Nations Unies », 9 janvier 2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

72. « China Says Cyber Hacking is Against the Law », *Voice of America*, 13 janvier 2010, www.voanews.com/content/china-says-cyber-hacking-is-againstlaw-81473967/111452.html.

73. JIAN, Gu, « Strengthening international cooperation and joining hands in fighting against transnational cybercrime », *China.org*, 9 novembre 2010, www.china.org.cn/business/2010internetforum/2010-11/09/content_21306503.htm.

74. FINKLE, Jim, MENN, Joseph, et VISWANATHA, Aruna, « US Accuses China of Cyber Spying on American Companies », *Reuters*, 20 novembre 2014, www.reuters.com/article/2014/11/20/us-cybercrime-usa-chinaidUSKCN0J42M520141120.

75. STOKES, Mark, *The Chinese Joint Aerospace Campaign: Strategy, Doctrine, and Force Modernization in China's Revolution in Doctrinal Affairs*, éd. MULVENON, James et FINKLESTEIN, David, Alexandria, VA, É.-U. : CNA Corporation, 2005, p. 272.

76. CHENG, *Winning Without Fighting*.

77. FERGUSON, « *Information Warfare with Chinese Characteristics* », p. 31.

78. MULVENON, James, « The PLA and Information Warfare », in *The People's Liberation Army in the Information Age*, éd. MULVENON, James et YANG, Richard H., Washington, DC, É.-U. : RAND, 1999, 180.

79. CHENG, *Winning Without Fighting*.

80. YANHUA, Guo, *Psychological Warfare Knowledge*, Washington, DC, É.-U. : National Defense University Press, 2005, pp. 14-16.

81. « Remarques du Président Obama et du Président Xi Jinping de la République populaire de Chine après une rencontre bilatérale », *The White House*, 8 juin 2013, www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obamaand-president-xi-jinping-peoples-republic-china-.

82. « China Says Cyber Hacking is Against the Law », *Voice of America*.

83. Assemblée générale des Nations Unies, A/66/359, « Courrier daté au 12 septembre 2011 ».

84. Assemblée générale des Nations Unies, A/69/723, « Courrier daté au 9 janvier 2015 ».

85. AUSTIN, Greg, « China's Cyber Turn: Recognizing Change for the Better », *The Diplomat*, 21 décembre 2015, http://thediplomat.com/2015/12/chinas-cyber-turnrecognizing-change-for-the-better/.

86. ORLIK, Tom, « Charting China's Economy: 10 Years Under Hu », *The Wall Street Journal* (blogue), 16 novembre 2012, http://blogs.wsj.com/chinarealtime/2012/11/16/charting-chinas-economy-10-yearsunder-hu-jintao/tab/print/.

87. « More than Minerals », *The Economist*, 23 mai 2013, www.economist.com/news/middle-east-and-africa/21574012-chinese-trade-africa-keeps-growing-fears-neocolonialism-are-overdone-more ; « China Overtakes U.S. as Brazil's Top Trade Partner », *Latin American Times*, 17 octobre 2013, www.laht.com/article.asp?ArticleId=333733&CategoryId=10718.

88. WENJUAN, Du, « China Investment in Brazil More Diversified », *China Daily*, 14 mai 2013, http://usa.chinadaily.com.cn/business/2013-05/14/content_16498645.htm.

89. « China's Mighty Telecom Footprint in Africa », *New Security Learning,* 14 février 2011, www.newsecuritylearning.com/index.php/archive/75-chinasmighty-telecom-footprint-in-africa.

90. IASIELLO, Emilio, « Stuffing the Genie Back into the Bottle: Can Threats to the IT Supply Chain Be Mitigated? », *Foreign Policy Journal*, 3 avril 2013, www.foreignpolicyjournal.com/2013/04/03/stuffing-the-genie-back-in-thebottle-can-threats-to-the-it-supply-chain-be-mitigated/.

91. CLARK, Liat, « Huawei Not a Threat to UK. Says Huawei Oversight Board », *Wired*, 27 mars 2015, www.wired.co.uk/news/archive/2015-03/27/huawei-nota-threat-to-national-security.

92. OSMAN, Hafizah, « Huawei Supports Australian Cyber Security Centre Development », *Arnnet.com*, 23 janvier 2013, www.arnnet.com.au/article/451519/huawei_supports_australian_cyber_security_centre_development_/.

93. ROGIN, « NSA Chief: Cybercrime ».

94. GREEN, Marcel A., « China's Growing Cyberwar Capabilities », *The Diplomat*, 13 avril 2015, http://thediplomat.com/2015/04/chinas-growing-cyberwarcapabilities/.

95. Témoignage de Richard Bejtlich devant la Commission d'examen de l'économie et de la sécurité de la Chine, lors d'une audience sur 'L'évolution des capacités cybernétiques et nucléaires de la Chine' », 26 mars 2012, U.S.-China Economic and Security Review Commission, www.uscc.gov/sites/default/files/3.26.12bejtlich.pdf.

96. FISHER, Jonathan, « China Has Hacked Every Major U.S. Company, Claims Richard Clarke », *Web Pro News*, 28 mars 2012, www.webpronews.com/china-has-hacked-every-u-s-major-company-claimsrichard-clarke-2012-03.

97. THOMAS, Timothy L., « New Developments in Chinese Strategic Psychological Warfare », *Special Warfare* 1, n° 9, 2003, www.dtic.mil/cgibin/GetTRDoc?AD=ADA434978.

98. THORNBURGH, Nathan, « Inside the Chinese Hack Attack », *Time*, 25 août 2005, http://content.time.com/time/nation/article/0,8599,1098371,00.html.

99. KOPAN, Tal, « White House Readies Cyber Sanctions Against China Ahead of State Visit », *CNN*, 24 septembre 2015, www.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-presidentobama/.

100. Department of Defense, *Strategy for Operating in Cyberspace,* Washington, DC, É.-U., U.S. Department of Defense, juillet 2011, www.defense.gov/news/d20110714cyber.pdf

101. KEROMYTIS, Angelos, « *Active Cyber Defense* », Program Information, Defense Advanced Research Projects Agency (DARPA), consulté le 28 septembre 2017, www.darpa.mil/program/active-cyber-defense.

102. REED, John, « Mike Rogers: Cool It with Offensive Cyber Ops », *ForeignPolicy.com*, 14 décembre 2012, http://foreignpolicy.com/2012/12/14/mike-rogerscool-it-with-offensive-cyber-ops/.

103. Government Accountability Office, *National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, Washington, DC, É.-U., Government Accountability Office, février 2013, www.gao.gov/assets/660/652170.pdf.

104. Government Accountability Office, *A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges*, Washington, DC, É.-U., Government Accountability Office, mars 7, 2013, www.gao.gov/assets/660/652817.pdf.

105. CHENG, *Winning Without Fighting*.

106. « China Accuses U.S. of Hypocrisy Over Internet Spying », *Sydney Morning Herald*, 28 juin 2013, www.smh.com.au/world/china-accuses-us-ofhypocrisy-over-internet-spying-20130628-2p0uk.html.

107. MESSMER, Ellen, « Don't Trust the NSA? China-based Huawei Says, 'Trust Us' », *Network World*, 18 octobre 2013, www.networkworld.com/news/2013/101813-nsa-huawei-274959.html?page=1.

