Global Network
on Extremism & Technology

Enquête du GNET sur le rôle des technologies dans l'extrémisme violent et l'état de la coopération entre la recherche et le secteur des technologies

Lydia Khalil

Le GNET est un projet spécial du Centre international d'étude de la radicalisation du King's College, à Londres.

L'auteure de ce rapport est Lydia Khalil, chercheuse au Lowy Institute.

Remerciements
L'auteure tient à remercier le Dr Maura Conway pour ses conseils sur l'élaboration des questions de l'enquête, J. M. Berger pour ses suggestions, Natasha Kassam et Alex Oliver du Lowy Institute pour leurs expériences et conseils en matière d'élaboration d'enquête, et le Dr Matteo Vergani pour sa contribution aux questions. Ce rapport n'aurait pu voir le jour sans la participation des nombreux universitaires et spécialistes qui ont répondu à l'enquête malgré leur temps et leurs ressources limités. Tout défaut de conception ou d'analyse est strictement le fait de l'auteure.

Le Global Network on Extremism and Technology (Réseau mondial sur l'extrémisme et la technologie – GNET) est une initiative de recherche universitaire bénéficiant du soutien du Forum mondial de l'Internet contre le terrorisme (GIFCT), une initiative indépendante mais financée par le secteur qui vise à mieux comprendre et lutter contre l'utilisation des technologies par les groupes terroristes. Le GNET est formé et dirigé par le Centre international d'étude de la radicalisation (ICSR), un centre de recherche universitaire basé dans les locaux du Département d'étude des guerres du King's College, à Londres. Les opinions et conclusions exprimées dans ce document sont celles des auteurs et ne doivent en aucun cas être interprétées comme représentant les opinions et conclusions, expresses ou implicites, du GIFCT, du GNET ou de l'ICSR.

COORDONNÉES

Pour toute question, demande d'information et demande de copies supplémentaires du présent rapport, contacter :

ICSR
King's College London
Strand
Londres WC2R 2LS
Royaume-Uni

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter : **@GNET_research**

Ce rapport peut, comme toutes les autres publications du GNET, être téléchargé gratuitement à partir du site Internet du GNET : www.gnet-research.org.

© GNET

Résumé exécutif

Quel rôle jouent les technologies, et plus particulièrement les communications assistées par ordinateur, dans l'extrémisme violent ? C'est la question que se pose le Global Network on Extremism and Technology (GNET) en sa qualité d'initiative issue de la recherche et du secteur des technologies. Les acteurs extrémistes ont été parmi les premiers à exploiter Internet et à reconnaître son potentiel comme outil de communication et de mobilisation. C'est pourquoi les chercheurs et chercheuses tentent, depuis plusieurs dizaines d'années, mais plus particulièrement depuis l'apparition de l'État islamique, l'essor de l'extrémisme violent motivé par des idéologies d'extrême droite et l'émergence rapide – et largement facilitée par le Net – de mouvements extrémistes et conspirationnistes violents, comme QAnon, de répondre à des questions portant sur les rapports entre technologie et extrémisme.

Le Lowy Institute a mené une enquête sur différents aspects de cette question centrale auprès des chercheurs et chercheuses spécialisé·e·s dans le terrorisme et l'extrémisme violent afin de compléter les études passées consacrées à l'influence d'Internet sur l'extrémisme, de comprendre les conclusions qui n'avaient pas nécessairement été prises en compte par la littérature analysée précédemment, et d'appréhender le niveau de collaboration entre la recherche et le secteur des technologies.

L'enquête révèle l'existence d'un vaste consensus au sein de la recherche, selon lequel les communications par Internet et les plateformes de médias sociaux « appuient, encouragent ou soutiennent la violence perpétrée dans la vie réelle ». Toutefois, si l'on en croit les réponses aux questions plus détaillées de l'enquête, l'analyse du rôle des technologies dans l'extrémisme violent est incroyablement complexe, pluridimensionnelle et encore contestée.

Les réponses aux questions sur la collaboration entre la recherche et le secteur des technologies ont montré que celle-ci est potentiellement bénéfique, mais également difficile – de la même manière que les spécialistes du terrorisme s'interrogent encore sur la collaboration avec les gouvernements et les agences de sécurité, et s'inquiètent de l'ampleur que prennent les aspects sécuritaires liés à la recherche universitaire. Plusieurs réponses ont mis en lumière un certain cynisme concernant la collaboration du secteur des technologies avec le monde de la recherche, des inquiétudes sur l'opacité et l'absence de transparence des principales plateformes, leur nature réactive et les priorités divergentes en matière de recherche du secteur, ainsi qu'un certain scepticisme vis-à-vis du sérieux et de l'efficacité des mesures prises par les médias sociaux pour lutter contre l'extrémisme violent et la désinformation préjudiciable.

Table des matières

1 Introduction 5

2 Étude des liens entre extrémisme et technologie 11
Ce que dit la littérature 11
Limites et données 13

3 Enquête 17
Le rôle d'Internet et des médias sociaux dans l'extrémisme 18
Interactions entre la recherche et le secteur des technologies 30

4 Conclusion 35

Contexte politique 37

1 Introduction

Quel rôle jouent les technologies, et plus particulièrement les communications assistées par ordinateur, dans l'extrémisme violent ? Cette question est si vaste qu'elle en appelle d'autres, par exemple : quel rôle joue Internet, y compris les médias sociaux, dans le processus de radicalisation ? L'utilisation des médias sociaux a-t-elle augmenté la production de contenus et récits extrémistes violents et l'exposition à ces derniers, et cette exposition entraîne-t-elle une radicalisation des individus ? L'usage des communications assistées par ordinateur et des plateformes de médias sociaux facilite-t-il le recrutement ou la mobilisation d'individus en faveur de causes extrémistes violentes ? L'une ou plusieurs caractéristiques des technologies et plateformes elles-mêmes – leur design, leur logique, leurs potentialités, leurs limites – favorisent-elles l'extrémisme, ou y contribuent-elles ? Le rôle précis joué par les technologies dépend-il du type d'idéologie extrémiste ou de structure d'un mouvement en particulier, voire du genre ou du profil d'une personne ? Comment les technologies virtuelles et les communications assistées par ordinateur favorisent-elles les rapports entre individus ou l'émergence d'écosystèmes sociaux en ligne contribuant à l'extrémisme ? L'adhésion d'un individu à des croyances extrémistes en raison de son exposition aux récits et contenus à caractère extrémiste en ligne ou de sa participation à des sous-cultures virtuelles conduit-elle nécessairement à la violence, au militantisme ou à la commission d'autres préjudices dans la vie réelle ?

Cette liste de questions n'est pas exhaustive, et ne date pas d'hier. Les acteurs extrémistes ont été parmi les premiers à exploiter Internet et à reconnaître son potentiel comme outil de communication et de mobilisation. C'est pourquoi les chercheurs et chercheuses tentent d'y répondre, entre autres interrogations sur le rôle joué par les technologies dans l'extrémisme, depuis plusieurs dizaines d'années, mais plus particulièrement depuis l'apparition de l'État islamique, puisque son essor rapide, son rayonnement international et son utilisation des médias sociaux ont constitué un véritable défi à la fois pour les spécialistes du terrorisme et les agents chargés de la lutte antiterroriste.

Nous en sommes désormais au même point avec l'essor de l'extrémisme violent motivé par des idéologies et complots d'extrême droite. Le monde a enregistré, ces cinq dernières années, une hausse de 205 % du terrorisme d'extrême droite[1], et assisté à l'émergence rapide, favorisée par Internet, de mouvements extrémistes complotistes et violents, comme QAnon. Si certains avancent que la peur suscitée par QAnon est peut-être exagérée[2], ce mouvement complotiste a été qualifié de menace extrémiste intérieure par le FBI[3] et a inspiré

1 Indice mondial du terrorisme (2020) Institute for Economics and Peace, https://www.visionofhumanity.org/global-terrorism-index-2020-the-ten-countries-most-impacted-by-terrorism/
2 CIVIQS (2021) Sondage « QAnon Support, Registered Voters », https://civiqs.com/results/qanon_support?uncertainty=true&annotations=true&zoomIn=true
3 Jana Winter (2019) « FBI document warns that conspiracy theories are a new domestic terrorism threat », Yahoo News, https://news.yahoo.com/fbi-documents-conspiracy-theories-terrorism-160000507.html

plusieurs attentats violents perpétrés récemment[4]. Pendant la pandémie de coronavirus, de nombreuses personnes ont vécu dans la peur et l'insécurité, tout en passant de nombreuses heures sur la toile. L'utilisation accrue d'Internet a suscité des inquiétudes, jusqu'ici infondées, quant à l'exposition accrue au risque de radicalisation en ligne ou, tout au moins, aux contenus à caractère extrémiste publiés sur la toile[5].

Le Dr Maura Conway a lancé le débat sur le rôle des technologies dans l'extrémisme violent en 2017 avec son article : « Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research »[6]. Elle y décrit comment les spécialistes du terrorisme s'attaquent à la question du rôle d'Internet. Mais comme elle l'indiquait au moment de la rédaction de son article, « il n'y a pas, à l'heure actuelle, suffisamment de recherches empiriques et de fond dans le domaine des sciences sociales pour nous permettre de répondre de manière convaincante à ces questions »[7].

Il y a encore peu de réponses définitives, mais depuis la publication de l'article, le milieu de la recherche sur l'extrémisme et le terrorisme a réussi à répondre à certaines questions sur le rôle d'Internet, les liens de causalité et les potentialités que certaines technologies et plateformes offrent aux acteurs extrémistes violents. Les nouvelles recherches portant sur le rôle d'Internet et d'autres technologies dans l'extrémisme et le terrorisme se multiplient depuis cinq ans. Les spécialistes des données et les chercheurs et chercheuses en sciences sociales spécialisé·e·s dans le terrorisme collaborent de plus en plus étroitement. Les recherches relatives à l'étude d'Internet prêtent aujourd'hui davantage attention à l'extrémisme et au terrorisme – de la même façon que les recherches en psychologie sociale et relatives aux médias et à la communication ont interagi avec les études sur le terrorisme.

La création même du Global Network on Extremism and Technology, le Réseau mondial sur l'extrémisme et la technologie, et le fait que le secteur des technologies soit plus disposé qu'auparavant à reconnaître, non sans peine, que ses plateformes et technologies sont non seulement exploitées par des acteurs extrémistes mais aussi que leurs fonctionnalités ont contribué à la diffusion rapide de leurs idéologies, ont permis de faire avancer la recherche[8]. Les plateformes principales sont aujourd'hui aux prises avec le rôle qu'elles ont joué dans la création de mondes virtuels extrémistes[9] et leur contribution à la nature changeante de l'extrémisme et de sa structure organisationnelle[10]. Le secteur participe également davantage aux travaux menés par la recherche spécialisée dans l'extrémisme violent.

---

4 Amarnath Amarasingham et Marc-André Argentino (juillet 2020) « The QAnon Conspiracy Theory: A Security Threat in the Making? » *CTC Sentinel* vol. 13 n° 7 : p. 37–41, https://ctc.usma.edu/the-qanon-conspiracy-theory-a-security-threat-in-the-making/

5 Caleb Spencer (2020) « Children may have been radicalised during lockdown », BBC News, https://www.bbc.com/news/uk-wales-53082476

6 Maura Conway (2017) « Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research », *Studies in Conflict & Terrorism* vol. 40 n° 1 : p. 77–98, DOI : 10.1080/1057610X.2016.1157408

7 *Ibid.*

8 Mason Youngblood (2020) « Extremist ideology as a complex contagion: the spread of far-right radicalization in the United States between 2005 and 2017 », *Humanities and Social Science Communications* vol. 7 n° 1 : p. 1–10, https://www.nature.com/articles/s41599-020-00546-3

9 Department of Security Studies and Criminology (2020) « Mapping Networks and Narratives of Online Right-Wing Extremists in New South Wales », http://doi.org/10.5281/zenodo.4071472

10 Bruce Hoffman et Colin Clarke (2020) « The Growing Irrelevance of Organizational Structure of Domestic Terrorism », The Cipher Brief, https://www.thecipherbrief.com/article/united-states/the-next-american-terrorist

De plus en plus de données factuelles prouvent en effet que les technologies virtuelles peuvent largement faciliter l'extrémisme. Il est néanmoins admis que nous devons approfondir davantage ce que cela signifie exactement pour donner un véritable sens à une conclusion aussi vaste. Un consensus plus nuancé, selon lequel la technologie Internet, si elle n'est pas la *cause* véritable de l'extrémisme violent, peut tout de même jouer des rôles *multiples* et *variés* et *faciliter* la radicalisation et la mobilisation en faveur de l'extrémisme violent, a vu le jour[11].

De plus, nous savons désormais qu'« il est difficile d'établir une dichotomie en ligne/hors ligne » concernant les comportements violents motivés par des croyances extrémistes[12]. Plutôt que de conceptualiser la « radicalisation en ligne » au sens large, nous avons pris conscience du fait que les technologies Internet jouent différents rôles dans le processus de radicalisation extrémiste et qu'elles sont exploitées de différentes manières et favorisent différentes actions[13].

