

RESEARCH ARTICLE

Tournant dans la conception du terrorisme et de l'anti-terrorisme aux Etats-Unis d'Amérique après le 11 Septembre 2001: Heurts et lueurs



HENRY LUKETU MBIYA

Docteur en sécurité intérieure (USA) | Master of Business Administration, in Finance and Accounting (USA) | Professeur

RÉSUMÉ

Les attentats du 11 septembre 2001 aux Etats-Unis d'Amérique ont marqué un tournant dans la lutte contre le terrorisme, entraînant une intensification des actions militaires et un renforcement des mesures de sécurité, tout en soulignant la complexité et les défis d'une telle lutte à l'échelle mondiale. A la suite de ces attentats, un bouleversement des stratégies sécuritaires a marqué le passage vers un terrorisme transnational et décentralisé. Les États-Unis d'Amérique ont déclaré une guerre contre le terrorisme, avec des opérations militaires en Afghanistan (pour déloger Al-Qaïda et les talibans) et en Iraq (pour renverser Saddam Hussein). L'ONU a joué un rôle crucial en adoptant la résolution 1373 pour lutter contre le terrorisme, et des alliances internationales se sont formées pour mener des actions conjointes. La guerre antiterrorisme a eu des conséquences profondes, notamment en termes de coûts humains et financiers, mais aussi en termes de respect des droits humains et de stabilité politique.

Mots clés : Terrorisme, antiterrorisme, stratégies sécuritaires, coordination internationale

A Turning Point in the Conceptualization of Terrorism and Counterterrorism in the United States After September 11, 2001: Clashes and Glimmers of Hope

ABSTRACT

The September 11, 2001 attacks in the United States of America marked a turning point in the fight against terrorism, leading to an intensification of military action and a strengthening of security measures while also highlighting the complexity and challenges of combating terrorism on a global scale. In the aftermath of the attacks, security strategies underwent a major shift in response to increasingly transnational and decentralized terrorism. The United States declared a war on terror and launched military operations in Afghanistan to dislodge Al-Qaeda and the Taliban and in Iraq to overthrow Saddam Hussein. The United Nations played a crucial role by adopting Resolution 1373 to combat terrorism, while international alliances were formed to conduct joint operations. The war on terror has had profound consequences in terms of human and financial costs, respect for human rights, and political stability.

Keywords: Terrorism, counterterrorism, security strategies, international coordination

HOW TO CITE

Luketu H. Mbiya (2026). Tournant dans la conception du terrorisme et de l'anti-terrorisme aux Etats-Unis d'Amérique après le 11 Septembre 2001: Heurts et lueurs. *East African Journal of Crime and Security*, 2(1), 35–46.
<https://doi.org/10.66699/3b7dbv60>

Open access under the Creative Commons Attribution 4.0 International license: creativecommons.org/licenses/by/4.0/

Introduction

Les attentats du 11 septembre ont marqué un tournant dans la politique antiterroriste à travers le monde. Ils ont fait prendre pleinement conscience aux nations de la présence et de l'ampleur de la menace terroriste, et soulignent tragiquement l'évolution de l'image de la violence politique et de la communauté internationale. Le terrorisme est devenu la principale menace pour la sécurité mondiale et la stabilité de l'ordre international depuis des décennies (Alexander, 2002). Ainsi, les premières années du 21ème siècle sont marquées par la « guerre contre le terrorisme ». Même l'État le plus puissant du monde, après avoir remporté la guerre froide, considère aujourd'hui le terrorisme, à tort ou à raison, comme la menace la plus grave pour sa sécurité nationale et ses intérêts stratégiques. Ainsi, d'une certaine manière, le terrorisme façonne les politiques nationales et internationales au plus haut niveau. Les terroristes opèrent actuellement à l'échelle mondiale et ont même la possibilité d'influencer directement les processus politiques des démocraties libérales (comme le démontrent les conséquences des attentats du 11 mars à Madrid).

Cependant, le futur défi terroriste exige donc une détermination tout aussi grande que celle qui a été nécessaire pour combattre le nazisme et le fascisme au siècle dernier. Malheureusement, le terrorisme n'a pas d'origine précise, on l'appelle seulement « terrorisme ». Le terrorisme n'est pas un groupe de personnes, une organisation, ni même un ensemble d'intérêts. Il sert et continuera de servir des objectifs divers et sera toujours façonné par divers conflits et facteurs. Il peut être comparé à un virus en constante évolution, aux multiples variantes, car il pénètre les sociétés et utilise leur système immunitaire contre elles-mêmes. Il est donc nécessaire d'examiner les aspects les plus importants et les plus controversés de la lutte antiterroriste dans le contexte du nouveau terrorisme transnational post-11 septembre 2001.

La Définition Problematique du Terrorisme et de la Lutte Contre le Terrorisme

La définition universelle du terrorisme et de sa lutte reste profondément problématique en raison de l'absence de consensus international global et de la politisation fréquente du terme. Toutefois, notre compréhension nous pousse d'en définir comme étant l'utilisation de la violence, de la terreur et de l'intimidation à des fins politiques, idéologiques ou religieuses. Il se traduit par des actes criminels (attentats, prises d'otages, assassinats) visant à frapper l'opinion publique et à exercer une pression sur un gouvernement ou une société. Selon White et Steven (2022), la notion de terrorisme et de lutte contre le terrorisme est complexe et fait l'objet de débats intenses parmi les scientifiques, car il n'existe pas de définition universelle du terrorisme, ce qui pose des problèmes pour la lutte contre ce phénomène. Définir le terrorisme, qui peut à première vue ressembler à une démarche académique classique, revêt en réalité une importance fondamentale pour l'efficacité des actions internationales de lutte contre le terrorisme. L'analyse détaillée de ce débat n'est pas le sujet ici, mais il faut être conscient que la question de la définition est l'un des problèmes cruciaux de la lutte contre le terrorisme. Il est indéniable qu'il est très difficile de parvenir à une coopération internationale efficace en l'absence d'une définition universellement acceptée du terrorisme. Malheureusement, l'élaboration d'une telle définition a toujours été impossible, principalement pour des raisons politiques.