108. « FACT SHEET: President Xi Jinping's State Visit to the United States », *The White House*, 25 septembre 2015, www.whitehouse.gov/the-pressoffice/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

109. « Chinese Hackers Arrested After U.S. Request », *BBC News*, 12 octobre 2015, accessible à l'adresse : www.bbc.com/news/technology-34504317.

110. House. *Déclaration de Paul K. Martin (Inspecteurr général, NASA) : NASA Cybersecurity: An Examination of the Agency's Information Security*, Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, 29 février 2012, https://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf.

111. Ministry of Foreign Affairs, *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on October 13, 2014*, Washington, DC, É.-U., Ministry of Foreign Affairs, 13 octobre 2015, www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1165638.shtml.

112. « S. Korea, Japan, China to Hold Cyber Policy Talks », *Yonhap News Agency*, 13 octobre 2015, http://english.yonhapnews.co.kr/news/2015/10/13/0200000000AEN20151013004800315.html.

113. « Malaysia, China to Work Together on Cyber Crimes », *The Malay Mail Online*, 22 août 2014, www.themalaymailonline.com/malaysia/article/malaysia-china-to-worktogether-to-combat-cyber-crimes.

114. « S. Korea, Japan, China to Hold Cyber Policy Talks », *Yonhap News Agency*.

115. NAKASHIMA, Ellen, « World's Richest Nations Agree Hacking for Commercial Benefits Is Off-Limits », *The Washington Post*, 16 novembre 2015, www.washingtonpost.com/world/national-security/worlds-richest-nationsagree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b_story.html.

116. NAKASHIMA, Ellen, « Chinese Government Has Arrested the Hackers Breached OPM Database », *The Washington Post*, 2 décembre 2015, www.washingtonpost.com/world/national-security/chinese-government-hasarrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

117. « S. Korea, Japan, China to Hold Cyber Policy Talks », *Yonhap News Agency*.

118. RAZUMOVSKAYA, Olga, Russia and China Pledge Not to Hack Each Other, *The Wall Street Journal* (blogue), 8 mai 2015, http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/.

119. WILLIAMS, Bo, Katie, « UK, China Mirror U.S. Anti-Hacking Pact », *The Hill*, 21 octobre 2015, http://thehill.com/policy/cybersecurity/257602-uk-china-mirror-usanti-hacking-pact.

120. « FACT SHEET: President Xi Jinping's State Visit », *The White House*.

121. NAKASHIMA, « *World's Richest Nations Agree* ».

122. BREWSTER, David, « The Bay of Bengal:« The Maritime Silk Route and China's Naval Ambitions », *The Diplomat*, 14 décembre 2014, http://thediplomat.com/2014/12/the-bay-of-bengal-the-maritime-silk-route-andchinas-naval-ambitions/.

123. PONGSUDHIRAK, Thitinan, « China's Aspiring Global Leadership », *East Asia Forum,* 25 novembre 2014, www.eastasiaforum.org/2014/11/25/chinasaspiring-global-leadership/.

L'opérationnalisation de la protection des civils dans les opérations de l'OTAN

Marla B. Keenan*
Alexander William Beadle**

Dans la plupart des opérations militaires internationales, la protection des civils est un objectif essentiel. Pourtant, les conflits du monde entier continuent de malmener les populations. Depuis le début des années 1990, l'Organisation du traité de l'Atlantique Nord (OTAN) a conduit plusieurs opérations dans lesquelles la protection des civils était une composante clé, inscrite explicitement au mandat d'une mission ou assurée par défaut pour l'accomplissement de cette dernière. Ces opérations se sont achevées avec un succès variable ou, pour certaines, soldées par un échec. Or cette situation n'est pas propre à l'OTAN. La mise en œuvre de la protection des civile reste une priorité et un défi pour de nombreuses organisations multilatérales, dont l'Organisation des Nations Unies (ONU) et l'Union africaine (UA). Cela s'explique en partie par le fait que chaque organisation a une conception différente de la protection des civils, en fonction de leur mission, de leurs capacités et du théâtre des opérations. Si des politiques, des doctrines, des lignes directrices et des formations ont vu le jour, la capacité de mise en œuvre de la protection des civils, à savoir la création et l'utilisation des moyens de

*Directrice de programmes au Center for Civilians in Conflict, Marla Keenan est experte fonctionnelle de la limitation des dommages causés aux civils, des mécanismes de suivi des victimes civiles et de la gestion des conséquences des dégâts infligés aux populations. Elle est chargée de recherche de l'association Truman National Security Project. Marla a instruit des officiers militaires dans plusieurs écoles supérieures et d'état-major.

**Alexander W. Beadle est chargé de recherche pour un projet financé par le CD & E sur la protection des civils, ainsi que pour un nouveau projet portant sur les tendances mondiales et les opérations militaires. Ses travaux portaient initialement sur la façon dont la force militaire peut être employée pour protéger les civils des auteurs de violence. Il a travaillé sur un projet avec le quartier général interarmées norvégien qui a développé un guide militaire d'évaluation et de planification pour la protection des civils dans les opérations militaires.

Marla B. Keenan et Alexander W. Beadle, « Operationalizing Protection of Civilians in NATO Operations », *Stability* : *International Journal of Security and Development*, 4, no 1, 2015, p. 55. DOI : http://doi.org/10.5334/sta.gr

défense destinés à protéger effectivement les populations civiles et vulnérables dans un conflit, fait encore défaut.

L'article porte non pas sur la décision d'intervention des responsables politiques, ni sur les faits se déroulant à l'issue de l'intervention, mais bien plus sur ce qui se passe entre les deux, afin de consolider la bonne compréhension opérationnelle de la protection des civils pour l'OTAN, en accord avec les attentes des civils, et des menaces spécifiques contre lesquelles ils devront être protégés. L'échelle de protection (*Protection Ladder*) étudiée dans ce document conceptualise de manière intéressante les différents niveaux de protection physique. Nous démontrerons ainsi que cet outil illustratif et hiérarchique aide les planificateurs militaires à comprendre les obligations légales et les autres couches opérationnelles nécessaires pour protéger les civils des préjudices physiques. Enfin, cet article présente des moyens pratiques pour protéger plus efficacement les civils avant, pendant et après les opérations.

Les auteurs espèrent que le développement d'une compréhension solide de la protection des civils pour l'OTAN renforcera la capacité de l'Organisation à protéger un plus grand nombre de civils lors des opérations futures.

L'OTAN et la protection des civils

La protection des civils est autant une question de volonté politique que de puissance militaire. Les pays fournisseurs de contingents peuvent être confrontés au terrible dilemme de troquer la vie de leurs soldats contre celle des civils. Un jour ou l'autre, il faudra nécessairement passer du conflit armé et des opérations de stabilisation à l'état de paix, dans le respect total de l'état de droit et des droits de l'homme. Signe de l'échec des acteurs tant militaires que civils, les transitions n'ont pas toujours été couronnées de succès. L'expérience a montré que sans une approche holistique de la stabilité et du maintien de la paix intégrant la protection des civils, la réussite globale d'une mission peut être illusoire.

Dès lors qu'une décision politique d'intervenir dans un conflit donné a été prise, les planificateurs militaires doivent appuyer leur opération sur une stratégie cohésive. Ils peuvent se concentrer sur l'objectif de la protection des civils sur le théâtre des opérations selon deux approches possibles, toutes deux expérimentées par l'OTAN.