Nous sommes également conscients que le rôle des technologies dans la radicalisation et la mobilisation en faveur de la violence a évolué au fil des années, parallèlement aux avancées technologiques. La transition entre les sites Internet statiques et forums à huis clos et les réseaux sociaux publics dans un premier temps, puis le passage à des plateformes technologiques alternatives et l'infiltration du « dark web » ou du « deep web »[14] par les acteurs extrémistes dans un second temps, a considérablement modifié le rôle joué par Internet et d'autres technologies dans l'extrémisme, en fonction des potentialités de chaque plateforme ou technologie. Les technologies actuelles, qui n'existaient pas il y a quelques années, telles que les services de messagerie chiffrés de bout en bout et les drones, ont influencé les tactiques, les communications et les opérations des acteurs extrémistes. Les avancées technologiques futures provoqueront d'autres évolutions de ce type. Dans un article dans lequel il se pose la question de savoir si Internet a conduit à une hausse du terrorisme transnational, David Benson affirme qu'« Internet est omniprésent ; il serait donc étrange que les terroristes d'aujourd'hui ne l'utilisent pas, tout comme il aurait été étrange que les terroristes du passé n'utilisent pas les services postaux ou le téléphone »[15]. Tout comme les avancées technologiques modifient tous les aspects de notre vie, elles influent sur l'extrémisme et le terrorisme.

Jusqu'à récemment, le consensus était que les technologies Internet étaient un « outil de facilitation » : la radicalisation menant à la violence, le recrutement, la mobilisation et la planification d'attentats pouvaient être facilités, mais ne dépendaient pas nécessairement d'Internet ; et Internet n'était pas cause de radicalisation[16]. C'est peut-être encore le cas. Mais, pendant la pandémie, et plus particulièrement après la

11 Paul Gill, Emily Corner, Amy Thornton et Maura Conway (2015) « What are the roles of the internet in terrorism? Measuring online behaviours of convicted UK terrorists », VOXPol Network of Excellence, https://www.voxpol.eu/download/vox-pol_publication/What-are-the-Roles-of-the-Internet-in-Terrorism.pdf

12 Paul Gill, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom et John Horgan (2017) « Terrorist Use of the Internet by the Numbers », *Criminology and Public Policy* vol. 16 n° 1 : p. 99–117

13 Gill *et al.* « What are the roles of the internet in terrorism? »

14 D'après le dictionnaire Merriam-Webster, le « dark web » se définit comme « un ensemble de pages web qui ne peuvent être indexées par les moteurs de recherche, ne sont pas consultables dans un navigateur standard, ne peuvent être consultées qu'à l'aide de moyens spécifiques (tels que des logiciels ou une configuration réseau spécialisés) et ont recours au chiffrage pour assurer l'anonymat des utilisateurs et protéger leur identité ».

15 David C. Benson (2014) « Why the Internet Is Not Increasing Terrorism », *Security Studies* vol. 23, n° 2 : p. 293–328, DOI : 10.1080/09636412.2014.905353

16 Alexander Meleagrou-Hitchens et Nick Kaderbhai (2017) « Research Perspectives on Online Radicalisation a literature review, 2006–2016 », VoxPol Network of Excellence, https://icsr.info/wp-content/uploads/2017/05/ICSR-Paper_Research-Perspectives-on-Online-Radicalisation-A-Literature-Review-2006-2016.pdf

prise d'assaut du Capitole, aux États-Unis, de nouvelles inquiétudes concernant le véritable rôle de ces technologies ont vu le jour. La prise d'assaut du Capitole a réuni un vaste éventail de réseaux, groupes et individus – groupes militants organisés, partisans de QAnon, sympathisants pro-Trump – croyant tous au mensonge, relayé et diffusé en ligne, selon lequel l'élection présidentielle américaine était frauduleuse. Différents groupes extrémistes établis avaient jeté les bases de la prise d'assaut du Capitole depuis plusieurs mois sur différents forums en ligne[17] et les désinformations relatives au processus électoral et aux résultats de l'élection inondaient Internet et les principales plateformes de médias sociaux[18]. Ces derniers ont également été au cœur de la prise d'assaut elle-même : selon un rapport préliminaire du Program on Extremism de la George Washington University, 68 % des participants inculpés ont « diffusé en temps réel leurs agissements présumés au Capitole »[19].

D'après ce rapport, les médias sociaux ont également « joué un rôle central dans l'organisation de la prise d'assaut et la diffusion de contenus qui ont aidé à motiver les participants ». Ils ont aussi permis à des groupes et individus disparates ayant participé à la prise d'assaut d'interagir, puis de se réunir à Washington, D.C., le 6 janvier 2021[20]. Les cas étudiés dans le rapport montrent comment les médias sociaux ont facilité la formation de « clusters » spontanés d'inconnus, qui se sont réunis et ont voyagé ensemble pour participer à la prise d'assaut sans grande planification préalable[21] – faisant écho, quelque part, aux départs d'étrangers inspirés par l'État islamique, mais dans des délais beaucoup plus courts, à moindre distance et avec moins d'obstacles aux déplacements.

Alors que les médias sociaux et les technologies algorithmiques s'introduisent de plus en plus dans notre vie quotidienne, est-il possible qu'Internet non seulement facilite, mais participe activement à l'extrémisme violent ? Dans une étude des comportements en ligne de terroristes condamnés au Royaume-Uni menée en 2015, Paul Gill, Emily Corner, Amy Thornton et Maura Conway avancent qu'« Internet n'a pas conduit à une montée du terrorisme. Il s'agit principalement d'un outil de facilitation ; la radicalisation est favorisée par Internet, mais n'en dépend pas »[22].

Mais assistons-nous à l'émergence d'un « nouveau type de terrorisme qui ne peut exister sans Internet »[23] ? La prise d'assaut du Capitole illustre-t-elle l'émergence d'un Internet favorisant et conduisant à la radicalisation numérique et à la mobilisation de masse[24] ? L'utilisation d'Internet par certains individus ayant participé à la prise d'assaut – en particulier ceux non affiliés à des organisations établies – et leur exposition constante à des récits extrémistes et à la désinformation

17 Robert Evans (2021) « How the Insurgent and MAGA Right are Being Welded Together on the Streets of Washington D.C. », Bellingcat, https://www.bellingcat.com/news/americas/2021/01/05/how-the-insurgent-and-maga-right-are-being-welded-together-on-the-streets-of-washington-d-c/
18 Network Contagion Research Institute (2021) « NCRI Assessment of the Capitol Riots – Violent Actors and Ideologies Behind the Events of January 6, 2021 », https://networkcontagion.us/wp-content/uploads/NCRI-Assessment-of-the-Capitol-Riots.pdf
19 George Washington University's Program on Extremism (2021) « This is Our House! A Preliminary Assessment of the Capitol Hill Siege Participants », https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/This-Is-Our-House.pdf
20 *Ibid.*
21 *Ibid.*
22 Gill *et al.* « What are the roles of the internet in terrorism? »
23 Craig Timberg, Drew Harwell, Razzan Nakhlawi et Harrison Smith (2021), « Nothing can stop what's coming: far right forums that fomented Capitol riots voice glee in aftermath », *The Washington Post*, https://www.washingtonpost.com/technology/2021/01/07/trump-online-siege/
24 Robert Pape et Keven Ruby (2021), « The Capitol Rioters Aren't Like Other Extremists », *The Atlantic*, https://www.theatlantic.com/ideas/archive/2021/02/the-capitol-rioters-arent-like-other-extremists/617895/

en ligne ont-elles accéléré leur processus de radicalisation menant à la violence ? Dans ce cas précis, leur radicalisation a-t-elle, en réalité, été déterminée par Internet, ou a-t-elle dépendu d'Internet ? La « logique » de différentes plateformes a-t-elle contribué à la croissance de l'extrémisme, et joue-t-elle aujourd'hui un rôle plus important dans la trajectoire d'un individu vers la radicalisation menant à la violence ?

En tentant de décrire la nouvelle logique des médias sociaux et de comprendre la façon dont ces plateformes se sont « enracinées dans la mécanique de la vie quotidienne » et affectent les structures institutionnelles et les interactions sociales, José van Dijck et Thomas Poell ont comparé la logique des médias sociaux à celle de leurs prédécesseurs, les médias de masse, et avancé que les médias sociaux ont créé un nouvel écosystème qui « remodèle l'ordre social ou les successions d'événements ». Les médias sociaux ayant la capacité de transférer leur logique dans la vie réelle par le biais de « stratégies, mécanismes et économies sous-tendant les dynamiques de leurs plateformes », la société au sens large est assujettie à leur logique et à leurs principes[25].

Si van Dijck et Poell n'étudient pas spécifiquement l'extrémisme, J. M. Berger, spécialiste de ce phénomène, a avancé un argument comparable sur la façon dont la logique et la nature des communications assistées par ordinateur, et plus particulièrement des médias sociaux, ont fondamentalement modifié les interactions sociales et réorganisé la sphère publique d'une façon qui a conduit à l'extrémisme. Selon lui, l'essor d'Internet, et en particulier des médias sociaux, a contribué à une hausse de l'incertitude et effiloché la « réalité du consensus » en créant un « environnement volatil et hostile à l'idée de vérité objective ». Les médias sociaux ont renforcé l'incertitude parce qu'ils ont permis à toutes sortes d'informations, opinions et analyses contradictoires de voir le jour sur leurs plateformes[26]. Selon Berger, « les médias sociaux créent un environnement dans lequel différentes perceptions de la réalité peuvent gagner en popularité en attirant des niveaux d'engagement mesurables suffisants pour être perçus comme un consensus par les membres du public. Afin de concilier l'incertitude créée par ces points de vue contradictoires, le public est susceptible de s'appuyer sur la validation collective d'une réalité perçue, qui s'accompagne souvent d'une hostilité envers les perspectives extérieures »[27]. C'est dans la nature humaine de répondre à cette fracture de la réalité du consensus en cherchant la certitude par le biais « d'identités exclusives et globales – dont beaucoup sont toxiques et fragiles et susceptibles de semer la graine de l'extrémisme violent »[28]. L'extrémisme voit aussi le jour parce que le consensus d'un groupe extérieur est considéré comme une menace existentielle qui doit être réduite à néant. Berger avance par ailleurs qu'il existe des différences fondamentales entre les anciens et les nouveaux médias, notamment en ce qui concerne l'absence de gardiens ou de régulation des contenus, le faible coût de production et les « indicateurs d'engagement inextricablement liés à la distribution »[29].

25 José van Dijck et Thomas Poell (2013) « Understanding Social Media Logic », *Media and Communication* vol 1 n° 1 : p. 2–14, https://ssrn.com/abstract=2309065
26 J. M. Berger (2020) « Our Consensus Reality Has Shattered », *The Atlantic*, https://www.theatlantic.com/ideas/archive/2020/10/year-living-uncertainly/616648/
27 Entretien par message avec J. M. Berger (6 avril 2021).
28 J. M. Berger, « Our Consensus Reality Has Shattered »
29 Entretien par message avec J. M. Berger (6 avril 2021).

2 Étude des liens entre extrémisme et technologie

La réalisation d'une analyse documentaire portant sur les recherches existantes est une façon de répondre aux débats persistants sur le rôle de la technologie dans l'extrémisme violent et d'examiner les derniers questionnements et problématiques en date. En effet, plusieurs analyses documentaires de grande qualité portant sur le rôle d'Internet et des technologies dans le processus de radicalisation et l'extrémisme violent ont été réalisées au fil des ans.

Ce que dit la littérature

En 2013, RAND Europe a mené une analyse documentaire dans le cadre de son étude *Radicalisation in the digital era* (« La radicalisation à l'ère numérique »), qui s'intéresse à la façon dont les individus en cours de radicalisation utilisent Internet. L'analyse documentaire et les recherches primaires menées dans le cadre de cette étude ont montré qu'Internet avait « accru les possibilités de se radicaliser, compte tenu de sa disponibilité généralisée et du fait qu'il facilite la création de liens 24 heures sur 24, 7 jours sur 7, avec des individus des quatre coins du monde partageant des points de vue similaires ». Elle conclut également qu'Internet peut faire office de caisse de résonance et donne davantage la possibilité aux individus d'exprimer des croyances extrémistes que les interactions dans le monde réel. Mais elle révèle aussi qu'à l'époque, Internet n'accélérait pas nécessairement cette radicalisation et ne servait pas non plus de substitut au besoin de rapports personnels pendant le processus de radicalisation[30].

En 2017, Alexander Meleagrou-Hitchens et Nick Kaderbhai ont mené une analyse documentaire sur la radicalisation en ligne, et confirmé que le « consensus est le suivant : Internet n'est pas une cause de radicalisation, mais facilite et favorise le glissement des individus vers la commission d'actes politiques violents ». Ils citent plusieurs études mettant en garde contre la surestimation du rôle d'Internet, à l'instar de Benson (2014), qui affirme que les études existantes « manquent de variables dépendantes et indépendantes traitant à la fois de l'utilisation d'Internet par les terroristes et par les États, omettant ainsi les cas négatifs qui permettraient de "déterminer l'effet net d'Internet sur le terrorisme transnational" »[31].