Pourtant, le terrorisme constitue une menace transnationale et mondiale qui exige des réponses et des réactions à l'échelle mondiale et internationale. Une coopération véritablement multilatérale et mondiale ne peut réussir sans un langage commun et une définition du terrorisme universellement acceptée et facile à mettre en œuvre. Comme l'a souligné le spécialiste israélien Ganor (2013), « sans répondre à la question de savoir ce qu'est le terrorisme, aucune responsabilité ne peut être imputée aux pays qui soutiennent le terrorisme, ni aucune mesure prise pour lutter contre les organisations terroristes et leurs alliés. »

Même si de nombreux pays ont signé des accords internationaux antiterroristes, ils peuvent toujours affirmer que certains phénomènes ne nécessitent pas leur intervention, car ils ne constituent pas des exemples de terrorisme. Ainsi, la nécessité d'une définition du terrorisme se manifeste à presque toutes les étapes de la lutte contre ce fléau :

- Législation et répression (il n'y a pas de crime sans définition, et nous ne pouvons percevoir/traiter le terrorisme comme un crime ordinaire)
- Coopération internationale

- États soutenant le terrorisme (sans définition claire du terrorisme, il est beaucoup plus difficile de convaincre les États soutenant le terrorisme de rompre leurs liens avec une organisation terroriste ; certains pays recourent encore à l'argument classique selon lequel « les terroristes des uns sont les combattants de la liberté des autres »)
- Actions offensives (« alors que les pays sur la défensive bénéficient naturellement de la sympathie des autres, les pays offensifs sont généralement censurés et critiqués par les autres. Pour garantir le soutien international aux États luttant contre le terrorisme, et peut-être même pour une offensive conjointe, une définition internationalement acceptée du terrorisme est nécessaire, qui distinguera la lutte pour la liberté de l'activité terroriste » ; cette affirmation est particulièrement importante dans le contexte actuel des interventions militaires en Afghanistan et en Irak).
- Attitudes envers une population soutenant le terrorisme (une définition claire et universellement acceptée du terrorisme rendrait plus difficile de brouiller les frontières entre lutte pour la liberté et terrorisme)
- Relations publiques (« une définition séparant le terrorisme des autres actes de violence permettra le lancement d'une campagne internationale visant à saper la légitimité des organisations terroristes, à réduire le soutien qui leur est apporté et à galvaniser un front international uni contre elles. ») analyse également l'attitude des organisations terroristes à l'égard de cette définition, démontrant de manière convaincante qu'une définition universelle du terrorisme pourrait influencer significativement au moins certaines d'entre elles (Ganor, 2013). On comprend ainsi comment l'absence de définition universelle du terrorisme en droit international complique considérablement la lutte contre le terrorisme.

Composantes de la Lutte Antiterroriste

Une politique antiterroriste efficace doit reposer sur un système de filtres fonctionnant à chaque étape des activités terroristes, le « cycle de vie » de ce terrorisme. Une approche unique ne suffit pas à garantir l'efficacité de la politique antiterroriste. Elle doit reposer sur une action bien orchestrée, intégrant un ensemble de composantes essentielles soigneusement coordonnées et calibrées.

Robert Pilar a comparé la politique antiterroriste à la sécurité routière : les gouvernements peuvent et doivent réduire le nombre de morts et de blessés sur les routes sur de nombreux fronts :

- amélioration des normes de résistance aux collisions,
- abaissement des limitations de vitesse, renforcement des patrouilles policières, etc.

Il serait vain de concentrer toutes les ressources, limitées en permanence, sur un seul aspect de la sécurité routière, et la politique antiterroriste est très similaire à cet égard. En cas de terrorisme, les services responsables doivent être prêts à intervenir à trois niveaux :

- prévention (traiter les conditions préalables et les facteurs déclenchants du terrorisme et déjouer les plans terroristes avant qu'ils ne se produisent)
- gestion des incidents (en cas d'échec de la prévention, minimiser la destructivité d'un acte terroriste)
- contrôle des effets (gérer les effets perturbateurs sociaux et politiques du terrorisme)

Il serait donc commode de traiter les cinq principales étapes du « cycle de vie » du terrorisme, et la politique antiterroriste qui doit prendre chacune d'elles en compte :

A. Causes (raisons, racines et principaux facteurs à l'origine du terrorisme).

Le terrorisme n'a pas de cause unique mais résulte d'une convergence complexe de facteurs politiques, sociaux, économiques et idéologiques. D'après Crenshaw (2011), le terrorisme est généralement alimenté par la marginalisation, l'oppression étatique, l'injustice institutionnelle, les conflits prolongés et l'extrémisme religieux ou politique, qui sont exploités par des groupes pour justifier la violence. Ainsi, les autorités et services compétents doivent s'attaquer aux racines du terrorisme à tous les niveaux. Il faut cependant être conscient que le célèbre slogan selon lequel « le véritable problème n'est pas le terrorisme, mais ses racines », et donc qu'il faut « traiter les causes plutôt que les symptômes », est une simplification dangereuse.

Bien sûr, une politique antiterroriste efficace ne peut ignorer la question des causes du terrorisme, et l'idée de soulager une tension à ses racines directes et indirectes, avant que la violence ne se manifeste, semble très tentante. En réalité, ce n'est pas aussi simple qu'il y paraît à première vue.

B. Potentiel

Si les causes du terrorisme ne sont pas éradiquées, l'étape suivante consiste à tenter de contenir les groupes terroristes, par exemple par des activités légales ou des opérations de renseignement. Cet élément crucial de la politique antiterroriste peut potentiellement être très efficace, mais ses effets secondaires peuvent entraîner des restrictions des libertés civiles et, dans des cas extrêmes, l'effondrement du système libéral-démocratique. Cet élément est lié à deux problèmes apparemment contradictoires. Premièrement, les activités terroristes ne requièrent aucune compétence particulière.