Tout d'abord, la protection des civils peut être l'objectif premier d'une opération, motivée par des considérations politiques ou morales, afin de mettre un terme aux violences massives infligées à une frange de la population. Ainsi, l'opération *Allied Force* était destinée à faire cesser le nettoyage ethnique des Albanais opéré par les forces serbes au Kosovo (1999) ; en Libye, l'opération *Unified Protector* visait à mettre fin à la violente répression du régime de Kadhafi contre son peuple (2011). Dans les deux cas, l'OTAN a joué un rôle moteur, par le biais de sa force aérienne, en instaurant des zones d'exclusion aérienne et en frappant les cibles militaires serbes et libyennes.

Au Kosovo, l'opération a été conduite sans mandat du Conseil de sécurité de l'ONU, ce qui n'était pas le cas de l'opération en Libye.

Deuxième cas de figure, le plus fréquent, la protection des civils peut être un objectif parmi d'autres dans le cadre d'une opération militaire de plus grande envergure. En Afghanistan, si la protection des civils n'était pas explicitement incluse dans le mandat de la Force internationale d'assistance à la sécurité (FIAS), c'était à n'en pas douter l'un des objectifs stratégico-militaires les plus importants de la mission. D'ailleurs, six ans après le début de la mission, lorsque les opérations cinétiques et de sécurité prirent de l'ampleur, les observateurs redoublaient d'attention. Quand la protection des civils ne figure pas explicitement au mandat d'une opération, cette dernière vise généralement un objectif premier d'un autre ordre, comme la contre-insurrection ou le contre-terrorisme. Par exemple, dans les opérations de l'OTAN, la protection des civils est souvent axée sur l'objectif stratégique de neutralisation des menaces pesant sur les états membres, et éventuellement sur d'autres états, et sur la lutte contre le terrorisme. Plus rares sont les opérations spécifiquement axées sur la protection proactive des civils. Notons toutefois que le défaut de protection des civils contre les dommages causés par les opérations de l'OTAN ou d'un autre acteur peut entraver sévèrement l'accomplissement de l'objectif premier[1].

Quelle que soit la raison de l'intervention dans un conflit, les civils s'attendent à être protégés[2]. Ils ne sont pas toujours en mesure d'identifier leur agresseur, mais bien souvent ils savent qui a les moyens d'assurer leur sécurité et leur protection. Or quand les forces ne répondent pas aux attentes des populations, voire leur font du mal, cela inspire leur colère et leur ressentiment. Les civils peuvent alors se détourner des forces sur lesquelles ils comptaient pour leur protection. À défaut de voir l'OTAN assurer sa sécurité, par exemple, la population soutiendra le premier acteur en mesure de la protéger, comme ce fut le cas dans certaines régions en Afghanistan[3]. Le défaut de protection peut également affaiblir la légitimité des parties au conflit, conduire à l'effondrement d'un état, perpétuer les cycles de violence et les déplacements internes et affecter les pays voisins par des flux de réfugiés.

Différentes doctrines et directives de l'OTAN, dont celles portant sur la contre-insurrection (COIN) et sur le contre-terrorisme (CT), étudient la primauté des civils en tant qu'impératif militaire stratégique dans chacun de ces contextes. Ce point est clairement mis en avant dans la doctrine de contre-insurrection de l'OTAN :

> Il convient de garder à l'esprit que tuer de nombreux insurgés sera largement contre-productif si les dommages collatéraux tuent également des civils pacifistes. Cela conférera une légitimité à l'insurrection et conduira à un soutien accru de la population. C'est pourquoi les commandants doivent mettre en place des proc*é*dures afin d'arriver à une utilisation équilibrée de la force et d'éviter une utilisation excessive de la force qui conduirait à des dommages collatéraux[4].

Mais cet exemple parmi d'autres montrent à quel point les doctrines et les politiques ignorent l'importance de protéger la population non seulement des opérations des autres acteurs, mais également de celles de l'OTAN[5].

En Afghanistan, par exemple, on pourrait avancer de façon très convaincante que la protection lors des opérations de la FIAS et d'autres groupes antigouvernementaux aurait dû se poser comme préoccupation centrale dès le départ. Les recherches menées par CIVIC, entre autres, ont révélé que des territoires stratégiques essentiels et le soutien des populations civiles ont été perdus, car le nombre de victimes civiles imputables aux actions de la FIAS s'ajoutaient aux pertes civiles causées par ses adversaires[6]. En changeant finalement sa tactique, la FIAS a pu effectivement limiter les dommages occasionnés aux civils par ses propres opérations. Mais la réponse était tardive, et les préjudices infligés aux populations par d'autres groupes persistaient. Par exemple, le recours par les groupes antigouvernementaux à des engins explosifs improvisés (EEI) ciblant les forces internationales et afghanes a touché massivement les civils afghans. Dans ce cas, la seule présence des forces internationales dans certaines régions augmentait les risques de dommages causés par les EEI parmi les civils, par rapport aux zones où elles n'étaient pas présentes. Toutefois, les initiatives de lutte contre les EEI lancées initialement par la FIAS pour la protection des forces ont rapidement été utilisées comme mesures proactives de protection, réduisant les dommages causés aux civils.

Cette situation traduit malheureusement le vide doctrinal existant dans de nombreuses organisations supposées aujourd'hui protéger les civils[7]. Les intervenants sont certainement animés des meilleures intentions, mais bien souvent ils ne démontrent pas d'une solide compréhension stratégique des défis posés par la protection, des outils opérationnels et de la formation tactique requise pour protéger efficacement les civils de la violence.

La mise en œuvre de la protection des civils nécessite une compréhension, une connaissance et une formation sur les moyens d'atteindre cet objectif sur le terrain. Les personnels militaires internationaux, régionaux et nationaux manquent généralement de directives sur la façon de protéger les civils plus efficacement lors des opérations militaires. Cela s'explique par l'absence de doctrines ou de principes éprouvés ou historiques sur lesquels les militaires chargés de planifier ou d'exécuter la mission pourraient s'appuyer. Et face au manque d'orientations, les planificateurs n'ont pas d'autre choix que d'improviser. La difficulté est d'autant plus grande pour les missions dont le mandat premier est de protéger les civils, car réparer les pertes humaines est impossible. À défaut d'une doctrine bien développée et d'une capacité de mise en œuvre correspondante, il y a fort à parier que la mission se soldera par un échec. Il convient de noter que dans les environnements complexes les militaires doivent introduire une flexibilité suffisante permettant une réponse prompte en cas d'évolution rapide de la situation sur le théâtre.

Signification de la « protection »

Les civils ont droit au spectre complet de la protection, qui inclut la protection physique face à la violence imminente, la fourniture des produits de première nécessité, la jouissance des droits de l'homme et des conditions favorables. Avec le cadre conceptuel de l'« oignon de la protection », le Professeur Paul D. Williams fournit la définition suivante :

> [L'oignon de la protection est une] adaptation de la « structure en œuf » développée par le CICR à la fin des années 1990 pour décrire le lien entre les types d'exaction et ce que l'organisation considérait comme les trois formes d'activités de protection (réactive, corrective et visant à améliorer l'environnement). Cette représentation montre que la protection peut être envisagée sous un angle minimaliste (survie physique) ou maximaliste (jouissance des droits), donc comme un concept comprenant de nombreuses couches interconnectées. Idéalement, les civils devraient bénéficier de l'ensemble, mais en pratique ils peuvent perdre les couches extérieures et cependant survivre, étant entendu que certaines personnes sont plus endurantes que d'autres. Le noyau central de la protection physique est toutefois essentiel à toutes les autres couches[8].