Meleagrou-Hitchens et Kaderbhai notent également que la littérature portant sur le rôle joué par les technologies et l'environnement virtuel dans la radicalisation est contestée, parce que le concept même de radicalisation est remis en cause dans les études sur l'extrémisme.

30 Ines von Behr, Anaïs Reding, Charlie Edwards, Luke Gribbon (n.d.) « Radicalisation in the digital era », RAND, https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf
31 Meleagrou-Hitchens et Kaderbhai, « Research Perspectives on Online Radicalisation »

Il existe toutefois un consensus sur le fait que la radicalisation menant à la violence est un processus social et qu'Internet, et plus particulièrement les médias sociaux, offre des espaces sociaux qui favorisent la création de cercles fermés, encouragent la formation identitaire et donnent aux influenceurs, influenceuses et leaders une plateforme pour s'exprimer.

Ils concluent que « selon la grande majorité des auteurs, si Internet joue un rôle de facilitateur, les individus doivent encore, dans la plupart des cas, être en contact avec des réseaux dans la vie réelle. Une enquête sur la trajectoire d'un individu est ainsi souvent une enquête sur les interactions uniques entre le monde réel et le monde virtuel »[32]. Des recherches plus récentes, menées en 2020 par Tinia Gaudette, Ryan Scrivens et Vivek Venkatesh et fondées sur des entretiens approfondis avec d'anciens extrémistes violents canadiens, montrent toutefois que « quelle que soit la façon dont les individus sont exposés aux idéologies et groupes extrémistes violents, c'est Internet, au bout du compte, qui facilite le processus de radicalisation violente en leur permettant de s'immerger dans des contenus et réseaux extrémistes. Cette conclusion est appuyée par la recherche empirique sur le rôle d'Internet dans l'émergence d'un ensemble de mouvements extrémistes violents en général, et du mouvement d'extrême droite en particulier »[33]. Cette étude d'anciens extrémistes canadiens fait écho aux conclusions de l'étude menée par Koehler en 2014 sur d'anciens extrémistes allemands et leur utilisation d'Internet. D'après l'auteur, « comparé à d'autres "institutions de socialisation", comme les activités collectives dans la vie réelle, la musique et les concerts, les rallies et formations politiques, Internet semble être l'élément le plus important dans les processus de radicalisation individuelle, en fonction des contenus consommés »[34].

Une autre étude systématique menée en 2018 a cherché à mettre en lumière, en n'analysant que des études empiriques, les liens entre l'exposition en ligne aux contenus radicaux violents et les agissements radicaux violents menés en ligne ou dans la vie réelle. D'après elle, « Internet semble jouer un rôle dans la formation de décisions ce qui, conjugué à d'autres facteurs de la vie réelle, peut être associé à une prise de décisions ». Mais sur les 5 182 études générées par ses recherches, seules 11, un chiffre extrêmement faible, pouvaient être incluses[35] – ce qui met en évidence l'absence de recherche empirique à l'époque.

En 2019, un autre examen systématique a produit 88 études sur le rôle d'Internet dans l'extrémisme djihadiste et d'extrême droite à partir d'une recherche de littérature portant sur la période 2000–2019. Mais ces études s'intéressaient aux caractéristiques et au contenu des sites Internet utilisés et non aux habitudes des internautes eux-mêmes[36]. Les auteurs de cet examen ont conclu que « les études existantes n'ont, jusqu'à présent, pas suffisamment examiné les

32 *Ibid.*
33 Tiana Gaudette, Ryan Scrivens et Vivek Venkatesh (2020) « The Role of the Internet in Violent Extremism: Insights from Former Right-Wing Extremists », *Terrorism and Political Violence*, DOI : 10.1080/09546553.2020.1784147
34 Daniel Koehler (2014) « The Radical Online: Individual Radicalization Processes and the Role of the Internet », *Journal for Deradicalization*, vol. hiver 2014/2015 n° 1 : https://journals.sfu.ca/jd/index.php/jd/article/view/8/8
35 Ghadya Hassan *et al.* (2018) « Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence », *International Journal of Development Science* vol. 12 n° 1–2 : p. 71–88
36 Ozen Odog, Anne Leiser et Klaus Boehnke (2019) « Reviewing the Role of the Internet in Radicalisation Processes », *Journal for Deradicalisation* n° 21, https://journals.sfu.ca/jd/index.php/jd/article/view/289

utilisateurs des sites disponibles, ni étudié les mécanismes de causalité qui sont en jeu dans les interactions entre Internet et ses utilisateurs ». Il n'existe que très peu d'études traitant des internautes eux-mêmes, leur historique de navigation et leurs motivations et expériences en ligne.

Plus récemment, en 2020, une analyse documentaire menée par Charlie Winter, Peter Neumann, Alexander Meleagrou-Hitchens, Magnus Ranstorp, Lorenzo Vidino et Johanna Furst a porté sur l'usage d'Internet par les extrémistes violents, à l'échelle à la fois organisationnelle et individuelle, et les objectifs poursuivis[37]. Cet examen de la littérature a conduit les auteurs à conclure que, tout comme Internet revêt une importance capitale pour tout un chacun, il est « devenu un environnement opérationnel de premier plan, dans lequel des idéologies politiques sont concrétisées, des attentats planifiés et des mouvements sociaux formés »[38]. C'est le cas parce que « la plupart du temps, l'extrémisme en ligne n'est que le fruit d'une utilisation intuitive d'Internet ». Les extrémistes utilisent Internet de la même façon que nous tous. Et si la prévalence de la propagande extrémiste en ligne et sa consommation accrue ne conduisent pas, à elles seules, à la radicalisation, les espaces en ligne peuvent servir de forums de mobilisation et d'interactions sociales qui peuvent contribuer à la radicalisation et à la mobilisation violentes[39]. Les espaces en ligne sont des espaces sociaux et fonctionnent de la même façon que ceux de la vie réelle, en fournissant une identité, une validation, une communauté, un sens. L'examen conclut que si les auteurs n'ont su trouver de lien de causalité entre les technologies Internet et l'extrémisme ou tirer de conclusions structurelles, « il ne fait aucun doute que les organisations extrémistes ne seraient pas où elles sont aujourd'hui sans une utilisation habile des mondes virtuels ».

Limites et données

Ces études systématiques et d'autres du même type ont été importantes pour comprendre l'état du champ de recherche et les évaluations du milieu de la recherche concernant le rôle des technologies Internet dans l'extrémisme violent. Toutefois, comme l'ont noté bon nombre des analyses documentaires effectuées, la littérature passée en revue était davantage orientée vers l'étude des djihadistes compte tenu de la prévalence de la recherche dans ce domaine. Elle avait ainsi tendance à moins s'intéresser aux autres idéologies, en particulier celles d'extrême droite, qui représentent aujourd'hui une grave menace dans toutes les régions du monde et font désormais l'objet d'un nombre croissant d'articles[40]. Les études s'intéressaient également aux recherches menées et aux articles rédigés avant la pandémie, dont l'impact réel sur la société et l'extrémisme reste encore à déterminer.

De plus, la qualité des conclusions de recherche dépend de la qualité des données sur lesquelles elles sont fondées, et une analyse documentaire est moins susceptible de bien mettre en lumière, d'une part, les problèmes relatifs à l'accès des chercheurs et chercheuses

37 Charlie Winter *et al.* (2020) « Online Extremism: Research Trends in Internet Activism, Radicalization and Counter-strategies », *International Journal of Conflict Violence* vol. 14
38 *Ibid.*
39 Department of Security Studies and Criminology, « Mapping Networks »
40 Meleagrou-Hitchens et Kaderbhai, « Research Perspectives on Online Radicalisation »

aux données, qui influe énormément sur le type de littérature analysée et sa qualité, et, d'autre part, le niveau de collaboration avec le secteur des technologies.

Les premières préoccupations sur l'état de la recherche en matière de terrorisme portaient sur l'absence d'accès aux données et l'absence de partage de données par les autorités[41]. Mais la recherche empirique[42] et l'utilisation de données primaires[43] dans l'étude du terrorisme et de l'extrémisme ont beaucoup évolué depuis les premières critiques portant sur l'absence de recherche guidée par les données[44]. En ce qui concerne le rôle joué par les technologies dans l'extrémisme, toutefois, bien qu'Internet soit inondé de données, comme nous l'avons vu dans les nombreuses analyses documentaires susmentionnées, le fait est que nous manquons encore d'études guidées par les données sur le rôle des technologies dans la radicalisation en ligne[45]. Les auteurs de l'article « Terrorist Use of the Internet by the Numbers », publié en 2017, concluent, à partir de l'analyse de 200 résumés de publications sur « la radicalisation en ligne », que seuls 6,5 % des articles sont fondés sur une forme de données, et que 2 % de ces études seulement utilisent des données primaires[46]. Les examens systématiques de 2018 et 2019, décrits plus hauts, sont parvenus aux mêmes conclusions.

En 2020, Ryan Scrivens, Paul Gill et Maura Conway ont observé, dans un article actualisé sur la façon de progresser dans la recherche sur le rôle d'Internet dans l'extrémisme violent, que le problème d'accès, de collecte et d'interprétation des données primaires existe toujours[47]. Leurs suggestions pour faire avancer les connaissances sur cette question, au nombre de cinq, tournent principalement autour des données. Ils proposent notamment de « recueillir des données primaires auprès de plusieurs types de populations » et de « rendre accessibles aux chercheurs et chercheuses et sur des plateformes faciles d'utilisation les archives de contenus à caractère extrémiste violent publiés en ligne »[48]. Ces problèmes liés aux preuves empiriques ont empêché les universitaires de parvenir à des conclusions convaincantes[49].

Tout à fait ironiquement, alors que la recherche sur le terrorisme commençait tout juste à intégrer des données primaires sur l'utilisation des plateformes de médias sociaux par les extrémistes, les principales entreprises de médias sociaux ont commencé à expulser de façon constante et définitive les acteurs extrémistes violents et à appliquer leurs conditions d'utilisation de façon plus stricte. Le fait que le débat sur le rôle d'Internet n'est toujours pas réglé s'explique notamment par des problèmes dans l'accès aux données, qui demeurent entre les mains des sociétés technologiques. C'est pourquoi une autre approche

41 M. Sageman (2014) « The stagnation in terrorism research », *Terrorism and Political Violence* vol. 26 n° 4 : p. 565–80, DOI : 10.1080/09546553.2014.895649
42 Sarah Knight et David A. Keatley (2020) « How can the literature inform counter terrorism practice? Recent advances and remaining challenges », *Behavioral Sciences of Terrorism and Political Aggression* vol. 12 n° 3 : p. 217–30, DOI : 10.1080/19434472.2019.1666894
43 Bart Schuurman (2020) « Research on Terrorism, 2007–2016 Review of Data, Methods, and Authorship », *Terrorism and Political Violence* vol. 32 n° 5 : p. 1 011–26, DOI : 10.1080/09546553.2018.1439023
44 Bart Schuurman et Quirine Eijkman (2013) « Moving Terrorism Research Forward: The Crucial Role of Primary Sources », ICCT Background Note, https://www.icct.nl/app/uploads/download/file/Schuurman-and-Eijkman-Moving-Terrorism-Research-Forward-June-2013.pdf
45 Gill *et al.*, « Terrorist Use of the Internet by the Numbers »
46 *Ibid.*
47 Ryan Scrivens, Paul Gill et Maura Conway (2020) « The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research », in T. J. Holt, A. M. Bossler (dir.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, https://doi.org/10.1007/978-3-319-78440-3_61
48 *Ibid.*
49 Meleagrou-Hitchens et Kaderbhai, « Research Perspectives on Online Radicalisation »

est nécessaire pour tenter de contribuer aux connaissances actuelles sur le rôle d'Internet dans l'extrémisme et le terrorisme, et plus particulièrement sur la collaboration entre le monde de la recherche et les plateformes de médias sociaux, qui détiennent la plupart des données pertinentes pour l'étude du rôle des technologies dans le processus de radicalisation menant à la violence.

3 Enquête

Le Lowy Institute a mené l'enquête auprès des chercheurs et chercheuses spécialisé·e·s dans le terrorisme et l'extrémisme violent afin de compléter les études passées consacrées à l'influence d'Internet sur l'extrémisme, de comprendre les conclusions qui n'avaient pas nécessairement été prises en compte par la littérature analysée précédemment, et d'appréhender le niveau de collaboration entre la recherche et le secteur des technologies.