C. Intentions

Si les responsables de la politique antiterroriste ne parviennent pas à éliminer ni les fondements du terrorisme ni les opportunités d'activités terroristes, il faille donc tenter d'influencer les intentions des terroristes, c'est-à-dire à les contraindre à renoncer à leurs attentats, même si l'action pourrait être menée successivement. Une telle situation peut être générée de plusieurs manières, mais chacune d'elles est potentiellement gênante : faire des concessions aux terroristes (ce qui accroît le risque d'escalade du conflit et de simulation) ; adopter une politique de non-négociation (ce qui peut discréditer l'engagement de négociations) ; appliquer des sanctions drastiques ou menacer les terroristes de représailles contre la partie de la population au nom de laquelle ils agissent (les dangers sont évidents dans ce cas).

D. Défenses et gestion des effets

Le dernier volet de la politique antiterroriste est la défense directe (généralement par le renforcement des cibles critiques) et la limitation des conséquences d'une attaque. Cela pourrait impliquer davantage de policiers, de militaires ou d'autres forces armées dans les rues, des constructions en béton armé, une protection spéciale des cibles vulnérables, un contrôle renforcé des bâtiments, l'introduction de systèmes de surveillance et d'autres types de protection, tels que des détecteurs de métaux ou d'explosifs. Les problèmes liés à cet élément découlent du fait que ce sont les terroristes qui choisissent le lieu et le moment de l'attaque, alors qu'un pays n'est pas en mesure de protéger toutes les cibles potentielles simultanément.

Cependant, la gestion des effets de la politique antiterroriste implique un équilibre délicat entre les impératifs de sécurité et la préservation des libertés fondamentales. Elle s'appuie sur la prévention, la coopération internationale, et l'adaptation du renseignement, tout en imposant des garde-fous stricts contre les abus et les impacts collatéraux sur la société.

Malgré les difficultés liées à la mise en œuvre des éléments susmentionnés, leur mise en œuvre correcte réduit considérablement le niveau de menace terroriste. La mise en œuvre de ces éléments particuliers doit s'accompagner du recours à des instruments de lutte contre le terrorisme, tels que la diplomatie, le droit pénal, la lutte contre le financement du terrorisme, les moyens militaires et de renseignement, et les opérations spéciales.

Reponses Militaires, Doctrines Preemptives et Droit International : Paradigme N° 1.

Les attentats terroristes de World Trade Center du 11 septembre 2001 à New York ont profondément bouleversé le paysage de la sécurité internationale, entraînant des mutations majeures dans les réponses militaires, l'émergence de doctrines de guerre préemptive et une remise en question profonde des cadres du droit international. Le bilan des interventions post-11 septembre démontre que la recherche d'une sécurité absolue par des méthodes d'exception a souvent produit l'effet inverse : elle a alimenté les récits radicaux, déstabilisé des régions entières et affaibli l'autorité morale du droit international. Aujourd'hui, ce précédent est fréquemment instrumentalisé par d'autres puissances mondiales pour justifier leurs propres actions unilatérales, menaçant l'équilibre multilatéral global.

Cependant, comprendre l'évolution des doctrines militaires de la légitime défense à la préemption, c'est chercher à comprendre le modèle de guerre conventionnelle (État contre État) vers des opérations asymétriques (États contre acteurs non étatiques). C'est pourquoi la doctrine Bush et la guerre préemptive introduite en 2002 a légitimé l'usage de la force non pas face à une menace imminente (concept classique de légitime défense), mais pour prévenir l'émergence d'une menace future. La doctrine préemptive formalisée par l'administration

américaine après les attentats théorise l'action militaire préventive contre les menaces terroristes ou les États dits « voyous » (Michał, 2018). Le droit international a été profondément mis à l'épreuve par cette approche, car la Charte des Nations Unies (notamment l'article 51) restreint historiquement l'usage de la force armée à la stricte légitime défense. L'invasion de l'Irak en 2003 en a été l'application la plus contestée. A partir de la guerre globale contre le terrorisme, le monde est devenu un champ de bataille global sans frontières claires. Les concepts de "combattant ennemi illégal" ont été créés pour contourner le statut traditionnel de prisonnier de guerre. D'après Khadidja (2018), la guerre à distance (guerre par procuration et technologie), face à l'usure des opinions publiques concernant les interventions au sol (boots on the ground), les armées occidentales ont pivoté dès les années 2010 vers l'usage massif de drones armés, de forces spéciales et de frappes chirurgicales (au Pakistan, au Yémen, en Somalie).

Le bilan des interventions majeures et respect des droits humains post-11 septembre était lourd sur le plan humain et juridique, marqué par des dérives documentées par les organisations internationales. En Afghanistan (de 2001-2021), Initialement légitimée par l'ONU, cette guerre de vingt ans s'est conclue par le retour au pouvoir des Talibans. Elle a été marquée par d'importantes pertes civiles ("dommages collatéraux") dues aux frappes aériennes et par l'incapacité à bâtir un État de droit stable. En Irak (2003), menée sans l'aval de l'ONU et sur de faux prétextes (armes de destruction massive), cette guerre a déstabilisé la région, favorisé l'émergence de Daech et provoqué le scandale des tortures à la prison d'Abou Ghraib. Dans les zones de non-droit et la torture, il y a eu la création du centre de détention de Guantánamo et l'existence de prisons secrètes de la CIA (black sites) ont institutionnalisé la détention sans procès et les "techniques d'interrogatoire renforcées" (assimilées à de la torture), en violation directe de la Convention des Nations Unies contre la torture. Enfin, il y avait l'ère des drones et assassinats ciblés dont si les frappes de drones réduisent les risques pour les soldats attaquants, elles posent de graves questions éthiques et juridiques quant à l'absence de procès, le manque de transparence des critères de ciblage et le nombre élevé de victimes civiles non reconnues.

Bref, le bilan des interventions armées post-11 septembre met en lumière une mutation profonde de la stratégie militaire face à la menace asymétrique, souvent au détriment des cadres du droit international et des droits humains. Les attentats de 2001 ont poussé les démocraties occidentales, menées par les États-Unis, à redéfinir la légitime défense et à adapter leurs doctrines à des acteurs non étatiques (groupes terroristes).