Une force militaire ne peut, à elle seule, entreprendre toutes ces activités. Elle doit comprendre ce qu'implique la protection des civils et identifier les domaines où elle peut être la plus utile dans l'espace de protection au sens large. Les décideurs politiques et les planificateurs militaires chargés du déploiement des forces d'intervention doivent se concentrer sur le « noyau central de la protection physique », car c'est là qu'une intervention militaire peut, en effet, être la plus utile, avec un usage mesuré de la force.

Pour protéger de manière effective, la force militaire doit comprendre les menaces existantes et mobiliser les capacités correspondantes afin de les contrer. Il s'agit d'un rôle unique qu'aucun autre acteur, non armé, n'est susceptible de tenir. Les groupes comme les organisations non gouvernementales (ONG) et la société civile ont d'autres rôles importants à jouer dans la protection des civils, en ce qui concerne par exemple la résolution des problèmes humanitaires. Si la force militaire est axée principalement sur la protection physique, elle peut toutefois coopérer avec des homologues à d'autres niveaux, par exemple en matière d'assistance logistique pour l'acheminement des articles de première nécessité. Pour optimiser l'ensemble des capacités, une communication efficace avec ces homologues, focalisée sur la protection des civils, s'impose.

Pour qu'une force militaire comprenne et opérationnalise la protection des civils, elle doit disposer d'une définition claire et d'une vision stratégique, communes à l'ensemble de l'organisation, du concept de protection. Par exemple, l'ONU définit dans les grandes lignes la protection comme étant :

> Toutes les activités visant à obtenir le respect intégral des droits de toutes les personnes conformément au droit international, dont le droit international humanitaire, les droits de l'homme et le droit des réfugiés, quels que soient leur âge, leur sexe, leur origine sociale, ethnique, nationale, religieuse ou autre.

En outre, l'ONU définit la protection des civils comme étant :

> La protection des civils (PdC) en conflit armé, par laquelle toutes les parties au conflit sont chargées de s'assurer que toute la population civile est respectée et protégée.

La compréhension actuelle de la protection des civils par l'OTAN est très différente de celle des autres organisations internationales ou régionales comme l'ONU ou l'UA. Certes l'OTAN n'a pas encore adopté de définition formelle de la protection des civils, mais elle s'est focalisée dans les conflits passés sur la protection de la population face à ses propres actions. Or dans un environnement où différents acteurs coopèrent, l'absence d'une définition commune peut compromettre les plans de protections les plus solides.

Conceptualisation de la protection physique

Après s'être penchés pendant plusieurs années sur le sujet, les auteurs sont convaincus que les planificateurs militaires ont besoin d'une structure plus formelle afin de comprendre les différentes couches de la protection des civils. L'échelle de protection a été pensée par le *Center for Civilians in Conflict* comme un outil illustratif à l'usage des planificateurs militaires et des dirigeants afin d'expliquer les obligations légales et les autres couches opérationnelles concernées par la protection des civils (voir Figure 1). L'échelle permet de conceptualiser et d'opérationnaliser les différentes couches, ou échelons. Pour chaque échelon, il faut mettre en place les capacités correspondantes afin d'assurer le spectre complet de la protection des civils. Les compétences acquises à chaque échelon servent de base pour le suivant. Comme dans toute échelle, plus les échelons sont nombreux, plus la structure est solide, et plus sa portée est longue.

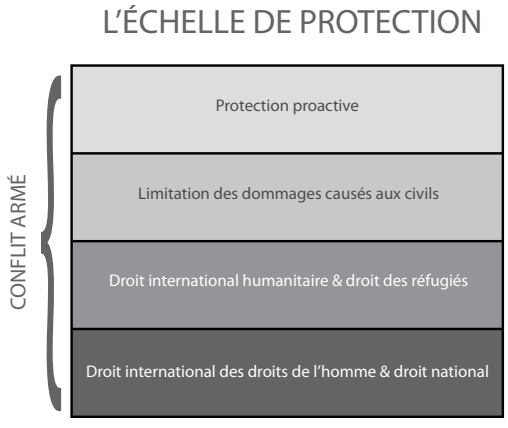

Figure 1

L'échelle de protection est un cadre conceptuel permettant de comprendre les différents niveaux de protection physique que les forces de sécurité peuvent fournir aux civils, soit en adhérant au droit national et international existant soit en adoptant des politiques et procédures spécifiques qui vont au-delà des exigences.

Droit international des droits de l'homme et droit national

Le niveau de base de la protection est l'application du droit national et du droit international des droits de l'homme. Cette couche normative, applicable en temps de paix comme en temps de troubles civils et de conflit armé, forme la base de la protection que les civils reçoivent du gouvernement de leur pays et des autres acteurs. La police et la gendarmerie sont le plus souvent les gardiens de ces lois. En cas de violation par les forces de sécurité et les autres acteurs armés, les contrevenants doivent être poursuivis par le biais des canaux appropriés.

Droit international humanitaire et droit des réfugiés

Le droit international humanitaire (DIH) et le droit des réfugiés sont destinés à protéger les civils des dangers des conflits armés. Ils interdisent de cibler directement les civils (distinction) et d'occasionner des dommages civils accidentels lors de l'attaque des cibles militaires (proportionnalité). Ils obligent les parties au conflit à prendre toutes les mesures possibles pour éviter de nuire aux civils. Les militaires respectant le DIH causent moins de dommages civils au cours de leurs opérations de combat. Dans les conflits actuels, toutefois, de nombreux acteurs armés (des acteurs gouvernementaux et des acteurs armés non étatiques) ne respectent pas toujours le DIH ou le méprisent délibérément. Les violations du DIF doivent être documentées et donner lieu à des poursuites.

Limitation des dommages causés aux civils

Malgré les efforts consentis lors d'une opération militaire donnée, et même si les principes du DIH sont rigoureusement appliqués, les dommages causés aux civils peuvent néanmoins être une conséquence directe de l'usage de la force. Ce type de dommage peut se produire au cours d'opérations planifiées ou d'actions d'autodéfense. Si ce type de « dommage accidentel », souvent désigné « dommage collatéral », n'est pas illégal, il doit cependant être limité, faire l'objet d'une enquête et être pris en charge de façon appropriée par la force militaire.

Protection proactive

Les acteurs armés ciblent parfois délibérément les civils, pensant que cela peut servir leur objectif global. Dans ce cas, il est nécessaire qu'un troisième acteur intervienne pour empêcher ou atténuer la violence. Ceux qui ciblent spécifiquement les populations sont responsables de la grande majorité des victimes civiles. Cet état de fait montre que pour protéger les civils de la violence physique, le recours proactif à la force contre les auteurs des violences est bien souvent nécessaire. Ainsi, il peut s'avérer nécessaire d'établir une présence à proximité des populations vulnérables, comme des patrouilles, en s'interposant entre les auteurs de violences et leurs victimes potentielles, et/ou de rechercher proactivement les groupes désireux de nuire aux civils et de neutraliser la menace. C'est aux responsables de la planification ou de l'exécution de ces opérations qu'incombe la décision cruciale d'adapter ces approches aux situations particulières.

Opérationnalisation de la protection physique

La protection des civils implique avant tout de susciter un état d'esprit, un mode de pensée parmi les décideurs politiques, les planificateurs militaires, les chefs, et les soldats. Elle doit être adoptée comme stratégie et politique, puis enseignée tout au long de la chaîne du commandement pour s'assurer que quiconque, du commandant le plus gradé au plus simple soldat, saisisse le concept et comprenne pourquoi elle est essentielle à la réussite d'une mission.