Une base de données contenant des universitaires et spécialistes siégeant au comité de rédaction des principales revues du secteur des études du terrorisme et de l'extrémisme, à savoir *Studies in Conflict and Terrorism*, *Terrorism and Political Violence*, *Critical Studies on Terrorism*, *Journal for Policing Intelligence and Counterterrorism*, *CTC Sentinel*, *Perspectives on Terrorism*, *Journal of Democracy and Security*, *Journal for DeRadicalization*, *Behavioral Sciences of Terrorism and Political Aggression* et *Dynamics of Asymmetric Conflict*, a été créée à partir de différentes sources. Des correspondants associés du GNET et contributeurs à GNET Insights ayant travaillé sur les liens entre Internet et extrémisme ont également été ajoutés à cette base de données, de même que d'autres spécialistes membres d'instituts de recherche et de réseaux reconnus, comme le Program on Extremism de l'Université George Washington, Resolve Network, le Centre for the Analysis of Radical Right, Vox Pol, l'Institute for Strategic Dialogue, le National Consortium for the Study of Terrorism and Responses to Terrorism, Hadayah, AVERT Research Network et le TSAS. Outre ces chercheurs et chercheuses établi·e·s, de jeunes chercheurs et chercheuses et d'autres expert·e·s travaillant sur les liens entre terrorisme et technologie ont été identifié·e·s au travers de programmes de colloques, tels que la Conférence TASM sur le terrorisme et les médias sociaux de l'Université de Swansea.

Un questionnaire en ligne a été envoyé aux personnes figurant dans la base de données, qui ont été invitées à le partager avec d'autres personnes ayant des compétences pertinentes. Les personnes interrogées avaient le choix de conserver leur anonymat et n'étaient pas tenues de fournir leur nom ou leur affiliation. Près de 158 chercheurs et chercheuses dans le domaine du terrorisme et de l'extrémisme violent ont répondu à l'enquête, dont le présent rapport reprend certaines des conclusions en présentant les réponses aux 44 questions posées aux participant·e·s, dont la plupart sont reproduites ici.

La démarche consistant à réaliser une enquête auprès de spécialistes présente des limites. Les résultats indiqués ici sont fondés sur un échantillon non aléatoire et ne représentent que les points de vue des personnes ayant répondu au questionnaire. En dehors des critères décrits ci-dessus pour construire la base de données de participant·e·s potentiel·le·s à l'enquête, nous n'avons pas élaboré de méthode visant à déterminer le niveau d'engagement de ces derniers sur les problématiques liées à la technologie et à l'extrémisme. Le fait que de nombreuses personnes interrogées aient choisi de conserver

leur anonymat nous a empêchés de déterminer ou de vérifier leur niveau d'expertise et d'expérience dans le domaine de la recherche. Il est par ailleurs possible que des universitaires et spécialistes ayant une expérience pertinente dans ce domaine n'aient pas répondu à l'enquête.

Concernant l'affiliation des participant·e·s à l'enquête, 72 % des 84 personnes ayant choisi de répondre à la question « affiliation actuelle » ont indiqué être issues principalement du monde universitaire ou de la recherche, et 12 % d'entre elles ont déclaré travailler pour des groupes de réflexion ou instituts stratégiques. Les autres étaient issues de divisions de recherche de sociétés technologiques, d'organisations de conseil ou encore d'organisations non gouvernementales et de la société civile. La plupart des participant·e·s (n=158) avaient pour champ de recherche principal les sciences politiques (42 %), tandis que les autres travaillaient dans les domaines de la sociologie, de la criminologie, de la psychologie, des communications et de l'histoire.

La plupart des personnes figurant dans la base de données, et donc des participant·e·s à l'enquête (n=158), ont par ailleurs déclaré cibler leurs recherches sur les régions Amérique du Nord (44 %) et Europe (48 %), probablement en raison du fait qu'une majorité d'entre elles travaille dans ces régions ou en est originaire. Le Moyen-Orient (23 %), l'Asie (15 %) et l'Océanie (20 %) figuraient aussi parmi les zones géographiques faisant l'objet de recherches (les participant·e·s ayant la possibilité d'en indiquer plusieurs). Ceci peut également tenir au fait que le monde de la recherche s'intéresse actuellement aux menaces que représente l'extrême droite en Amérique du Nord, en Europe, en Océanie et, dans une moindre mesure, en Asie.

À noter tout de même qu'à la question « Sur quelle idéologie extrémiste vos recherches ont-elles porté ? », les personnes sondées (n=158), invitées à choisir toutes les réponses applicables, ont tout autant répondu « djihadiste » qu'« extrême droite » (79 % et 80 % respectivement). Un nombre plus faible de participant·e·s à l'enquête a également répondu « extrémisme violent à motivation raciale ou ethnique » (41 %), « extrême gauche » (29 %), « incel » (22 %) et autres (17 %) à cette question.

Le rôle d'Internet et des médias sociaux dans l'extrémisme

La première partie de l'enquête portait sur le point de vue des spécialistes concernant le rôle d'Internet, et plus particulièrement des médias sociaux, dans l'extrémisme. Les questions ont été formulées de façon à ne pas solliciter l'avis ou les impressions des personnes interrogées, mais à les inciter à fonder leurs réponses sur des « recherches empiriques » qu'elles auraient elles-mêmes menées, lues ou exploitées dans le cadre de leur travail.

La première question a cherché à obtenir leur point de vue sur le fait de savoir si les activités extrémistes en ligne satisfaisaient le désir d'une action concrète ou incitaient, encourageaient ou poussaient les individus à agir dans la vie réelle. Interrogées sur le fait de savoir si les communications par Internet et les activités en ligne des acteurs extrémistes « soutiennent, encouragent ou favorisent la commission d'actes préjudiciables dans la vie réelle », « satisfont à elles seules

un désir d'action ou de participation à l'extrémisme » ou « les deux », la majorité des personnes sondées (60 %) ont répondu qu'elles « soutiennent, encouragent ou favorisent la commission d'actes préjudiciables dans la vie réelle » ou les deux (36 %). Elles étaient peu nombreuses à estimer que les seules activités en ligne satisfaisaient un désir d'action ou de participation à l'extrémisme (moins d'1 %). Les participant·e·s à l'enquête ont indiqué que les activités sur Internet facilitaient la planification et l'exécution d'attentats (p. ex., logistique, financement, ressources humaines) ; favorisaient la provocation ou l'exercice d'une influence en vue de commettre des violences ; et encourageaient la glorification d'attentats passés susceptibles d'en inspirer d'autres. Plusieurs d'entre eux ont également souligné que les « vidéos des djihadistes [par exemple] détenues par des personnes arrêtées ou poursuivies pour actes de terrorisme sont un indicateur de la fonction de soutien [d'Internet] », comme le montrent certaines études portant sur des djihadistes prisonniers qui ont indiqué que la communication les avait fortement influencés. Le point de vue de la majorité des personnes interrogées, selon lequel l'activité en ligne peut soutenir, encourager ou favoriser la commission d'actes préjudiciables dans la vie réelle, concorde avec les conclusions récentes d'un examen approfondi de la « participation électronique » mené aux États-Unis et fondé sur un échantillon représentatif. Cette étude conclut que « les formes d'expression et d'interaction en ligne [sont] associées à une plus grande participation des citoyens dans la vie réelle »[50].

Il est intéressant d'observer que la plupart des participant·e·s a conclu que les activités en ligne conduisent à la commission d'actes préjudiciables dans la vie réelle. En effet, il existe des recherches, de même que des participant·e·s, qui avancent que certains individus ne se limitent qu'à des activités en ligne et ne représentent pas une menace dans la vie réelle, parce que leur activité en ligne a satisfait leur désir d'exprimer et de défendre leurs points de vue et d'extérioriser leurs doléances[51]. Par ailleurs, certaines études passées sur les djihadistes avaient conclu que la participation virtuelle pouvait avoir la même légitimité et les mêmes impacts que les activités hors ligne, atténuant ainsi potentiellement le besoin de commettre des actes dans la vie réelle. Selon Akil Awan et d'autres chercheurs et chercheuses, le « djihad virtuel » ou le « djihad médiatique » constituent une solution alternative légitime et crédible au militantisme dans le monde réel[52]. Le califat virtuel de l'État islamique, par exemple, était tout aussi important[53] que son califat territorial en Syrie et en Iraq, avec lequel il entretenait des liens très étroits[54].

De plus, la dichotomie en ligne/hors ligne s'estompe peu à peu à mesure que l'usage des technologies s'introduit dans les fonctions de la vie quotidienne. Selon un·e participant·e à l'enquête, « les actes préjudiciables commis dans la vie réelle [peuvent] recouvr[ir] des actions commises sur la toile. Ces dernières ont un véritable impact sur la réalité. Le swatting, le trollage, le harcèlement, le doxing, les

50 K. Tai, G. Porumbescu et J. Shon (2020) « Can e-participation stimulate offline citizen participation: an empirical test with practical implications », DOI : 10.1080/14719037.2019.1584233

51 J. Suler (2004) « The online disinhibition effect », *Cyberpsychology and Behavior*, DOI : 10.1089/1094931041291295

52 A. Hoskins, A. Awan et B. O'Loughlin (2011) *Radicalisation and Media: Connectivity and Terrorism in the New Media Ecology* (1e éd.), Routledge, https://doi.org/10.4324/9780203829677

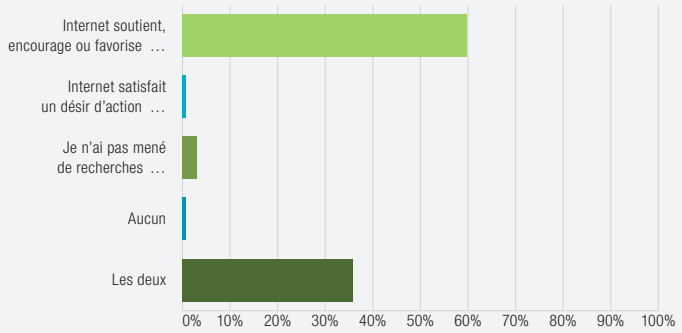
53 Charlie Winter (2015) « The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy », Quilliam, https://www.stratcomcoe.org/charlie-winter-virtual-caliphate-understanding-islamic-states-propaganda-strategy

54 Haroro Ingram et Craig Whiteside (2017) « In Search of the Virtual Caliphate », *War on the Rocks*, https://warontherocks.com/2017/09/in-search-of-the-virtual-caliphate-convenient-fallacy-dangerous-distraction/

insultes sur Internet ont des effets importants dans la vraie vie. » Les communications et activités favorisées par Internet ont entraîné une fusion des cadres numérique et physique[55], qui met en lumière le besoin de procéder à une conceptualisation plus globale des sphères virtuelle et réelle. D'autres personnes ont émis des réserves en soulignant que, si elles étaient d'accord avec la conclusion selon laquelle les activités en ligne conduisent à la commission d'actes préjudiciables dans la vie réelle, « ce processus n'est ni linéaire, ni unidirectionnel. Les dynamiques en ligne et hors ligne se cocréent et se soutiennent mutuellement. »

Q7 Avez-vous observé, dans les recherches empiriques sur l'extrémisme et les technologies que vous avez menées ou consultées, qu'Internet favorisait la communication et les activités en ligne ?

Réponses : 134 Abstentions : 24



CHOIX DE RÉPONSES	RÉPONSES	
Internet soutient, encourage ou favorise la commission d'actes préjudiciables dans la vie réelle.	59,70 %	80
Internet satisfait un désir d'action ou de participation par les seules activités en ligne.	0,75 %	1
Je n'ai pas mené de recherches ou consulté d'articles sur ce sujet.	2,99 %	4
Aucun	0,75 %	1
Les deux	35,82 %	48
TOTAL		134

Cette vaste question a ensuite été décomposée en plusieurs autres questions portant sur l'utilisation d'Internet par les extrémistes pour lever des fonds, recruter, mobiliser et planifier des actions violentes.

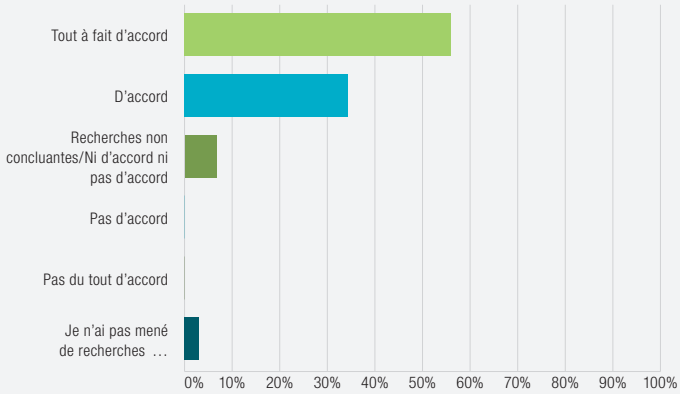
Bon nombre de participant·e·s à l'enquête ont indiqué que les communications par Internet avaient facilité le recrutement d'individus au sein de mouvements extrémistes. Près de 90 % d'entre eux étaient d'accord ou tout à fait d'accord avec cette affirmation. S'il semble y

55 D. Valentini, A. M. Lorusso et A. Stephan (2020) « Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization », *Frontiers in Psychology* n° 11 : p. 524, https://doi.org/10.3389/fpsyg.2020.00524 ; B. Ducol (2015) « A Radical sociability: in defense of an online/offline multidimensional approach to radicalization », in M. Bouchard (dir.) *Social Networks, Terrorism and Counter-Terrorism: Radical and Connected* (New York, NY : Routledge): p. 82–104

avoir un vaste consensus sur la question, le « recrutement » en ligne n'est toutefois pas bien défini ou conceptualisé. Celui-ci pourrait prendre la forme de processus de recrutement spécifiques menés à l'aide de mécanismes assistés par ordinateur ou de l'exercice d'une influence sociale de grande ampleur, ou encore se traduire par la création de communautés résultant des efforts de communication stratégique déployés par les groupes extrémistes en ligne.
Les recherches comparatives sur l'environnement de recrutement antérieur et postérieur à Internet sont rares, voire inexistantes. Mais les participant·e·s s'accordent pour dire qu'Internet, plus que toute autre technologie du passé, a permis aux messages à caractère extrémiste de circuler plus largement et donné aux groupes extrémistes un accès plus vaste, plus rapide et plus efficace à des recrues potentielles. Selon une personne, « plusieurs recherches ont montré comment les médias sociaux ont permis à des individus autrement dépourvus de liens mutuels d'atteindre et d'être atteints par les groupes extrémistes, et suppriment pour ces derniers la nécessité de se tourner vers des structures organisationnelles formelles pour recruter ».