Lutte contre les Réseaux Terroristes. Paradigme N° 2.

Lutter efficacement contre les réseaux terroristes exige une approche globale et multidimensionnelle, allant du renseignement à la cybersécurité en passant par l'assèchement de leurs sources de financement. Les stratégies s'articulent autour de plusieurs piliers majeurs:

A. Renseignement et Coopération Internationale

- Partage d'informations : La coordination entre les services de renseignement nationaux et internationaux (comme via Interpol) est essentielle pour suivre les déplacements des combattants étrangers et déjouer les attentats.
- Démantèlement des cellules : Neutraliser les réseaux de soutien logistique, les filières de recrutement et les caches d'armes.

B. Cybersécurité et Lutte en Ligne

- Contrôle des contenus : Les groupes terroristes exploitent les réseaux sociaux et le dark web pour la propagande et la radicalisation. La modération et le retrait des contenus illicites sont renforcés par des réglementations (comme en Europe).
- Contre-discours : Produire des récits alternatifs pour contrer l'idéologie extrémiste et décourager les candidats au départ.

1) Utiliser les technologies de l'information à trois fins offensives :

La gestion de l'image et la propagande (l'efficacité de cette approche est démontrée par les activités terroristes en Irak) ; les attaques perturbatrices (frappes électroniques qui désactivent temporairement, sans toutefois détruire, les infrastructures physiques et/ou virtuelles) ; et les attaques destructrices (cyberterrorisme).

2) Déstabiliser le financement du terrorisme

Déstabiliser le financement du terrorisme repose sur une stratégie internationale globale appelée lutte contre le financement du terrorisme (LFT), qui vise à couper les ressources financières des réseaux terroristes en ciblant leurs sources de revenus, leurs canaux de transfert et leurs dépenses. Cela passe par le suivi des flux financiers, la surveillance des réseaux informels et la régulation des technologies modernes. Williams (2023) dans son article « Récupérer les revenus d'Al-Shabaab », déclare que pour couper les revenus annuels d'Al Shabaab, estimés à 100 millions de dollars et générés par les extorsions, il faudra rétablir l'intégrité des agences financières, judiciaires et de renseignement de la Somalie. Ainsi donc, la lutte contre le financement du terrorisme regorge entre autres l'évolution des normes du Groupe d'Action Financière (GAFI), la régulation des cryptomonnaies et les actifs numériques, la lutte contre le blanchiment et l'encadrement des transferts informels. C'est pourquoi les normes du GAFI ont évolué pour imposer une régulation stricte des actifs numériques et de la lutte contre le blanchiment d'argent.

Les normes du GAFI se penchent à l'élargissement de recommandations pour couvrir les actifs virtuels (AV) et les prestataires de services d'actifs virtuels (PSAV) ; à la règle du voyage (Travel Rule) qui oblige les prestataires à transmettre les informations sur l'émetteur et le bénéficiaire lors des transferts de cryptomonnaies ; et à la surveillance accrue afin de cibler les risques émergents comme la finance décentralisée (DeFi), les portefeuilles non hébergés (unhosted wallets) et les transactions de pair à pair (P2P) (GAFI, 2025; Financial Crime Academy, 2026).

Cependant, en ce qui concerne la régulation des cryptomonnaies et actifs numériques, au niveau international, les États sont recommandés d'adapter leurs lois nationales pour exiger l'enregistrement ou l'agrément des plateformes d'échange de cryptomonnaies, alors qu'au niveau de la Régulation régionale, l'Union européenne déploie le règlement sur les marchés des crypto-actifs (Markets in Crypto-Assets ou MiCA) pour harmoniser la conformité des acteurs du secteur. La lutte contre le blanchiment et transferts informels a opté d'abord pour l'approche par les risques, en poussant les institutions à appliquer des obligations de vigilance à l'égard de leurs clients et déclare les transactions suspectes, ensuite pour les transferts informels, renforcer la surveillance des réseaux de type hawala ou les transferts de fonds non déclarés afin de couper les canaux de financement du terrorisme.

En cette matière, Borlant-Clément (2021) déclare que jusqu'à ce jour, la réglementation LCB-FT a largement échappé à une analyse nationale parce que les travaux sur la compliance l'en ont exclue en postulant la puissance économique des entités assujetties ou leur dimension transnationale, alors qu'une grande partie des professionnels concernés par la LCB-FT ne sont ni puissants ni transnationaux, et parce qu'elle s'est largement construite dans l'émotion en réaction à des événements marquants.

Efficacité du Système de Renseignement et Prévention

Les attentats du 11 septembre 2001 ont révélé de graves failles dans le partage des informations entre les services de renseignement américains, entraînant une refonte majeure de la sécurité mondiale et de la prévention antiterroriste (Ramos, 2019). L'échec du système de renseignement le plus puissant au monde à prévenir les attentats du 11 septembre a été un véritable choc pour l'opinion publique américaine et occidentale. Bien que des réformes des structures de renseignement soient nécessaires, même les services de renseignement les plus performants auront probablement une efficacité relativement limitée comme instrument de lutte contre le terrorisme (Betts, 2002). Comme l'a déclaré. Les attaques ont pris au dépourvu une communauté du renseignement fragmentée et opaque, incapable de relier les signaux d'alerte. L'auteur montre que les structures ont du mal à surmonter leurs divisions historiques et bureaucratiques profondes, rappelant les difficultés structurelles déjà observées après Pearl Harbor (Ramos, 2019). Face à l'émoi national, la pression politique et médiatique a exigé une refonte globale pour unifier et centraliser les agences de sécurité et du renseignement pour leur efficacité.