Une force militaire ne peut pas entreprendre toutes les activités de protection. Elle doit identifier effectivement les domaines où elle peut être la plus utile. Pour assurer une protection effective, la force militaire doit comprendre les menaces existantes et adapter les capacités afin de les contrer, rôle que les acteurs non armés ne sont pas en mesure de tenir. La protection est exécutée tout au long du développement complet de l'opération militaire, c'est-à-dire avant, pendant et après. Une stratégie de protection n'est pas en soi suffisante ; elle doit être planifiée, mise en œuvre et faire l'objet d'une instruction à tous les échelons. Dans la partie suivante, nous étu-

dions des suggestions pratiques afin d'intégrer efficacement la protection des civils aux phases de planification, d'exécution et d'évaluation des opérations militaires conduites par l'OTAN[9].

Avant les opérations

La stratégie, la planification et l'instruction sont les pivots d'une protection réussie des civils dans les opérations de l'OTAN. Sans une vision explicite de la protection des civils en amont des opérations, il y a peu de chances que les civils soient effectivement protégés lors du conflit.

Adopter une politique et des outils permanents

Le concept de protection, comprenant une définition en accord avec les autres organisations internationales, devrait être intégré à une politique militaire permanente de l'OTAN, indépendamment de tout conflit. Dans la planification stratégique, la protection devrait être traitée en priorité et enseignée dans le cadre d'entraînements basés sur des scénarios. Elle devrait être intégrée au processus de décision militaire et au processus de décision individuel de chaque soldat.

La *Civilian Casualty Mitigation Team* (CCMT) (équipe de la FIAS chargée de réduire le nombre de victimes civiles, et les directives) et les *Nonbinding Guidelines on Monetary Payments to Civilian Casualties in Afghanistan* (des lignes directrices non contraignantes sur les compensations financières versées aux familles de civils blessés) offre quelques exemples de la politique et des pratiques menées par l'OTAN. De fait, elles n'existent que dans le cadre d'un conflit donné. Ces pratiques doivent néanmoins être intégrées par l'OTAN dans une politique permanente, ce qui comporte un risque, celui de perdre les enseignements tirés des conflits récents. Nous étudierons ces pratiques plus avant dans la partie *Au cours des opérations*.

Développer un processus robuste d'évaluation des menaces

En fin de compte, ce sont les auteurs mêmes des violences qui choisissent le type de menace qu'ils font peser sur les victimes. Il est impossible de répondre à la question de savoir *comment* les civils peuvent être protégés sans connaître de prime abord la raison, les moyens et les méthodes employées par les auteurs.

L'absence de recommandations concerne surtout la phase *proactive* de la protection des civils et toutes les organisations, y compris l'OTAN, ont eu jusqu'à présent des difficultés à la rendre opérationnelle. Des recherches ont révélé que le spectre des menaces auxquelles l'OTAN est susceptible de devoir faire face comprend sept scénarios[10].

- **Le génocide**, dans lequel les auteurs cherchent à exterminer un groupe communautaire (par exemple, au Rwanda en 1994).

- **Le nettoyage ethnique**, où les auteurs cherchent à expulser un groupe communautaire (par ex., au Kosovo en 999).
- **La répression**, où un régime réprime par la violence toute résistance (par exemple, en Libye, en 2011).
- **Les représailles post-conflit**, par lesquelles les individus ou les foules se vengent de crimes passés (par exemple, au Kosovo après 1999).
- **Le conflit communautaire**, où des communautés entières cherchent à la fois à se venger d'un premier épisode de violence et à dissuader les représailles afin de se protéger elles-mêmes (par exemple, dans l'Ituri en RD Congo, de 1999 à 2003).
- **La violence prédatrice**, où les auteurs exploitent les civils pour survivre ou pour en tirer un profit (par exemple, l'Armée de résistance du Seigneur, de 1994 à aujourd'hui).
- **L'insurrection**, où les rebelles ciblent les civils afin de contrôler la population et de saper le contrôle des autres acteurs (par exemple, en Afghanistan, de 2002 à aujourd'hui).

L'OTAN, qui a rencontré la plupart de ces scénarios, se distingue particulièrement en ce qu'elle compte au nombre des quelques acteurs dont on peut attendre qu'ils protègent les civils de *l'ensemble* de ces menaces, y compris dans le pire des cas de figure de violence à grande échelle.

Chacune de ces situations représente une menace distincte dans la mesure où les civils les plus exposés, la façon dont ils sont ciblés, les moyens dont disposent les persécuteurs et le type de souffrance civile susceptible d'être engendrée diffèrent selon les cas. Cela montre à quel point il est important d'identifier les types particuliers de menaces pesant sur les civils dans la zone d'opération. Dans la plupart des conflits, des scénarios différents peuvent toutefois se produire simultanément dans des zones distinctes ou à différentes phases d'un conflit. Par exemple, la répression exercée initialement par le régime contre l'opposition armée ou non armée au Kosovo au cours des années 1990 s'est intensifiée, laissant place à un nettoyage ethnique de la population albanaise vers 1999, ce qui a déclenché l'intervention de l'OTAN. Après le retrait des troupes serbes et le déploiement des forces de l'OTAN, le nettoyage ethnique a conduit à des représailles post-conflit contre les Serbes et les autres minorités non albanaises. Une situation qui s'est détériorée et s'est soldée par le nettoyage ethnique des Serbes en 2004.

Le fait est que pour assurer une protection physique effective, il est essentiel d'évaluer en permanence les menaces. Différents scénarios impliquant le même agresseur peuvent aussi se dérouler simultanément. Par exemple, une milice communautaire peut attaquer une autre communauté pour se protéger tout en adoptant un comportement prédateur à l'égard de toutes les communautés de la région. Certains motifs poussant à cibler des civils s'excluent les uns les autres. Il est par exemple im-

possible d'expulser et, dans le même temps, exterminer physiquement un pan entier de la population. Même dans les rangs de l'agresseur, les motivations peuvent varier. Les combattants individuels peuvent gagner le respect de leurs camarades ou bien être mus par la crainte d'être eux-mêmes tués. Pour les chefs de grade intermédiaire, ce peut être d'étendre leur pouvoir. Cela dit, pour que la violence devienne systématique et suffisamment étendue pour déclencher une réponse militaire, il est fort probable que la situation globale réponde à l'une des catégories de motivation de la violence mentionnées ci-dessus.

Conséquence principale : des scénarios différents exigent des réponses militaires différentes si l'on veut protéger les civils sans leur infligé plus de mal. D'une part, cela nécessite des réponses qui limitent la vulnérabilité des civils ciblés et appuient leur propre stratégie de défense, comme en construisant une infrastructure leur donnant accès à l'eau dans un périmètre relativement sécurisé et en les informant sur les menaces possibles[11]. D'autre part, cela requiert souvent le recours aux forces militaires pour lutter plus directement contre les menaces de violence.