Q9 L'utilisation des communications par Internet et/ou des plateformes de médias sociaux par les acteurs extrémistes a-t-elle facilité le recrutement d'individus au sein de leurs mouvements.

Réponses : 134 Abstentions : 24

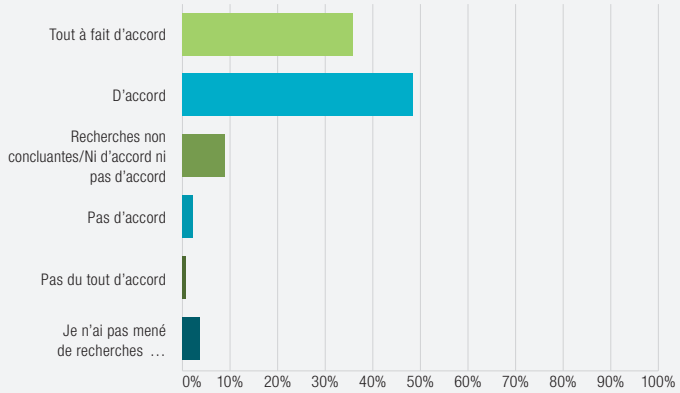


CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait d'accord	55,97 %	75
D'accord	34,33 %	46
Recherches non concluantes/Ni d'accord ni pas d'accord	6,72 %	9
Pas d'accord	0,00 %	0
Pas du tout d'accord	0,00 %	0
Je n'ai pas mené de recherches ou consulté d'articles sur ce sujet.	2,99 %	4
TOTAL		134

De même, la plupart des personnes sondées (84 %) ont indiqué être d'accord ou tout à fait d'accord avec le fait qu'Internet avait facilité la planification d'attentats ou la mobilisation en faveur de la violence. L'une d'elles a déclaré à propos du rôle d'Internet : « Internet, et plus particulièrement les communications chiffrées des médias sociaux, ont conduit à une multiplication des échanges d'informations et de ressources, à un accroissement du soutien tactique et logistique et à une hausse des contacts en temps réel, ce qui a éliminé ou réduit les obstacles à la planification d'attentats qui existaient auparavant ». Mais si Internet a facilité la recherche, la planification et la coordination d'actes violents, il constitue également une bénédiction pour les autorités chargées de l'application des lois. De nombreux complots ont été déjoués, et leurs instigateurs poursuivis, grâce aux preuves recueillies sur les plateformes virtuelles. Un grand nombre de participant·e·s a émis des réserves, en indiquant que si les communications par Internet, et en particulier les communications chiffrées, facilitent la mobilisation, la planification détaillée des attaques a, quant à elle, souvent lieu dans la vie réelle, en particulier si le plan est complexe.

Q10 L'utilisation des communications par Internet et/ou des plateformes de médias sociaux par les acteurs extrémistes a facilité la planification d'attaques violentes/la mobilisation à cette fin.

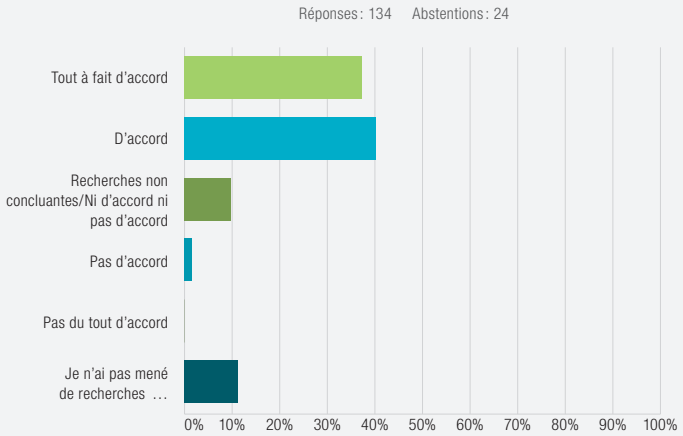
Réponses : 134 Abstentions : 24



CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait d'accord	35,82 %	48
D'accord	48,51 %	65
Recherches non concluantes/Ni d'accord ni pas d'accord	8,96 %	12
Pas d'accord	2,24 %	3
Pas du tout d'accord	0,75 %	1
Je n'ai pas mené de recherches ou consulté d'articles sur ce sujet.	3,73 %	5
TOTAL		134

Par ailleurs, la plupart des personnes interrogées ont déclaré être d'accord ou tout à fait d'accord (78 %) avec le fait que les communications par Internet avaient facilité la levée de fonds par les acteurs extrémistes. Internet a favorisé les échanges de fonds anonymes et sécurisés sous forme de dons collaboratifs, de ventes de marchandises, de revenus publicitaires des chaînes de diffusion, et de cryptomonnaie. Un·e participant·e a fait valoir que de nombreux groupes ou individus extrémistes avaient créé des entreprises commerciales en ligne ; ils sont motivés par des « incitations monétaires à rendre le contenu de leurs sites aussi sensationnel et attrayant que possible tout en restant suffisamment vagues pour attirer le plus grand nombre de spectateurs possible ».

Q11 L'utilisation des communications par Internet et/ou des plateformes de médias sociaux par des acteurs extrémistes a facilité la levée de fonds.



CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait d'accord	37,31 %	50
D'accord	40,30 %	54
Recherches non concluantes/Ni d'accord ni pas d'accord	9,70 %	13
Pas d'accord	1,49 %	2
Pas du tout d'accord	0,00 %	0
Je n'ai pas mené de recherches ou consulté d'articles sur ce sujet.	11,19 %	15
TOTAL		134

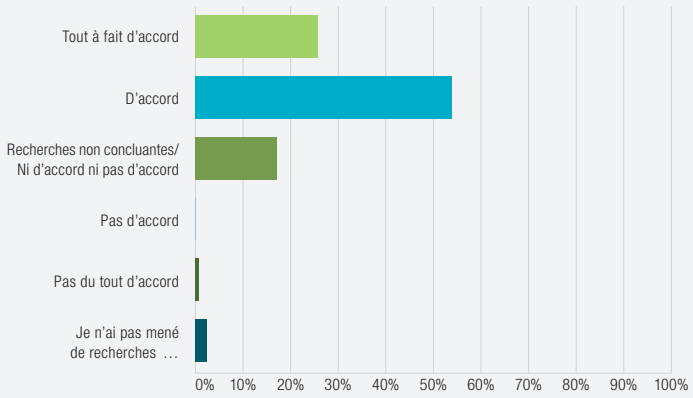
Les réponses des participant·e·s à l'enquête étaient moins tranchées concernant la question de savoir si l'exposition et l'intérêt porté à des contenus à caractère extrémiste entraînaient la commission d'actes préjudiciables dans la vie réelle. En examinant l'exposition aux contenus plutôt que les « activités en ligne » (communication, levée de fonds, recrutement, etc.), les personnes interrogées ont suggéré, conformément aux analyses documentaires menées, que l'intérêt porté aux contenus à

caractère extrémiste peut être un facteur contributif mais pas un facteur causal, déterminant ou suffisant. Selon l'une d'entre elles, « il existe de nombreux facteurs de disposition qui font que les interactions avec des contenus à caractère extrémiste conduisent à la commission d'actions dans la vie réelle, et le lien de causalité ne sera pas perceptible ».

Ce consensus sera toutefois peut-être remis en cause ultérieurement puisque, comme l'a souligné la majorité des participant·e·s à l'enquête, les « recherches menées [à cet égard] n'ont pas été concluantes ». De nombreuses personnes ont déclaré « ne pas avoir suffisamment de données probantes sur cette question », mentionné « l'absence de données de bonne qualité », affirmé que « la recherche est fondée sur un nombre très limité de données » et souligné « le très faible nombre de recherches empiriques mettant en exergue clairement l'existence d'un lien entre l'exposition/l'interaction avec les contenus à caractère extrémiste et la commission d'actes préjudiciables dans la vie réelle ». Ces réponses font de nouveau écho aux préoccupations anciennes concernant l'accès aux données dans ce domaine de recherche.

Q13 L'exposition et l'intérêt porté aux contenus à caractère extrémiste en ligne contribuent à la commission d'actes préjudiciables dans la vie réelle.

Réponses : 128 Abstentions : 30



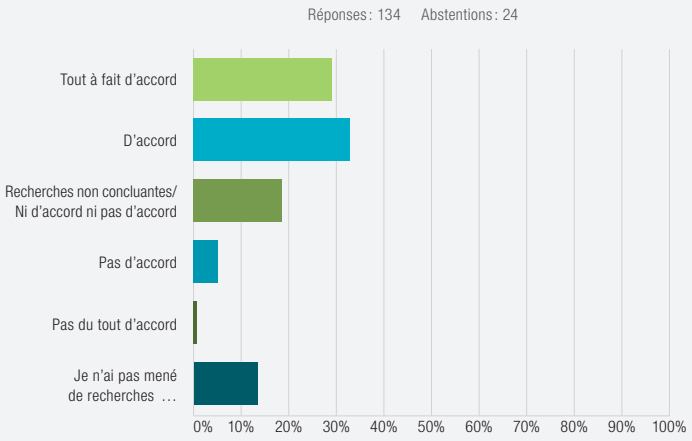
CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait d'accord	25,78 %	33
D'accord	53,91 %	69
Recherches non concluantes/Ni d'accord ni pas d'accord	17,19 %	22
Pas d'accord	0,00 %	0
Pas du tout d'accord	0,78 %	1
Je n'ai pas mené de recherches ou consulté d'articles sur ce sujet.	2,34 %	3
TOTAL		128

À la question de savoir comment certains individus avaient eu accès ou avaient été exposés à des contenus à caractère extrémiste, par le biais notamment de la fonction de recommandation algorithmique des plateformes de médias sociaux, les personnes sondées ont confirmé que cette technologie contribuait de façon notable à l'amplification des contenus (les réponses « D'accord » et « Tout à fait d'accord » ayant obtenu 62 % des réponses), mais se sont avérées plus circonspectes quant au fait de savoir si elle jouait un rôle dans la radicalisation progressive des individus. Nombre d'entre elles ont souligné que la recherche ne permettait pas de trancher cette question ou qu'il n'existait pas suffisamment d'études sur le rôle

joué par les recommandations algorithmiques dans le processus de radicalisation. Pour reprendre les termes de l'une d'entre elles, cette question « nécessite des connaissances plus perfectionnées sur la socialité imbriquée et les économies sociales relatives à la façon dont les communautés d'utilisateurs interagissent avec les contenus qu'elles visionnent et l'intérêt qu'elles y portent ».

La recherche relative aux contenus à caractère extrémiste et aux recommandations algorithmiques est largement axée sur YouTube[56] ; une personne sondée a indiqué avoir mené des recherches sur les recommandations algorithmiques et être parvenue à la conclusion que les « algorithmes de recommandation jouent un rôle central dans le recrutement, la radicalisation et la propagande ». Selon une autre personne, il existe « des preuves convaincantes selon lesquelles les algorithmes de recommandation peuvent, à tout le moins, désensibiliser, ce qui peut réduire l'inhibition de l'internaute face à la violence. (…) La recherche postule que la nature immersive des médias sociaux, y compris leurs algorithmes de recommandation, peut modifier la perception qu'a l'internaute de la réalité et créer un sentiment d'imminence poussant à l'action immédiate »[57].

Q12 Les algorithmes de recommandation des plateformes technologiques peuvent être un facteur important dans la radicalisation progressive d'un individu.



CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait d'accord	29,10 %	39
D'accord	32,84 %	44
Recherches non concluantes/Ni d'accord ni pas d'accord	18,66 %	25
Pas d'accord	5,22 %	7
Pas du tout d'accord	0,75 %	1
Je n'ai pas mené de recherches ou consulté d'articles sur ce sujet.	13,43 %	18
TOTAL		134

Les personnes interrogées qui connaissaient le sujet ou menaient des recherches sur cette question ont eu tendance à répondre à la question de savoir si *la modération de contenu, c'est-à-dire le retrait*

56 Ribeiro *et al.* (2019) « Auditing Radicalization Pathways on YouTube », *Computers and Society* ; selon Derek O'Callaghan *et al.* et Tania Bucher, il existerait un lien solide entre les algorithmes et le comportement social sur YouTube.