Etant donné que ces attentats ont pris de court l'administration américaine et, ainsi, posé la question de l'efficacité de la communauté du renseignement, le pouvoir a commandité plusieurs enquêtes afin d'identifier, puis rectifier les dysfonctionnements du système de renseignement. Ces démarches ont mis en lumière un certain nombre de failles structurelles, et ont engendré une réforme en demi-teinte, conclue à la hâte. Les dissensions au sein de l'administration n'ont pas permis d'aboutir à des changements d'ampleur conformes aux préconisations des

commissions. Néanmoins, l'ensemble du processus de réforme permet de mettre en évidence la primauté du pouvoir politique dans l'organisation, les activités et les dysfonctionnements du renseignement.

Si les attentats de 2001 ont attiré l'attention des pouvoirs publics et de l'opinion sur la communauté du renseignement, cette dernière s'est également affirmée comme un instrument indispensable pour faire face à cette surprise stratégique (Damien, 2022). Il s'agissait en effet de confondre les commanditaires de ces attaques coordonnées et de comprendre comment une telle opération avait pu être conduite sur le territoire national. Pour les cadres de la CIA, la responsabilité d'Oussama Ben Laden et d'Al-Qaïda s'est rapidement imposée comme une évidence. Cette piste a pu être étayée dans les heures qui ont suivi l'effondrement des tours du World Trade Center, lorsque les analystes de la CIA sont parvenus à identifier dans les listes de passagers des avions détournés au moins deux individus liés à l'organisation terroriste.

Toutefois, après chaque échec du renseignement, de nombreux experts, journalistes et politiciens prônent avec vigueur des formes de réorganisation radicale. Cependant, ces réformes, bien que souvent nécessaires, génèrent toujours des effets secondaires et n'empêcheront pas le renseignement de connaître des échecs à l'avenir. L'un des problèmes majeurs du renseignement est qu'il recueille une quantité considérable d'informations fragmentaires, indirectes ou ambiguës (Betts, 2004). L'excès d'informations rend la compréhension de ce qui est quoi extrêmement difficile, même avec les technologies les plus avancées. Il est également difficile de distinguer l'information de la désinformation, ce qui peut être particulièrement dangereux.

Les services de renseignement devraient être améliorés, mais il s'agit d'un processus continu et très coûteux qui, surtout, n'empêchera pas les défaillances catastrophiques. La stratégie antiterroriste ne peut pas se limiter à la prévention : la gestion des conséquences doit également être prise en compte. La responsabilité des services de renseignement ne se limite pas à la prévention. Lorsqu'une attaque se produit, ils doivent coopérer avec les forces de l'ordre pour identifier et traquer les auteurs et, éventuellement, organiser des opérations secrètes pour les capturer ou les exterminer. Ceci, entre autres, appelle une discussion sur les assassinats comme outil de lutte contre le terrorisme, qui ne sera pas analysée dans ce texte.

Négociations, Concessions, Apaisement

Si toute réaction trop hâtive, hystérique, inconsidérée ou unilatérale au terrorisme constitue un danger évident pour la stabilité internationale, un autre extrême peut s'avérer tout aussi déstabilisateur et dangereux. L'absence de réaction ou l'insuffisance de réaction, l'évitement de la confrontation à tout prix ou les concessions aux terroristes peuvent déshonorer l'institution de l'État, donner aux terroristes un sentiment d'impunité et aboutir à leur propagande et à leur victoire politique. Une politique égoïste, excessivement prudente et lente des gouvernements pourrait sérieusement entraver la construction de coalitions et d'alliances antiterroristes multilatérales plus larges, ce qui suscite une suspicion internationale et une préférence pour une action unilatérale, menée de manière isolée et en violation du droit international.

Céder aux exigences des terroristes est tout aussi dangereux que tolérer leur présence et leurs actions sur son propre territoire. Évidemment, dans certains cas, la stratégie du « sans concession » ne peut être appliquée avec rigueur, notamment lorsqu'une crise risque de se solder par un nombre considérable de morts parmi les otages ou d'autres innocents. D'autre part, il convient de rappeler que satisfaire aux exigences des terroristes peut entraîner une escalade de la violence et, par conséquent, une augmentation du nombre de victimes. En temps de crise, les exigences sont généralement de nature tactique ou opérationnelle et impliquent une rançon et/ou la libération de compagnons de prison des terroristes.

Face au grave danger pour la vie de l'otage et à l'inévitable médiatisation de la situation, les autorités peuvent être contraintes à des concessions qui seraient bien plus difficiles à accorder dans le cas d'exigences strictement politiques. Bien que les dilemmes des gouvernements dans des situations similaires soient très complexes et que les négociations (qui n'impliquent pas toujours des concessions) puissent être autant que possible judicieuses pour le bien des otages, il ne faut pas oublier que céder aux terroristes constitue une menace sérieuse. Les extrémistes perçoivent cela comme une faiblesse des structures étatiques et sont encouragés à commettre de nouvelles attaques et à développer le potentiel humain et matériel des groupes terroristes. Comme l'a noté Wilkinson (2004) « étant donné la grande valeur que nous accordons à chaque vie individuelle, il existe un besoin naturel de céder aux exigences des terroristes afin de sauver la vie des otages. Mais imaginez qu'en cédant si facilement au chantage terroriste, nous encourageons davantage de prises d'otages, mettant ainsi en danger de

nombreuses autres vies ? Parfois, les terroristes exigent des changements de politique ou de loi : est-il moralement juste d'opérer de tels changements pour apaiser les terroristes ? Les gouvernements ont une responsabilité envers l'ensemble de la société. Ils sont responsables non seulement de la vie des otages ou des victimes potentielles, mais aussi de la sécurité stratégique, de la crédibilité et de la stabilité de leurs pays respectifs.

La tolérance manifestée par divers pays envers les terroristes en échange d'une sécurité (souvent illusoire) est l'un des principaux obstacles au développement d'une politique antiterroriste cohérente et homogène à l'échelle internationale. Cela donne souvent lieu à des accusations mutuelles, à des animosités et à des conflits. Dans certaines régions du monde, le terrorisme est un outil régulier de la politique internationale, et il est difficile de distinguer entre le soutien actif au terrorisme et la tolérance à l'égard des activités terroristes, ou le fait de permettre aux terroristes d'agir sur son propre territoire à des fins politiques. Cette dernière option peut parfois impliquer une tentative d'« immuniser » l'État contre les attaques terroristes, mais elle peut aussi révéler la faiblesse et le manque de pouvoir des structures étatiques. De telles pratiques, bien qu'efficaces à l'échelle individuelle, sont incontestablement préjudiciables à la stabilité internationale.