Les différentes visions de l'utilisation de la force militaire pour protéger les civils impliquent des niveaux différents de proactivité :

- Assistance et acheminement de l'aide humanitaire pour atténuer la crise (par exemple, transport, largages, construction de camps ou de routes, convois, installations de stockage sécurisées).
- Endiguement du conflit (par exemple, zones d'exclusion aérienne, embargos, dépôts d'armes sécurisés).
- Dissuasion ou défense contre les attaques ciblant les civils (par par exemple, patrouilles ; escortes ; protection de lieux sûrs/zones comme les villages, les stades, les bâtiments publics ou les camps ; interposition).
- Usage coercitif de la force contre les auteurs (par exemple, menaces, démonstration de force, frappes punitives stratégiques).
- Attaque ou neutralisation des auteurs (par exemple, frappes aériennes stratégiques, action directe, combat).

La question centrale des planificateurs militaire est : *laquelle de ces approches est la plus à même de protéger les civils de la situation de conflit et face à quel type d'agresseur se trouvent-ils ?* Deux réponses sont envisageables.

Premièrement, pour être efficace du point de vue stratégique, la réponse doit tenir compte de la *motivation* initiale de l'agresseur à cibler les civils. Par exemple, il est très probable que la dissuasion n'ait pas d'effet sur les auteurs d'un génocide, engagés dans un jeu à somme nulle et convaincus que l'extermination d'un groupe spécifique est la seule option viable. Les leçons tirées des extrémistes hutus au Rwanda et de l'Allemagne nazie pendant la Seconde Guerre mondiale montrent que, tant qu'ils ne seront pas totalement vaincus, les auteurs continueront à exterminer les civils. En

revanche, les groupes armés prédateurs ciblant les civils uniquement pour amasser des richesses nécessaires à leur survie (par exemple, en pillant les denrées alimentaires ou en enrôlant de force les enfants pour maintenir leur mainmise) sont autrement plus faciles à dissuader et peuvent être contraints à cesser totalement leurs activités. En effet, leur motivation première étant de rester en vie, ils éviteront la confrontation. C'est pourquoi ils viseront généralement des lieux non défendus, présentant peu de risques et promettant des gains élevés. Par le passé, même des démonstrations de force de faible envergure ont permis de démobiliser et de désarmer de nombreux combattants.

Deuxièmement, l'opération doit s'accorder au mode opératoire de l'agresseur. Cela nécessite d'avoir une bonne compréhension de la façon dont les auteurs ciblent les civils et les moyens dont ils doivent disposer pour y parvenir. Par exemple, l'OTAN a conduit des actions similaires au cours de ses opérations au Kosovo et en Libye, avec un résultat toutefois très différent en matière de protection des civils face aux menaces respectives pesant sur eux. Dans les deux opérations, l'OTAN a imposé des zones d'interdiction de survol et conduit des frappes aériennes contre des cibles militaires et des sites de commandement et de contrôle. Or les menaces contre les civils étaient différentes, ce qui signifie que l'utilité de cette conception opérationnelle différait également.

Au Kosovo, Milosevic a cherché à chasser une grande partie de la population albanaise par un usage démesuré de la violence. Son objectif n'était pas de l'éliminer ni même de la contrôler à l'avenir, mais de la faire fuir. Il devait donc s'appuyer sur la liberté de mouvement des unités irrégulières et paramilitaires chargées de brutaliser la population pour provoquer sa fuite. De ce fait, les frappes contre les unités militaires conventionnelles ont eu un impact limité sur la capacité du régime serbe à procéder au nettoyage ethnique, car ces opérations ont été menées sans l'appui des forces conventionnelles. En fin de compte, l'opération a duré bien plus longtemps que prévu, et quelque 90 pour cent des Albanais du Kosovo ont été déplacés, nombre d'entre eux ayant fui pendant la campagne aérienne. Même si Milosevic s'est finalement avoué vaincu, s'il a retiré ses forces et si les Albanais du Kosovo ont pu revenir, on ne pouvait pas vraiment dire que l'opération en soi avait protégé efficacement les civils de l'expulsion.

En Libye, Kadhafi ne cherchait pas à éliminer ni à chasser une frange de la population, mais à avoir la mainmise sur le peuple. Il a dû, pour cela, réprimer toute opposition, armée ou non. Il nécessitait d'abord et avant tout une puissance de feu substantielle (comme l'a montré Assad en Syrie, en recourant aux bombardements aériens, aux tirs de missiles SCUD et aux armes de destruction massive). En fait, la répression par le régime est la seule situation où les forces régulières et une puissance de feu massive sont les premières causes de victimes civiles. Ainsi, cibler les forces régulières de Kadhafi et ses capacités de commandement et de contrôle en Libye a

permis d'affaiblir sa capacité à cibler les civils. En comparaison avec la campagne aérienne au Kosovo, les civils ont été progressivement protégés de la menace que Kadhafi représentait. Avec la mort du Guide libyen, la menace a été éliminée, et c'était probablement le seul moyen, car rares sont les leaders autoritaires, dont le seul objectif est de sauver leur peau, ayant négocié leur propre retrait du pouvoir. Rien cependant n'a été fait pour mettre fin aux représailles post-conflit ; la détérioration progressive de la sécurité a fait place à de nouvelles menaces différentes contre les civils.

Limiter les dommages causés aux civils

Dans la plupart des situations mentionnées plus haut, un usage offensif de la force militaire sera nécessaire pour atténuer les menaces physiques contre les civils. Cela comporte toutefois un risque, celui de causer des dommages aux civils lors des opérations de protection. Plus les menaces pesant sur la population sont importantes, plus l'emploi de la force va s'imposer pour affronter les auteurs, et plus le danger pour les civils est grand.

Le risque de dommages peut être limité par l'adoption et la mise en œuvre d'une politique, d'outils et de pratiques de limitation des dommages. Par exemple, même si les forces sont souvent entraînées aux principes de proportionnalité, de distinction et de nécessité du DIH, les acteurs étatiques et les groupes non armés souhaitant protéger la population des dommages doivent aller beaucoup plus loin pour s'assurer de l'effectivité des mesures dès le début du conflit. La protection exige une planification et une tactique avancées pour inciter les commandants militaires et les soldats à se demander non pas « est-ce que je *peux* appuyer sur la détente ? » (est-ce conforme au DIH ?), mais plutôt « *devrais*-je appuyer sur la détente ? » (selon les principes de limitation des dommages causés aux civils, est-ce la meilleure option, quelle sont les exigences éthiques et stratégiques, existe-t-il une meilleure façon ?), voire « comment *empêcher* mon ennemi d'appuyer sur la détente ? » (selon les principes de protection proactive, puis-je empêcher de causer des dommages aux civils ?)

La planification de pré engagement peut inclure, sans s'y limiter, les activités suivantes : évaluer les dommages collatéraux potentiels dans un cadre restrictif ; adopter des règles d'engagement limitant les dommages causés aux civils ; entraîner les forces dans un esprit de protection des civils ; se doter d'armes non létales à employer dès que possible ; s'assurer de l'existence de pratiques de ciblage strictes et appropriées ; enfin et surtout, mettre en place des systèmes de collecte et d'analyse des données, des capacités d'enquêtes et réparer les torts subis[12].

Toutes ces activités doivent être effectuées *avant* le début des opérations. Lorsque de nouveaux enseignements sont tirés, les recommandations des commandants, les règles d'engagement et les autres directives devraient être révisées et intégrées aux instructions et aux entraînements dispensés en cours de mission.