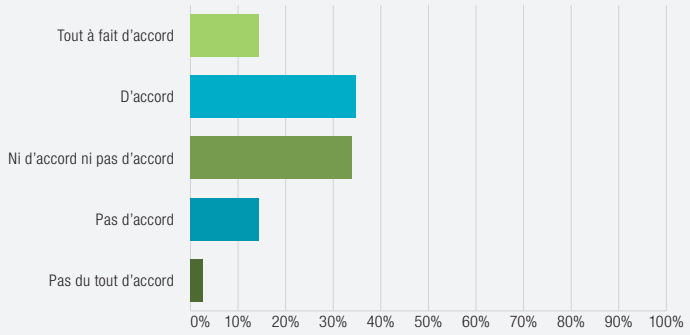
57 J. Berger (2015) « The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion », *Perspectives on Terrorism* vol. 9 n° 4, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/444

ou la suppression des contenus à caractère extrémiste, était un moyen efficace pour lutter contre l'extrémisme et réduire la commission d'actes préjudiciables dans la vie réelle qu'elles étaient « d'accord » ou « tout à fait d'accord » (48 %) ou que « les recherches n'étaient pas concluantes » (37,5 %). Un petit nombre de participant·e·s à l'enquête n'avait pas mené de recherches ni consulté d'articles sur le sujet (7,8 %). Les nombreuses personnes sondées qui se disaient d'accord avec le fait qu'il s'agissait d'un moyen efficace pour lutter contre l'extrémisme et réduire la commission d'actes préjudiciables dans la vie réelle ont également observé qu'il ne s'agissait que d'une intervention parmi d'autres ; selon l'une d'entre elles, il s'agit d'« une pièce du puzzle que représente la stratégie générale ; cette mesure ne suffit probablement pas à elle seule à lutter efficacement contre l'extrémisme dans la sphère numérique ».

Près de 49 % des personnes interrogées ont toutefois déclaré que la modération de contenu avait un impact sur leur capacité à accéder aux données et à mener des recherches sur ce sujet, et 34 % d'entre elles n'étaient ni d'accord ni pas d'accord, laissant entendre que cette question ne s'inscrivait pas dans leurs recherches. Certaines ont indiqué que la modération de contenu avait entraîné un changement de cap dans la recherche et que « les contenus qui ont été bloqués, supprimés ou rendus inaccessibles ne pouvaient être étudiés ». Bon nombre d'entre elles ont avancé que l'archivage des contenus et comptes extrémistes devait être plus systématique, et une personne a proposé que « les plateformes fournissent aux chercheurs et chercheuses certifié·e·s un accès aux contenus modérés ». La Plateforme d'analyse des contenus à caractère terroriste, développée par Tech Against Terrorism et Sécurité publique Canada, est l'une des initiatives visant à alerter les sociétés technologiques partenaires sur la présence de contenus à caractère terroriste sur leurs plateformes, aux fins à la fois de suppression, mais aussi d'archivage dans une base de données de contenus vérifiés de ce type pour la recherche[58].

Q36 Mon accès à des données de recherche pertinentes a été affecté par la modération de contenu et/ou la suppression de comptes.

Réponses : 112 Abstentions : 46



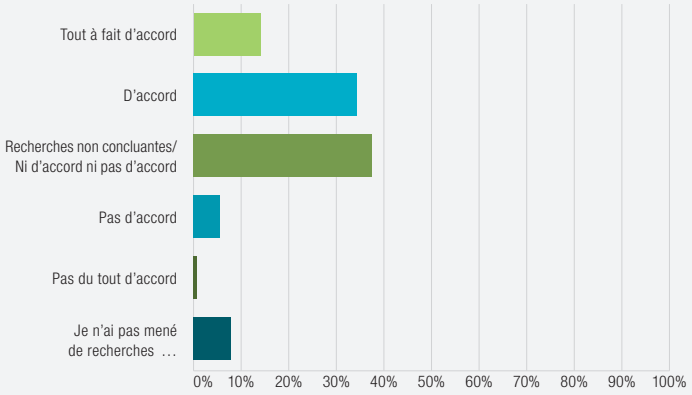
CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait d'accord	14,29 %	16
D'accord	34,82 %	39
Ni d'accord ni pas d'accord	33,93 %	38
Pas d'accord	14,29 %	16
Pas du tout d'accord	2,68 %	3
TOTAL		112

58 https://www.terrorismanalytics.org/blog/tcap-newsletter-january-2021-jfwmj

Selon plusieurs participant·e·s, la modération de contenu peut servir à limiter l'impact des influenceurs et influenceuses ou l'accessibilité des manuels d'information sur la conduite d'attentats, empêcher la création de réseaux et protéger les individus contre une exposition accidentelle ou passive aux contenus à caractère extrémiste. Elle ne permet toutefois pas de lutter directement contre les facteurs de radicalisation menant à la violence et ne doit pas être considérée comme une solution unique, mais plutôt comme un élément d'une stratégie plus vaste de lutte contre l'extrémisme violent. Une personne a également proposé que la modération de contenu se traduise par un ensemble de mesures : plutôt que de supprimer du contenu, il pourrait être plus efficace de mettre en place une échelle progressive de modération passant par la démonétisation, l'interdiction de rechercher certains contenus, le shadow banning (blocage total ou partiel d'un compte sans que son ou sa propriétaire en soit informé·e) et la limitation des interactions entre les utilisateurs et certains types de contenus.

Q14 La modération de contenu en ligne, c'est-à-dire le retrait ou la suppression des contenus à caractère extrémiste, est un moyen efficace pour lutter contre l'extrémisme et/ou réduire la commission d'actes violents ou préjudiciables dans la vie réelle.

Réponses : 128 Abstentions : 30

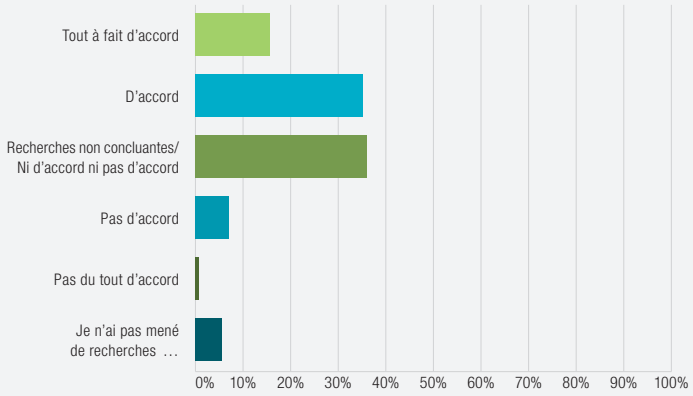


CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait d'accord	14,06 %	18
D'accord	34,38 %	44
Recherches non concluantes/Ni d'accord ni pas d'accord	37,50 %	48
Pas d'accord	5,47 %	7
Pas du tout d'accord	0,78 %	1
Je n'ai pas mené de recherches ou consulté d'articles sur ce sujet.	7,81 %	10
TOTAL		128

En ce qui concerne la suppression des comptes d'acteurs extrémistes, un peu plus de la moitié des personnes sondées se sont dites d'accord ou tout à fait d'accord (51 %) avec l'affirmation selon laquelle les mesures de suppression des comptes réduisent la commission d'actes préjudiciables dans la vie réelle et constituent un moyen efficace pour lutter contre l'extrémisme. Près de 41 % d'entre elles ont indiqué que les recherches n'étaient pas concluantes ou qu'elles n'avaient pas consulté d'articles sur le sujet. Seules 8 % d'entre elles n'étaient pas d'accord, voire pas du tout d'accord, avec cette affirmation.

Q15 La suppression des comptes des acteurs extrémistes sur les médias sociaux et d'autres plateformes technologiques réduit la commission d'actes préjudiciables dans la vie réelle et/ou est un moyen efficace de lutter contre le terrorisme.

Réponses : 128 Abstentions : 30



CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait d'accord	15,63 %	20
D'accord	35,16 %	45
Recherches non concluantes/Ni d'accord ni pas d'accord	35,94 %	46
Pas d'accord	7,03 %	9
Pas du tout d'accord	0,78 %	1
Je n'ai pas mené de recherches ou consulté d'articles sur ce sujet.	5,47 %	7
TOTAL		128

Les commentaires des participant·e·s à l'enquête tournaient autour de deux thématiques principales. La suppression de compte est utile, en ce qu'elle limite le rayonnement des acteurs extrémistes, en particulier des influenceurs, ces derniers étant obligés de se tourner vers d'autres plateformes constituées d'une base d'utilisateurs globale moins importante. Une personne a indiqué que cette mesure « limite considérablement leur rayonnement, ce qui, par défaut, réduit leur public. Nous savons aussi que, même s'ils reviennent, il est rare qu'ils récupèrent le même [nombre] de followers ». Cette mesure sert aussi à démonétiser les comptes à caractère extrémiste et limite ainsi leur financement et les flux de revenus. Tout comme la modération de contenu, la suppression de compte s'inscrit dans un effort plus large de lutte contre l'extrémisme violent.

La suppression de compte peut néanmoins aussi enflammer les passions et pousser les acteurs extrémistes vers des plateformes non modérées, de niche et parfois chiffrées, où ils peuvent continuer à interagir avec des contenus et réseaux extrémistes. Les réponses à la question de savoir si les acteurs dangereux ou extrémistes sont plus susceptibles de migrer vers une autre plateforme ou d'essayer de reconstituer leur public sur la même plateforme après une suspension (mais non une suppression finale) indiquent que nous ne disposons pas encore suffisamment de données ou d'études sur cette question. La majorité des participant·e·s à l'enquête a indiqué ne pas avoir mené de recherches ou consulté d'articles sur le sujet (30 %), tandis que les autres réponses étaient réparties entre les autres options.

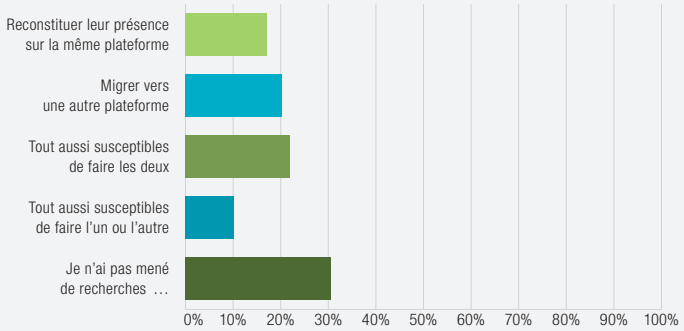
Certaines personnes ont par ailleurs souligné que la situation à cet égard a évolué. Alors que les acteurs dont les comptes avaient été

supprimés tentaient auparavant de reconstituer leur présence sur la même plateforme, ils semblent depuis peu migrer vers d'autres plateformes, avant l'interdiction définitive de leur compte, pour tenter de conserver leur public. Quelqu'un a donné l'exemple des « influenceurs et influenceuses de la droite alternative qui avaient reçu quelques "avertissements" et qui ont, de manière stratégique, communiqué leur intention de migrer avant l'interdiction définitive. Ces personnes d'influence avaient un large public qu'elles essayaient "d'emmener avec elles" sur des plateformes comme BitChute » de façon à conserver leurs sources de revenus et de donner à leur public le temps de s'ajuster à une nouvelle plateforme. Une autre personne sondée a indiqué que tout dépendait de la plateforme concernée. Si l'État islamique a fini par laisser tomber l'idée d'une présence sur Twitter, il a toutefois été plus persistant avec le maintien de sa présence sur Telegram, parce qu'il trouve les caractéristiques de la plateforme particulièrement utiles.

On craint que la suppression de comptes agisse comme incitatif à la radicalisation violente ou serve à consolider les points de vue extrémistes. Cette préoccupation, mentionnée par plusieurs participant·e·s, est potentiellement contredite par les recherches de Richard Rogers, lequel affirme que les acteurs dont les comptes ont été supprimés et qui migrent vers d'autres plateformes adoptent un langage plus modéré[59]. Il est utile de noter, toutefois, que la modération du langage utilisé n'est pas nécessairement un indicateur de modération des opinions ; cela peut signifier simplement que ces personnes répondent à un besoin de communication différent.

Q16 Les acteurs dangereux/extrémistes sont-ils plus susceptibles de tenter dans un premier temps de reconstituer leur présence en ligne sur la même plateforme lorsque leur compte a été suspendu OU de migrer vers une autre plateforme ?