Il faut garder à l'esprit qu'abriter les terroristes et tolérer leurs activités (y compris leurs activités de propagande au nom de la démocratie) engendre inévitablement des conflits internationaux et attire les ennemis des extrémistes (y compris les services de renseignement étrangers et autres groupes extrémistes). Ainsi, se soucier de sa propre sécurité peut engendrer une menace encore plus grande. Les terroristes sont généralement conscients de ces dilemmes et exploitent la peur, l'égoïsme, l'animosité mutuelle de certains pays, la méfiance et la réticence à partager l'information, caractéristiques des services de renseignement, ainsi que la réticence des gouvernements à partager leur indépendance.

Dans des discours de nombreux pays, on entend le slogan : « On ne négocie jamais avec les terroristes ». En réalité, pourtant, les négociations et, malheureusement, l'apaisement semblent monnaie courante. À la question de savoir si les gouvernements doivent négocier avec les terroristes et leur faire des concessions, la réponse est, encore une fois : cela dépend.

Armes de Destruction Massive (ADM) et Terrorisme

Les armes de destruction massive (ADM) sont des armes non conventionnelles capables d'infliger des pertes humaines et matérielles à très grande échelle. Elles se classent principalement en quatre catégories, couramment désignées par l'acronyme NRBC : Nucléaire, Radiologique, Biologique et Chimique. Les derniers développements technologiques augmentent le risque que des acteurs terroristes aient accès à des armes NRBC (Gregory, 2020). Il y a lieu de comprendre aisément l'inquiétude que peut susciter l'idée que des terroristes puissent utiliser ces armes. Ces armes, associées au terrorisme font l'objet de nombreuses analyses stratégiques, juridiques et géopolitiques. Contrairement aux attaques traditionnelles, l'État islamique ne revendique généralement pas la responsabilité des actes terroristes commis avec des armes NRBC : il semble que Daech, durant la période où il contrôlait un vaste territoire, ne voulait pas perdre de soutien à cause de cela, compte tenu de l'indignation que les images des attaques chimiques pendant la guerre civile en Syrie avaient provoquée dans l'opinion publique (Ilaria, 2021). Cependant, dans l'ère post-califat, les contraintes liées à la nécessité de l'unité se sont estompées. Le passage du califat physique au virtuel, a permis la fragmentation des identités qui se renforcent dans les communautés locales : la décentralisation de la propagande a créé de nouvelles possibilités de participation pour les individus (Krona, 2020). Ce constat de Michael Krona met en lumière une mutation fondamentale de la stratégie des groupes terroristes ou extrémistes, particulièrement illustrée par l'évolution de l'État islamique (Daech) après la perte de son territoire en Irak et en Syrie. En outre, Briglia (2021), argumente que le web et les réseaux sociaux offrent des possibilités infinies de radicalisation, généralement sous la forme d'un terrorisme de bricolage, qui peut inclure l'utilisation d'armes NRBC. Les attaques sont planifiées et contrôlées à distance sur des plateformes en ligne, tandis que l'acte extrême est exécuté physiquement par des sympathisants formés virtuellement dans le monde entier. Ce n'est pas une coïncidence si les tentatives d'utilisation d'armes biologiques précédemment signalées en Europe en 2018 ont été précédées d'une phase de radicalisation en ligne.

À l'avenir, cela pourrait conduire à une percée décisive des barrières technologiques, stratégiques et morales. Bien que les terroristes aient prouvé qu'ils pouvaient causer des pertes massives sans recourir aux ADM (et, d'un autre côté, le recours aux ADM n'est pas nécessairement lié à de telles pertes), la menace du terrorisme par ADM

doit rester un sujet d'intérêt pour la lutte antiterroriste, aujourd'hui comme demain. Les analystes s'accordent généralement à dire que le terrorisme par ADM est une menace peu probable, mais aux conséquences graves (Schweitzer, 2020). Cela pose un autre dilemme en matière de lutte antiterroriste : combien de ressources, intrinsèquement limitées, devraient être allouées à la prévention de ce type de menaces sans compromettre l'efficacité sur d'autres fronts. Bien sûr, les gouvernements devraient disposer de plans pour faire face à une catastrophe (comme des plans d'évacuation et d'autres éléments de « gestion des conséquences »). Mais cela pourrait créer un autre problème : des discussions trop ouvertes et des exercices de lutte antiterroriste pourraient encourager les terroristes à perpétrer certains types d'attaques. Cela pourrait également favoriser des phénomènes d'imitation et une épidémie de fausses menaces, susceptibles de semer la panique ou de provoquer le syndrome du « cri au loup » déjà évoqué. D'autre part, certains analystes estiment que, bien que la dissuasion traditionnelle par la punition soit inefficace contre les nouveaux réseaux terroristes transnationaux, des préparatifs vastes et visibles pour faire face aux effets d'un terrorisme de masse peuvent fonctionner comme une « dissuasion par le déni ».

Le Cyberterrorisme, La Propagande et la Radicalisation En Ligne.

Le cyberterrorisme, la propagande et la radicalisation en ligne représentent des défis majeurs pour la sécurité internationale au XXI^e siècle. Internet a transformé la façon dont les groupes extrémistes recrutent, communiquent et mènent leurs opérations.