Au cours des opérations
Comprendre la réalité des civils pendant le conflit

Pour s'assurer que la force employée par un acteur armé protège effectivement les civils, les commandants militaires doivent comprendre, en temps réel, de quelle manière les dommages sont infligés. Une force militaire devrait disposer en permanence d'une petite équipe chargée de conseiller le commandant sur la protection des civils. Il est important dans cette équipe de développer la capacité à suivre en permanence, dans une base de données centralisée, tous les dommages causés aux civils et, par une analyse systématique des informations, de déterminer les tendances et les défis et d'en tirer des leçons[13]. Concept relativement nouveau dans l'art de faire la guerre, la "cellule de suivi" est généralement composée de plusieurs personnels experts et équipée du matériel et des logiciels appropriés au suivi et à l'analyse des données. C'est en incorporant cette analyse à la boucle de retour d'expérience du commandant que les défis de la protection pourront être surmontés. La tactique peut être ajustée pour améliorer la protection et des exercices sur le théâtre peuvent être mis en place pour s'assurer que les soldats disposent d'outils de protection actualisés pour, *in fine*, sauver plus de vies. De même, des enquêtes correctement conduites à chaque épisode comportant des victimes civiles potentielles permettent aux forces militaires d'acquérir des données cruciales sur les menaces pesant sur la population. C'est ce que l'OTAN a mis en pratique en Afghanistan.

En 2008, la FIAS, la mission de sécurité dirigée par l'OTAN en Afghanistan, a créé la *Civilian Casualty Tracking Cell* (CCTC), une cellule chargée du suivi des victimes civiles, la première du genre tous conflits confondus. La cellule fonctionnait initialement comme une simple base de données. La procédure SOP 307 publiée en juillet 2009 émettait des recommandations sur la réponse à apporter face aux victimes civiles à l'aide d'une liste de vérification, ou « *drill de combat* » comme l'appellent les commandants militaires. En renforçant le rôle de la cellule, la procédure l'a confortée comme « base de données faisant autorité concernant les victimes civiles sur le théâtre des opérations en Afghanistan[14] ». En 2011, la cellule était devenue essentielle à la FIAS pour comprendre les dommages causés aux civils et les réponses à apporter. Elle fut alors renommée *Civilian Casualty Mitigation Team*, afin de refléter plus précisément l'ampleur formelle et fonctionnelle qu'elle avait gagnée[15].

Il existe un paramètre aussi important, mais plus difficile à évaluer : le degré selon lequel les actions de l'OTAN améliorent la protection des civils contre des acteurs armés qui les attaquent délibérément. Plusieurs méthodes permettent d'évaluer la protection physique des civils contre les auteurs de violence[16]. Au-delà du simple suivi des dommages causés aux civils, la mission doit surveiller le comportement de ces derniers, leur perception de la sécurité, les glissements de contrôle sur le territoire, l'acheminement de l'aide humanitaire et les capacités des auteurs.

L'adéquation d'une mesure est fonction du type de menace, cela va sans dire. Il est, par exemple, vain de sonder l'opinion publique quand des pans entiers de la population sont assassinés (c'est-à-dire, lors d'un génocide). Il est également peu utile de se pencher sur les pertes civiles si les personnes sont enlevées ou déplacées en nombre. Ce qui est particulièrement important du point de vue de la planification militaire et de l'exécution, c'est la surveillance des *capacités* de l'agresseur. Les réduire permet de toute évidence de surveiller la protection proactive des civils et la capacité de l'auteur à intensifier ses actions.

La seule véritable façon de savoir si les civils sont effectivement protégés est de mesurer leurs souffrances et de les comparer au résultat attendu si les auteurs de violence arrivaient à leur fin en l'absence de tout effort de protection. Une solution certes difficile à appliquer, mais qui peut être mise en place en évaluant le mode opératoire de l'auteur et les données empiriques issues des conflits précédents où des situations semblables se sont présentées. Par exemple, au cours des génocides passés, plus de la moitié du groupe ciblé de la population a été tué. Quelque 80 pour cent des Africains herero ont été massacrés en Namibie (1904), chiffre qui s'élève à environ 67 pour cent pour les juifs européens pendant l'Holocauste et à environ 75 pour cent pour les Tutsis du Rwanda (1994). En comparaison, seul un faible pourcentage de la population ciblée est susceptible d'être éliminé lors d'un nettoyage ethnique. En revanche, une vaste majorité de la population (plus de 90 pour cent) sera vraisemblablement déplacée soit temporairement (comme les Albanais du Kosovo) soit de façon permanente (comme dans le cas de nombreux musulmans qui vivaient dans les régions de Bosnie tombées aux mains des Serbes).

Traiter les dommages causés aux civils

Tous les dommages causés aux civils résultant des actions de l'OTAN devraient faire l'objet d'une enquête exhaustive. Les cas avérés de violation du droit international devraient être poursuivies par les voies juridiques correspondantes. S'il est déterminé que les dommages causés aux civils, incluant les dommages matériels, la mort ou les blessures, entrent dans les limites des règles d'engagement de la force de maintien de la paix, et qu'ils sont donc accidentels, ils devraient alors être reconnus. Les personnes ou les communautés doivent être assistées en conséquence. Réparer les torts infligés dans le périmètre légal des opérations contribue au respect de la dignité humaine et apaise les communautés. Du point de vue stratégique, la reconnaissance des dommages et la réponse qui leur est apportée limitent l'hostilité suscitée quand la souffrance est ignorée. La reconnaissance des torts peut se manifester par des excuses et des gestes valorisants ou encore par une aide en nature, dans le respect de la culture locale et selon les préférences de la victime.

Dès le début du conflit, plusieurs pays fournisseurs de contingents versaient des indemnités aux familles touchées par leurs actions sur le théâtre des opérations. Or il

n'existait pas de directives standardisées communes à l'OTAN. Les civils ont donc été indemnisés différemment en fonction du pays à l'origine des dommages, ce qui a engendré la confusion et la colère parmi la population civile[17]. En août 2010, les membres de l'OTAN ont approuvé les *Non-binding Guidelines on Monetary Payments for Civilian Casualties in Afghanistan* établies afin de rationaliser les efforts des pays fournisseurs de contingents au moment de réparer les dommages qu'ils avaient causés eux-mêmes aux civils. Quoique non contraignants, ces principes directeurs ont contribué de manière exceptionnelle à aligner les pratiques des pays à l'égard des civils touchés par les opérations de combat. Mais si leur effet s'est révélé positif en Afghanistan, ces principes doivent néanmoins être incorporés dans la politique permanente ou dans des procédures de l'OTAN. En Libye, les victimes civiles de la campagne aérienne de l'OTAN ont réclamé des paiements, mais en l'absence d'une politique établie sur cette question, leur demande n'a pas été entendue.

Après les opérations
Tirer les leçons des conflits passés

L'une des pratiques les plus importantes qu'une force militaire puisse mettre en place à l'issue d'un conflit est la collecte des meilleures pratiques et des enseignements identifiés. Les leçons ne pourront être apprises que si des ajustements stratégiques, opérationnels et tactiques sont intégrés à une politique et à une procédure permanentes, afin de garantir de meilleurs résultats lors du conflit suivant. L'OTAN conduit depuis plusieurs années son propre processus d'identification des leçons qui inclue la publication de rapports sur la Libye et l'Afghanistan et un effort constant de cartographie des capacités de protection des civils.