Réponses : 128 Abstentions : 30



CHOIX DE RÉPONSES	RÉPONSES	
Reconstituer leur présence sur la même plateforme	17,19 %	22
Migrer vers une autre plateforme	20,31 %	26
Tout aussi susceptibles de faire les deux	21,88 %	28
Tout aussi susceptibles de faire l'un ou l'autre	10,16 %	13
Je n'ai pas mené de recherches ou consulté d'articles sur ce sujet.	30,47 %	39
TOTAL		128

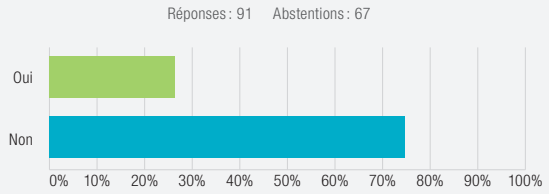
59 R. Rogers (2020) « Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media », *European Journal of Communication* vol. 35 n° 3 : p. 213–29, https://doi.org/10.1177/0267323120922066

Interactions entre la recherche et le secteur des technologies

La deuxième partie de l'enquête s'est intéressée aux interactions entre la recherche et le secteur des technologies lui-même. Nous avons cherché à savoir si les chercheurs et chercheuses interagissaient avec les technologies, et si oui, comment. Les réponses portant sur le type d'interactions mises en place entre la recherche et les sociétés technologiques et le niveau des relations établies étaient très contrastées, citant la réalisation de travaux en collaboration étroite avec les sociétés technologiques, la production conjointe de recherches, la communication d'informations sur les dernières recherches en cours ou l'absence totale d'interactions. Une grande partie de ces interactions avaient lieu dans le cadre du GIFCT ou de colloques universitaires. Plusieurs personnes interrogées ont fait part d'un certain cynisme concernant la collaboration du secteur des technologies avec la recherche. L'une d'entre elles a même déclaré : « les sociétés technologiques ne « collaborent » pas ; elles se contentent de faire croire qu'elles s'attaquent aux problèmes, tout en perpétuant leurs pratiques jusqu'à ce qu'une crise les oblige à changer ».

L'une des raisons, mais certainement pas la seule, poussant les chercheurs et chercheuses (47 % des personnes sondées) à collaborer davantage avec les sociétés technologiques est le souhait d'accéder aux données. Pourtant, 75 % des personnes interrogées ont répondu « non » à la question de savoir si elles avaient contacté une entreprise pour obtenir des données afin d'étayer leurs recherches. La plupart des personnes qui avaient demandé n'ont pu obtenir les données souhaitées. Certaines des personnes qui ont indiqué ne pas avoir, dans un premier temps, demandé aux entreprises de médias sociaux de leur communiquer des données, savaient que les politiques de ces dernières ne les autorisaient pas à y accéder, ou ne disposaient pas des canaux appropriés pour aborder leurs représentants. À la question de savoir si elles disposaient de moyens d'accès aux départements concernés de ces sociétés clairement définis pour discuter de leurs recherches ou si elles comprenaient leurs procédures d'accréditation en matière de collaboration de recherche ou d'accès aux données, la majorité des personnes sondées (46 % et 60 % respectivement) ont répondu par la négative. L'une d'elles a indiqué que le processus de demande de partage de données ou de collaboration en matière de recherche était « très opaque ». De nombreuses personnes ont reconnu ne pas connaître les opportunités d'interactions qui s'offraient à elles et ne pas savoir qui contacter ni comment les contacter, ou indiqué simplement que la création de liens avec le secteur technologique n'était pas une priorité pour elles.

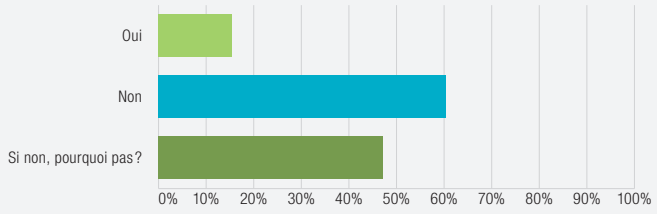
Q40 Avez-vous contacté une société technologique pour obtenir des données dans le but d'éclairer vos recherches ?



CHOIX DE RÉPONSES	RÉPONSES	
Oui	26,37 %	24
Non	74,73 %	68
Total personnes interrogées : 91		

Q41 Avez-vous pu obtenir ces données ?

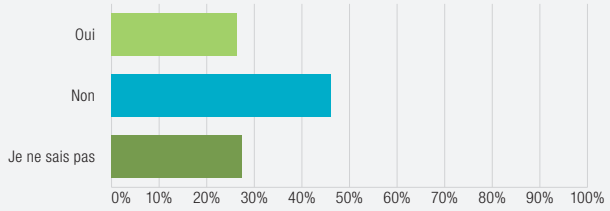
Réponses : 91 Abstentions : 67



CHOIX DE RÉPONSES	RÉPONSES	
Oui	15,38 %	14
Non	60,44 %	55
Si non, pourquoi pas ?	47,25 %	43
Total personnes interrogées : 91		

Q42 Disposez-vous de moyens d'accès aux départements des sociétés technologiques clairement définis pour discuter de vos recherches ?

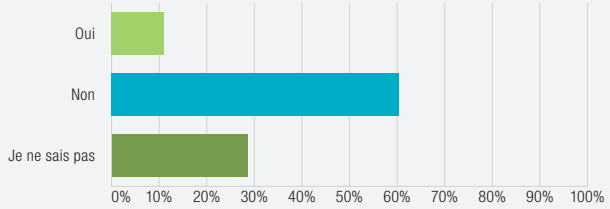
Réponses : 91 Abstentions : 67



CHOIX DE RÉPONSES	RÉPONSES	
Oui	26,37 %	24
Non	46,15 %	42
Je ne sais pas	27,47 %	25
TOTAL		91

Q43 Comprenez-vous les procédures d'examen mises en place par les sociétés technologiques pour approuver des projets de recherches ou autoriser l'accès aux données ?

Réponses : 91 Abstentions : 67

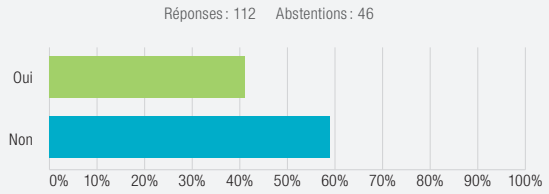


CHOIX DE RÉPONSES	RÉPONSES	
Oui	10,99 %	10
Non	60,44 %	55
Je ne sais pas	28,57 %	26
TOTAL		91

Concernant les autres contraintes liées aux données, 59 % des personnes interrogées ont répondu négativement à la question de savoir si les lois, procédures universitaires de validation en matière éthique et questions liées au respect de la vie privée avaient une incidence sur leur accès aux données, contre 41 % de réponses affirmatives. Cet écart s'explique par le fait que les processus universitaires de validation en matière éthique diffèrent d'un pays à l'autre et que les chercheurs et chercheuses ne travaillent pas tous pour une université. D'autres limites que l'obtention d'une validation en matière éthique ont été mentionnées : la possession de matériel en rapport avec le terrorisme est en effet une infraction dans certains pays, et l'étude de ce type de matériel et la recherche en la matière ne sont pas considérées comme une défense valable. La législation relative au RGPD a également été citée. Comme l'a souligné une personne, selon laquelle les procédures de validation en matière éthique et les questions de respect de la vie privée n'empêchaient pas d'accéder aux données, cette législation a forcé de nombreux chercheurs et de nombreuses chercheuses à recourir à des données secondaires.

Plusieurs personnes ont parlé de la difficulté à traiter avec les commissions d'examen ou comités de déontologie institutionnels. L'une d'entre elles a affirmé avoir « évité les questions de recherche qui auraient donné lieu à des échanges difficiles avec les commissions d'examen institutionnelles ». Ces commissions sont nombreuses à ne fournir une validation en matière éthique que si la collecte de données respecte les conditions d'utilisation de la plateforme utilisée, ce qui, compte tenu de la formulation de la plupart de ces textes, signifie en réalité qu'il est impossible d'accéder aux données. Selon un·e participant·e, ces commissions devraient se pencher sur la question de l'utilisation des données en ligne aux fins de recherche, parce que, comme l'ont souligné ses pairs, un nombre considérable d'entre elles avaient une « définition trop large de l'espace privé en ligne » et « les commissions déontologiques ne comprennent pas la nature de la recherche sur Internet/l'extrémisme ». En outre, le délai d'obtention d'une validation en matière éthique empêche la recherche d'accéder aux données ou de communiquer leurs conclusions sur ces données, puisque ces dernières sont susceptibles d'avoir été supprimées au moment où elle reçoit le feu vert pour poursuivre leurs activités.

Q32 Les procédures universitaires de validation en matière éthique et/ou les questions, politiques ou lois en matière de respect de la vie privée ont-elles eu une incidence sur votre capacité d'accéder aux données ?

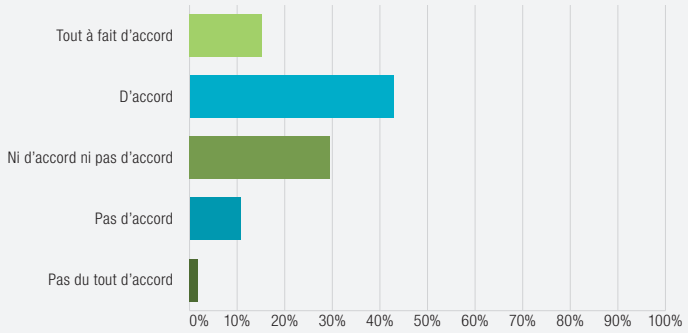


CHOIX DE RÉPONSES	RÉPONSES	
Oui	41,07 %	46
Non	58,93 %	66
TOTAL		112

Une autre question a porté sur le fait de savoir plus généralement si les « procédures universitaires de validation en matière éthique et/ou les questions, politiques ou lois en matière de respect de la vie privée [faisaient] obstacle à la recherche sur les acteurs et mouvements extrémistes ou dangereux présents sur Internet ». Les travaux de John Morrison, Andrew Silke et Eke Bont, qui affirment qu'« il n'existe jusqu'à présent aucun critère objectif pour aider les commissions d'examen à juger du risque ou des avantages liés à la recherche sur le terrorisme » font écho aux préoccupations des participant·e·s à l'enquête concernant la validation en matière éthique. Ces auteurs ont par conséquent élaboré récemment un cadre en matière d'éthique de la recherche applicable aux études sur le terrorisme, qui peut aider à satisfaire ce besoin[60].

Q31 Les procédures universitaires de validation en matière éthique et/ou les questions, politiques ou lois en matière de respect de la vie privée font obstacle à la recherche sur les acteurs et mouvements extrémistes ou dangereux sur Internet.

Réponses : 112 Abstentions : 46



CHOIX DE RÉPONSES	RÉPONSES	
Tout à fait d'accord	15,18 %	17
D'accord	42,86 %	48
Ni d'accord ni pas d'accord	29,46 %	33
Pas d'accord	10,71 %	12
Pas du tout d'accord	1,79 %	2
TOTAL		112

Si beaucoup de personnes sondées ont parlé des difficultés liées aux procédures universitaires de validation en matière éthique, plusieurs d'entre elles estimaient également que ces obstacles étaient pertinents et nécessaires : « ils imposent des contraintes à la recherche, mais sont globalement pertinents », ou « il est important de disposer de mesures strictes lorsque l'on travaille dans ces domaines, pour des raisons éthiques, mais aussi pour assurer la sécurité des chercheurs et des chercheuses. Je connais des chercheurs et chercheuses indépendant·e·s qui ont reçu des menaces en raison de la façon dont ils ou elles interagissaient avec leurs sujets de recherche extrémistes ».

60 John Morrison, Andrew Silke et Eke Bont (2021) « The Development of the Framework for Research Ethics in Terrorism Studies (FRETS) », *Terrorism and Political Violence*, 33:2, 271–289, DOI : 10.1080/09546553.2021.1880196

Les questions liées au respect de la vie privée, les procédures de validation en matière éthique, les conditions d'utilisation des plateformes et d'autres considérations de ce type ont compliqué l'étude, par la recherche, des activités en ligne des individus et/ou de l'intérêt qu'ils portent aux contenus à caractère extrémiste. Les personnes interrogées qui ont pu faire ces études se sont appuyées sur des « documents judiciaires liés à des affaires terroristes » et des données secondaires en libre accès, telles qu'articles de journaux, communiqués de presse, etc. D'autres ont pu se pencher sur les activités en ligne d'individus par le biais de questionnaires administrés directement à des détenus isolés et les déclarations de participants volontaires ou de groupes de discussion sur la question de savoir pourquoi et comment les jeunes s'intéressent aux contenus à caractère extrémiste. Seule une poignée de participant·e·s ont indiqué avoir été en mesure d'effectuer une analyse approfondie des activités en ligne, de procéder à des études longitudinales des individus en surveillant leur activité en ligne avant leur engagement dans des activités militantes, et de réaliser des études comparatives du comportement d'extrémistes violents et non violents en matière de publications. Les réponses précisent qu'il existe des recherches récentes dans ce domaine et que d'autres devraient paraître prochainement. Une personne a indiqué être « impliqué[e] dans l'acquisition de mégadonnées tirées de différentes plateformes de médias sociaux conformément à une requête déontologique approuvée, ce qui a permis de mieux comprendre les activités des individus en ligne en lien avec des contenus associés aux idéologies extrémistes violentes. »

4 Conclusion

Cette enquête vise à compléter les analyses documentaires portant sur le rôle de la technologie Internet dans l'extrémisme violent et à constituer un premier point d'interrogation sur l'état des interactions entre le secteur des technologies et la recherche. Il est ressorti de l'élaboration et de la synthèse des réponses à cette enquête que l'analyse du rôle joué par les technologies dans l'extrémisme violent est incroyablement complexe, pluridimensionnelle et encore contestée. La recherche empirique dans ce domaine est encore limitée, mais est aujourd'hui en pleine croissance.