A travers ses différentes dimensions techniques et stratégiques, on peut mentionner entre autres :

1. Les réseaux sociaux comparés au Dark Web

Il s'avère que les acteurs malveillants adaptent l'usage des technologies en fonction de leurs objectifs cibles. Les réseaux sociaux grand public (Surface Web) sont utilisés pour la propagande de masse dont l'objectif est d'atteindre un public large, souvent jeune, en utilisant des algorithmes de recommandation pour amplifier la visibilité de contenus clivants ; ensuite il y a des applications de messagerie chiffrée telles que les Telegram, Signal ou WhatsApp qui servent de passerelles. Une fois le premier contact établi sur les réseaux sociaux, les recrues sont redirigées vers des boucles de discussion privées et chiffrées pour approfondir le processus de radicalisation ; et l'analyse de Weimann (2016) qui met en évidence une répartition claire des tâches dans la stratégie numérique de ces organisations, en argumentant que le Dark Web est moins utilisé pour le recrutement de masse en raison de sa complexité d'accès, mais sert de hub logistique pour le financement (via les cryptomonnaies), l'achat d'armes, le partage de manuels d'instructions terroristes (fabrication d'explosifs) et l'hébergement de sites miroirs résistant à la censure.

2. Les technologies de modération et limites

Les plateformes et les gouvernements déploient des outils technologiques de pointe, confrontés à des limites techniques afin de contrer certaines menaces. On peut mentionner les Hachage et empreintes numériques, pour bloquer instantanément les images ou vidéos terroristes connues grâce à leur "hash" (empreinte numérique unique) ; ensuite l'Intelligence Artificielle et le traitement automatique du langage naturel (Natural Language Processing - NLP) et la vision par ordinateur pour détecter les symboles, les discours de haine et les contenus extrémistes avant même qu'ils ne soient signalés par les utilisateurs ; et puis les limites du contournement dont les groupes radicaux s'adaptent constamment, en utilisant des fautes d'orthographe délibérées, du langage codé, des mèmes (une image, une vidéo ou un texte rigolo que l'on partage très vite sur Internet), ou intègrent du texte dans des images/vidéos pour duper les algorithmes de l'IA.

3. La Cyberguerre qui est au-delà de la propagande

Comme le cyberterrorisme ne se limite pas aux mots, il s'étend aux actions offensives visant les infrastructures critiques. On parle donc des attaques par déni de service (DDoS), qui consistent à submerger les sites gouvernementaux ou médiatiques pour paralyser la communication d'un État et démontrer une force asymétrique ; ensuite il y a le sabotage d'infrastructures ; et puis les Hactivisme et Vol de données, qui constituent le piratage de bases de données militaires ou étatiques, suivi de la divulgation d'informations personnelles (doxing) de soldats ou de fonctionnaires pour instaurer un climat de terreur (Reynaud, 2024).

4. Les récits de contre-discours (Contre-narratifs)

Comme la réponse sécuritaire et technique ne suffit pas, il faut mener une guerre idéologique. Les stratégies de contre-discours se divisent en deux approches : Le contre-discours direct : Déconstruire de front la propagande en pointant du doigt les mensonges, les contradictions théologiques ou politiques, et la réalité violente des groupes terroristes ; ensuite le discours alternatif qui met en avant des valeurs de pluralisme, d'inclusion, des témoignages de repentis (anciens radicaux) ou des réussites citoyennes pour offrir des perspectives d'avenir aux jeunes vulnérables ; et puis le ciblage algorithmique dont les initiatives consistent à utiliser des publicités ciblées. Lorsqu'un internaute cherche des mots-clés liés à la radicalisation, l'algorithme lui propose des vidéos de contre-discours ou des contenus éducatifs au lieu des liens extrémistes (Ajil, 2021).

Malgré des connaissances encore imparfaites sur le rôle d'Internet et des médias sociaux en ce qui a trait aux phénomènes de radicalisation et d'extrémisme violent, certains États et acteurs de la société civile n'ont pas tardé à mobiliser les sphères numériques comme outil de prévention. Une foule d'initiatives de lutte contre l'extrémisme violent mobilisent aujourd'hui Internet à la fois comme terrain d'action, mais également comme canal de sensibilisation et de communication. Pour la plupart mis en œuvre dans des contextes occidentaux (Royaume-Uni, Canada, France, Australie, États-Unis, etc.), ces initiatives sont extrêmement variables dans leurs ambitions, modalités et moyens mis en œuvre (Davies et al., 2016). Certaines d'entre elles déploient des contre-discours afin de faire contrepoids à la propagande extrémiste et radicalisante diffusée en ligne ou de narratifs alternatifs visant à mettre en lumière des voix concurrentes aux discours extrémistes (Braddock & Horgan, 2015). D'autres s'orientent davantage vers la littératie numérique et l'éducation critique, en particulier des jeunes, vis-à-vis des pratiques de navigation du Web et de consommation des contenus disponibles sur les médias sociaux. Toutes ces initiatives varient aussi considérablement dans les types de radicalités violentes visés. Alors que certaines initiatives visent exclusivement une forme d'extrémisme violent (le plus souvent, le jihadisme), d'autres s'attaquent à l'ensemble des formes de radicalités violentes.

Recommandations et réalisations possibles

En raison de l'évolution (voire de la révolution) des tactiques, des structures, des motivations et des idéologies terroristes, caractérisée par le développement de ce que l'on appelle le nouveau terrorisme, la complexité du phénomène terroriste a considérablement augmenté. Nous sommes désormais confrontés à une combinaison d'acteurs nouveaux et traditionnels, à un éventail élargi de motivations et de tactiques, de structures et de principes organisationnels, ainsi qu'à un éventail plus large de menaces technologiques, notamment face au potentiel accru d'utilisation d'armes de destruction massive à des fins terroristes. La lutte antiterroriste doit faire face simultanément à un éventail plus large de menaces. La lutte antiterroriste est devenue plus difficile que par le passé et cette évolution va probablement se poursuivre. Par conséquent, la politique antiterroriste doit être planifiée et exécutée avec une efficacité maximale.