Il convient de noter également que la simple transposition des leçons d'un théâtre d'opérations à l'autre, sans ajustement relatif à la spécificité de la menace, comporte un danger. Ceci est *a fortiori* vrai pour les leçons retenues sur l'emploi proactif de la force dans le but de protéger, où les menaces sur les civils et l'utilité des différentes réponses militaires peuvent varier considérablement. Les enseignements directs sont utiles uniquement quand les menaces contre les civils sont identiques à celles du conflit où la leçon a été identifiée. Par conséquent, pour garantir une efficacité maximale, les leçons doivent être examinées, modifiées et appliquées au sein d'un conflit et d'un contexte existant.

Conclusion

Tant que des guerres sont menées parmi ou contre les civils, voire pour les défendre, la capacité à les protéger restera essentielle[18]. De nouvelles opérations potentielles, dans lesquelles la protection des civils sera un facteur important, se dessinent,

comme en Syrie, en Irak, ou à nouveau en Libye. L'OTAN devrait donc développer sa capacité de planification et de mise en œuvre effective des stratégies de protection.

Élaborer une capacité de réponse pour une protection effective nécessite une bonne compréhension de la protection des civils et une approche stratégique du développement des capacités sur le théâtre des opérations. L'OTAN devrait étendre ses capacités de planification, de préparation, d'exécution et d'évaluation des missions futures, que la protection des civils soit l'objectif premier ou qu'elle soit imposée par des considérations stratégico-militaires. Le succès de des prochains efforts de l'Organisation en dépend.

Notes

1. WILLIAMS, Paul, « Enhancing Civilian Protections in Peace Operations: Insights from Africa », *Africa Center Research Paper no1*, Washington, DC : Africa Center for Strategic Studies, 20 septembre 2010, http://africacenter.org/wp-content/uploads/2010/09/ACSS-Research-Paper-1.pdf.

2. D'après les recherches menées pendant 10 ans par le CIVIC, sur la base des informations collectées sur les perceptions, les désirs et les besoins des civils. Les travaux ont été menés en Irak, en Syrie, en Afghanistan, en Somalie, au Pakistan et au Mali, etc.

3. Headquarters, Department of the Army, « *Army Tactics, Techniques, and Procedures (ATTP) 3-37.31, Civilian Casualty Mitigation* », juillet 2012, 1-8, para. 1-43, https://fas.org/irp/doddir/army/attp3-37-31.pdf

4. Organisation du traité de l'Atlantique Nord, «*Allied Joint Doctrine for Counterinsurgency (COIN), - AJP-3.4.4*», 2011, https://publicintelligence.net/nato-allied-joint-doctrine-for-counterinsurgency/.

5. La protection des civils face aux actions de l'OTAN, plus communément désignée par les termes de limitation des dommages causés aux civils (*Civilian Harm Mitigation*, ou CHM), est une composante très importante du concept plus global de protection des civils, mais l'OTAN a historiquement utilisé ces deux définitions de façon interchangeable.

6. GASTON, E.L., WRIGHT, Rebecca, *Losing the People: The Costs and Consequences of Civilian Suffering in Afghanistan*, Campaign for Innocent Victims in Conflict (CIVIC) Conflict Series, Washington DC : CIVIC, 18 février 2009, http://civiliansinconflict.org/wp-content/uploads/2017/09/losing-the-people_2009.pdf.

7. GIFFEN, Alison, *Addressing the Doctrinal Deficit: Developing guidance to prevent and respond to widespread or systemic attacks against civilians*, Rapport d'un atelier d'experts internationaux, 21-24 septembre 2009, Washington DC : The Henry L. Stimson Center, 2010, www.stimson.org/sites/default/files/file-attachments/1_-_Addressing_the_Doctrinal_Deficit_2010.pdf.

8. WILLIAMS, Paul, « *Enhancing Civilian Protections in Peace Operations* ».

9. Le FFI, l'établissement norvégien de recherches pour la défense, a développé des recommandations pour les personnels militaires sur la façon dont les principales considérations relatives à la protection des civils peuvent être intégrées à un processus régulier de l'OTAN de planification militaire. Voir BEADLE, Alexander W., KJEKSRUD, Stian, « *Military planning and assessment guide for the protection of civilians* », FFI-rapport 2014/00965, Kjeller : Norwegian Defence Research Establishment, 2014.

10. *Id.*

11. GORUR, Aditi, *Community Self-Protection Strategies : How peacekeepers can help or harm*, Civilians in Conflict Issue Brief no 1, Washington DC : The Henry L. Stimson Center, août 2013, www.stimson.org/sites/default/files/file-attachments/Stimson_Community_Self-Protection_Issue_Brief_Aug_2013_0.pdf.

12. La réparation des torts infligés est la pratique des parties belligérantes selon laquelle elles reconnaissent les dommages causés aux civils dans le périmètre légal des opérations, sans pour autant avoir l'obligation de le faire. La pratique de réparation des torts est en soi un geste de respect pour les victimes. Les dédommagements, qui peuvent prendre des formes variées, doivent respecter la culture locale. Ils peuvent inclure des excuses publiques, des paiements d'argent, des programmes de moyens de subsistance ou d'autres gratifications, selon les besoins et les préférences des victimes.

13. Deux méthodes, différentes, mais reliées entre elles, de documentation des dommages causés aux civils dans les conflits armés sont progressivement appliquées comme bonnes pratiques par les militaires du monde entier : le « suivi des dommages causés aux civils », et l'« enregistrement des victimes ». L'enregistrement des victimes consiste à consigner de façon systématique et continue chaque personne tuée par la violence armée (ce qui comprend, sans s'y limiter, le conflit armé conformément à la définition du DIH). Le suivi des dommages causés aux civils désigne la collecte et l'analyse systématiques par la partie belligérante elle-même (militaires d'état, soldat de la paix, membres d'une coalition militaire) des données relatives à ses opérations et aux impacts sur la population civile, incluant des données sur les pertes civiles, les blessures, les dommages matériels et autres préjudices infligés à la population, selon le cas. Le suivi des données permet ensuite d'utiliser le résultat de l'analyse pour réviser la tactique et l'entraînement de la partie belligérante, afin de réduire les dommages causés aux civils dans les opérations futures, d'assurer des enquêtes approfondies et de permettre aux parties au conflit de répondre de façon appropriée aux dommages infligés, en accordant un dédommagement pour les pertes subies. L'enregistrement des victimes civiles et le suivi des dommages sont tous deux nécessaires et utiles en ce qu'ils visent à reconnaître le préjudice subi par les victimes et leur famille, à informer les différents acteurs cherchant à réparer les dommages et à renforcer la protection. De plus, les informations issues des deux approches sont, dans la mesure du possible, combinées pour offrir une vision plus complète des dommages causés aux civils.

14. KEENE, Jennifer, *Civilian Harm Tracking: Analysis of ISAF Efforts in Afghanistan*, Campaign for Innocent Victims in Conflict (CIVIC), Washington DC : CIVIC, 2014, http://civiliansinconflict.org/uploads/files/publications/ISAF_Civilian_Harm_Tracking.pdf.

15. *Id.*

16. BEADLE, Alexander W., VÅGE, Anders S., «*Assessing Protection of Civilians in Military Operations*», FFI-rapport 2014/00966, Kjeller : Norwegian Defence Research Establishment, 2014.

17. GASTON, WRIGHT, *Losing the People*.

18. BEADLE, « Protection of Civilians as a New Objective for Military Forces » in *International Military Operations in the 21st Century: Global trends and the future of intervention*, Norheim-Martinsen, P. M., Nyhamar T., dir., New York : Routledge, 2015, pp. 195–205.