En guise de conclusion, la Stratégie antiterroriste mondiale des Nations Unies s'organise autour de quatre piliers fondamentaux. Ces principes servent de guide pour structurer des politiques de sécurité nationales et internationales cohérentes :

Pilier de la Stratégie	Objectif Principal	Actions Recommandées
1. Éliminer les conditions propices au terrorisme	S'attaquer aux causes profondes de la radicalisation.	Résoudre les conflits prolongés, promouvoir la tolérance, réduire la marginalisation socio-économique et renforcer l'inclusion culturelle ou religieuse.
2. Prévenir et combattre le terrorisme	Priver les terroristes des moyens de mener leurs attaques.	Améliorer le partage de renseignements, sécuriser les frontières et traquer le financement du terrorisme (via la cybercriminalité, le trafic de ressources ou le détournement d'ONG).
3. Renforcer les capacités des États	Développer les outils de défense et optimiser le rôle de l'ONU.	Partager l'assistance technique, moderniser les systèmes de justice pénale et harmoniser les législations grâce au soutien du Bureau de lutte contre le terrorisme (UNOCT).
4. Garantir les droits de l'homme et l'État de droit	Maintenir la légitimité démocratique comme base de la lutte.	Veiller à ce que les mesures de sécurité n'enfreignent pas les libertés fondamentales, éviter les définitions nationales ambiguës du terrorisme et interdire strictement la torture ou la discrimination.

Source : Le septième examen de la Stratégie antiterroriste mondiale (A/RES/72/284) approche, et le rapport correspondant sera finalisé en juin 2021.

Références Bibliographiques

- Ajil, A. (2021). Au-delà du contre-discours : Repenser la prévention de la radicalisation en ligne par l'engagement citoyen. *Déviance et Société*, 45(3), 415–442.
- Alexander, Y. (Dir.). (2002). *Combating terrorism: Strategies of ten countries*. University of Michigan Press. <https://doi.org/10.3998/mpub.11969>
- Anne-Sophie, M. (2017/2022). *La généralisation à partir du conflit afghan (2001-2013) : Les mutations de la guerre asymétrique* [Thèse de doctorat, HAL-SHS].
- Betts, R. K. (2003). Fixing intelligence. Dans R. D. Howard & R. L. Sawyer (dir.), *Terrorism and counterterrorism: Understanding the new security environment*. McGraw-Hill/Dushkin.
- Borlant-Clément, S. (Dir.). (2021). *État des lieux et perspectives de la lutte contre le blanchiment de capitaux et contre le financement du terrorisme*. Dalloz. ISBN 978-2-247-21226-2.
- Braddock, K., & Horgan, J. (2016). Towards a guide for constructing and disseminating counternarratives to reduce support for terrorism. *Studies in Conflict & Terrorism*, 39(5), 381–404. <https://doi.org/10.1080/1057610X.2015.1116277>
- Conway, M. (2017). Determining the role of the Internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77–98. <https://doi.org/10.1080/1057610X.2016.1157408>
- Crenshaw, M. (2011). *Explaining terrorism: Causes, processes and consequences*. Routledge.
- Ducol, B. (2015). Radicalisation générale vs radicalisation en ligne : Vers une typologie des usages d'Internet dans les processus de radicalisation. *Revue internationale de criminologie et de police technique et scientifique*, 68(2), 143–156.
- Financial Crime Academy. (2026). *Le guide définitif des recommandations du GAFI*. Financial Crime Academy.
- GAFI. (2025). *Méthodologie d'évaluation de la conformité technique aux recommandations du GAFI et de l'efficacité des systèmes de LBC/FT*. Groupe d'action financière, Paris.
- Ganor, B. (2013, 5 octobre). *The definition of terrorism: A fundamental counter-terrorism measure*. International Institute for Counter-Terrorism.
- Ilaria Briglia. (2021, 17 mai). Nouvelles technologies et armes de destruction massive : Vers un nouveau terrorisme ? *Le Grand Continent*, rubrique « Guerre numérique ».
- Koblentz, G. D. (2020). Emerging technologies and the future of CBRN terrorism. *The Washington Quarterly*, 43(2), 177–196. <https://doi.org/10.1080/0163660X.2020.1770969>
- Marcou, L. (2018). *Le Djihad numérique : Internet et les réseaux sociaux, nouveaux champs de bataille de l'EI*. Éditions L'Harmattan.
- Michael, K. (2020, 21 octobre). Revisiting the ecosystem of Islamic State's "virtual caliphate". *Global Network on Extremism and Technology*. <https://gnet-research.org/2020/10/21/revisiting-the-ecosystem-of-islamic-states-virtual-caliphate/>
- Nemar, K. (2018). *Le cadre juridique des opérations militaires de stabilisation et de reconstruction : Vers un code de conduite des opérations militaires en situation post-conflictuelle fondé sur les droits de l'Homme ?* [Thèse de doctorat en droit, Aix-Marseille Université]. <https://www.academia.edu/44875969/>
- P. M., Michał. (2018). Guerre préventive en vertu du droit international. *Études autoritaires et totalitaires*, 39(4), 69–79. <https://doi.org/10.19195/2300-7249.39.4.6>
- Ramos, R. (2018). *Une chimère américaine : Genèse de la communauté du renseignement des États-Unis, de la CIA à la NSA*. Presses Universitaires de la Méditerranée. ISBN 978-2-36781-270-0.

- Ramos, R. (2022). Le 11 Septembre et la réorganisation du renseignement aux États-Unis : Aux sources d'une réforme inachevée. *Représentations dans le monde anglophone*, (24). <https://doi.org/10.35562/rma.538>
- Reynaud, C. (2024, 29 août). La plus grande attaque DDoS de l'histoire a visé un serveur Minecraft. *Minecraft.fr*. <https://minecraft.fr/la-plus-grande-attaque-ddos-de-lhistoire-a-vise-un-serveur-minecraft/>
- Van Steenberghe, R. (2017). Les interventions militaires étrangères récentes contre le terrorisme international – Seconde partie : Droit applicable (*jus in bello*). *Annuaire français de droit international*, 63, 37–91. <https://doi.org/10.3406/afdi.2017.5365>
- Weimann, G. (2015). *Terrorism in cyberspace: The next generation*. Woodrow Wilson Center Press; Columbia University Press.