Nous avons pu tirer des enseignements non seulement des réponses obtenues aux questions posées, mais aussi des questions qui n'ont pas été posées et des questions portant sur notre démarche. En effet, certaines personnes interrogées ont mis en lumière la nécessité de faire preuve de davantage de précision dans les questions. Nos questions ont globalement porté sur les « acteurs extrémistes », mais un grand nombre de personnes interrogées ont précisé que leurs réponses dépendaient du type d'acteur et de mouvement, et qu'il n'était pas possible de généraliser. De plus, nombre des questions posées sur l'incidence des technologies, et en particulier des médias sociaux, sur l'extrémisme violent, étaient comparatives par nature. Pourtant, comme l'a souligné une personne, il n'existe que très peu de recherches comparatives sur les environnements antérieur et postérieur à l'avènement d'Internet. Il s'agit là d'une lacune de la recherche, qu'il est difficile de combler et qui aura nécessairement une incidence sur la conception des questions des recherches et enquêtes futures.

En ce qui concerne la collaboration entre la recherche et le secteur des technologies, celle-ci semble potentiellement bénéfique, mais également difficile – de la même manière que les chercheurs et chercheuses spécialisé·e·s dans le terrorisme s'interrogent encore sur la collaboration avec les gouvernements et les agences de sécurité, et s'inquiètent de l'ampleur que prennent les aspects sécuritaires liés à la recherche universitaire. Certains chercheurs et certaines chercheuses ont émis des préoccupations similaires concernant la collaboration avec le secteur des technologies, entre autres inquiétudes, par exemple sur l'éthique de la collaboration avec des entreprises à but lucratif, l'opacité et l'absence de transparence des principales plateformes, leur nature réactive et les priorités divergentes en matière de recherche du secteur, ainsi qu'un certain scepticisme vis-à-vis du sérieux et de l'efficacité des mesures prises par les médias sociaux pour lutter contre l'extrémisme violent et la désinformation préjudiciable. On espère que les lacunes, difficultés et opportunités liées à la collaboration entre la recherche et le secteur des technologies mises en lumière dans cette enquête pourront être étudiées et traitées de manière plus approfondie.

Contexte politique

Cette section a été rédigée par Lucy Thomas et Constance Woollen, toutes deux adjointes de recherche au Policy Institute du King's College, à Londres. Elle fournit un aperçu du contexte politique dans lequel s'inscrit ce rapport.

Introduction

Nous étudions dans ce rapport le paysage politique et la législation relative au financement de la recherche dans la lutte contre le terrorisme en vigueur dans neuf pays et organisations. Les financements prennent différentes formes et proviennent de différentes sources. Il peut en effet s'agir de financements directs versés par une agence gouvernementale ou de financements indirects alloués au travers, par exemple, d'un conseil de recherche, comme c'est le cas au Royaume-Uni et en France. Certaines des recherches financées sont clairement destinées à étayer la prise de décisions politiques ; la Commission européenne, la Nouvelle-Zélande et les Nations Unies financent toutes des recherches visant à répondre à des besoins politiques spécifiques en matière de lutte contre le terrorisme. Ailleurs, comme au Royaume-Uni et en France, le versement de bourses aux étudiants en doctorat peut contribuer de façon moins directe aux stratégies actuelles de lutte antiterroriste, mais ouvrir la voie au recrutement de ces étudiants au sein des organes chargés de la sécurité nationale. La création de réseaux de partage des recherches actuelles en matière de lutte contre le terrorisme est également monnaie courante, cinq des neuf pays et organisations étudiés ici ayant fait ce choix au cours des dix dernières années (Canada, Commission européenne, France, Nouvelle-Zélande et Nations Unies).

Nous concluons notre rapport en abordant les enjeux éthiques généraux qui caractérisent de manière implicite la collaboration entre recherche et responsables politiques, et décrivons les mesures qui permettraient d'avancer vers la mise en place d'un programme de recherche en matière de lutte contre l'extrémisme violent (LEV) qui soit conforme à l'éthique. Il serait par exemple envisageable : 1) d'abandonner le paradigme « solutionniste » pour se concentrer sur l'incidence de la lutte contre le terrorisme sur les communautés racialisées et marginalisées et formuler des recommandations stratégiques visant à modifier les politiques en conséquence ; 2) de s'appuyer sur la recherche en matière de LEV pour plaider en faveur de politiques cherchant à réparer les violences historiques et structurelles ; 3) d'effectuer des recherches concernant l'incidence des politiques qui améliorent le sort des communautés, relatives par exemple aux investissements dans le logement et aux services d'appui à la santé mentale et utiliser, par conséquent, la recherche en matière de LEV pour plaider en faveur d'interventions différentes pour éviter le recours à la violence.

Recherche financée par l'État en matière de lutte contre l'extrémisme

Canada

La stratégie adoptée par le gouvernement canadien en matière de lutte contre le terrorisme et la radicalisation est vaste, et englobe des activités de renseignement et de sécurité traditionnelles, la collaboration avec la société civile, des initiatives collaboratives avec le secteur et la mise en place de services de police axés sur la communauté. Sa stratégie, telle qu'énoncée dans sa Stratégie nationale de lutte contre la radicalisation menant à la violence, comporte trois volets : concevoir des contre-discours en collaboration avec la société civile, appuyer la recherche relative à la LEV et développer des partenariats avec des initiatives internationales et des sociétés technologiques[61].

Le gouvernement canadien ayant fait des investissements dans la recherche l'un de ses objectifs annoncés, il n'est pas surprenant que son programme de recherche financée par l'État figure parmi les plus élaborés et engagés de ceux que nous passons en revue dans ce rapport. Sécurité publique Canada, la direction canadienne chargée des questions de sécurité publique et de préparation à l'urgence, héberge le Centre canadien d'engagement communautaire et de prévention de la violence, qui dirige la réponse de l'État en matière de LEV. Le Centre canadien, qui a vu le jour en 2017, est chargé de la coordination de différentes activités relatives à la LEV, telles que l'orientation stratégique, la collaboration avec différents intervenants, l'appui aux initiatives et interventions, et le financement et la réalisation de recherches. La recherche financée par le Centre comprend des bourses visant à « mieux comprendre la radicalisation menant à la violence et la meilleure façon de la combattre, et mobiliser la recherche aux personnes en première ligne pour prévenir la radicalisation menant à la violence »[62].

En collaboration avec le Fonds pour la résilience communautaire, une initiative qui travaille avec les organisations et communautés locales, le Centre a financé un ensemble de projets portant, entre autres, sur la résilience face aux discours haineux en ligne, l'étude de la communauté incel, les familles et la radicalisation menant à la violence, l'extrême droite au Québec, les initiatives de contre-discours. Des établissements d'enseignement supérieur canadiens et étrangers, des acteurs politiques tels que Moonshot CVE, des groupes de réflexion comme l'Institute for Strategic Dialogue, et des acteurs locaux et issus de la société civile comme l'hôpital de Boston pour enfants figurent parmi les parties prenantes et partenaires des recherches financées[63]. Le dernier appel à propositions publié couvrait la période 2018–2019. On ne sait donc pas précisément si les autorités canadiennes continuent de financer des recherches sur la LEV par ce biais[64].

61 « Stratégie nationale de lutte contre la radicalisation menant à la violence »., Sécurité publique Canada. Disponible à l'adresse : https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-fr.aspx
62 https://www.securitepublique.gc.ca/cnt/bt/cc/index-fr.aspx
63 https://www.securitepublique.gc.ca/cnt/bt/cc/fpd-fr.aspx
64 https://www.securitepublique.gc.ca/cnt/bt/cc/fpd-fr.aspx

Par ailleurs, le Réseau canadien de recherche sur le terrorisme, la sécurité et la société (TSAS), financé en 2012, appuie la recherche sur « la menace du terrorisme, les interventions sécuritaires de lutte contre le terrorisme, et l'incidence du terrorisme et de la sécurisation sur la société canadienne » et sa diffusion[65]. Le TSAS est une organisation indépendante d'étude qui mène fréquemment des recherches en collaboration avec différents services du gouvernement[66]. Elle vise principalement à cultiver la communication et la collaboration entre les universitaires de différents horizons, à faciliter les interactions et la collaboration entre la recherche et les responsables politiques, et à aider à encourager l'émergence d'une nouvelle génération élargie de chercheurs et chercheuses qui s'intéressent à ces domaines d'étude[67].

Commission européenne

La stratégie de lutte contre le terrorisme de la Commission européenne relève de la responsabilité de la Direction générale de la migration et des affaires intérieures (DG Home)[68]. La Commission finance la recherche dans le domaine de la lutte contre le terrorisme depuis environ 15 ans, et plus particulièrement depuis l'adoption du septième programme-cadre 2007–2013, qui prévoyait la réalisation des toutes premières recherches en matière de radicalisation[69]. Plus récemment, elle a publié et présenté aux responsables politiques des différentes institutions de l'UE deux communications (documents de politique générale) sur la prévention de la radicalisation. Le financement de la recherche en matière de lutte contre le terrorisme, et plus particulièrement la radicalisation, est au cœur de ces textes, qui poursuivent des objectifs plus axés sur la politique et orientés vers l'obtention de résultats que jamais.

La communication COM(2016) 379 a été publiée en 2016 en réaction aux attentats terroristes perpétrés sur le sol européen[70]. Elle visait à aider les « États membres (…) à prévenir la radicalisation conduisant à l'extrémisme violent sous forme de terrorisme »[71]. Dans cette communication, la Commission avance que le processus de radicalisation menant aux dernières attaques terroristes affichait de « nouvelles tendances », qui devaient être examinées de manière plus approfondie. Elle a donc introduit des priorités de recherche pour « combler davantage le fossé entre les universités et les spécialistes de la sécurité dans ce domaine »[72]. Ces recherches consacrées aux causes profondes de la radicalisation violente, qui visaient à fournir des outils concrets permettant de réaliser des interventions plus éclairées[73], ont été mobilisées dans le cadre d'Horizon 2020, « le plus important programme européen de tous les temps en matière de recherche et d'innovation », doté de près de 80 milliards d'euros de financements disponibles entre 2014 et 2020[74]. La volonté de la Commission d'impliquer un grand nombre d'acteurs dans sa stratégie de lutte antiterroriste est mise en évidence par la création d'un Centre

65 https://www.tsas.ca/about/
66 https://www.securitepublique.gc.ca/cnt/bt/cc/res-fr.aspx ; voir section « Le Réseau canadien de recherche sur le terrorisme, la sécurité et la société »
67 *Ibid.*
68 https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/radicalisation_en
69 https://ec.europa.eu/transport/themes/research/fp7_en
70 https://ec.europa.eu/transparency/regdoc/rep/1/2016/FR/COM-2016-379-F1-FR-MAIN-PART-1.PDF, p. 2
71 *Ibid.*, p. 3
72 *Ibid.*, p. 4
73 *Ibid.*, p. 5
74 https://ec.europa.eu/programmes/horizon2020//en/what-horizon-2020

d'excellence du réseau de sensibilisation à la radicalisation (RSR), aujourd'hui obsolète, un réseau d'intervenants des États membres visant à partager, entre autres, leurs connaissances sur le phénomène de radicalisation[75].

Une autre communication de la Commission, COM(2020) 795, adoptée en 2020, présente un programme de lutte antiterroriste beaucoup plus ambitieux pour l'UE[76]. Ce programme s'appuie sur les recherches financées par le septième programme-cadre pour la recherche et Horizon 2020 pour élaborer des plans visant à poursuivre la recherche relative à la lutte contre le terrorisme. Cette communication vise notamment à financer, spécifiquement, « les travaux de recherche menés à l'échelle de l'UE en matière de sécurité afin de renforcer la capacité de détection précoce et de mettre au point de nouvelles technologies dans le cadre du programme urbain pour l'UE »[77]. Ces recherches serviraient à renforcer la capacité de détection précoce des menaces terroristes potentielles grâce à l'intelligence artificielle et des projets impliquant des mégadonnées ; la lutte contre la radicalisation faisait encore une fois partie de la stratégie[78]. Ces recherches seront financées par le successeur d'Horizon 2020, Horizon Europe, qui devrait courir jusqu'à 2027[79]. Si les chercheurs et chercheuses, universitaires et instituts de recherche ne sont pas explicitement nommés dans cette communication, il est évident que l'UE souhaite que ces recherches soient orientées vers l'obtention de résultats, profondément intégrées dans le cycle d'élaboration de la politique de sécurité, et qu'elles répondent aux besoins cernés en matière de répression[80]. Outre la recherche financée par Horizon Europe, la Commission encourage, dans cette communication, le partage des recherches et des connaissances entre les responsables politiques, les praticien·ne·s et les spécialistes de la lutte contre le terrorisme. Elle propose de mettre en place un « pôle de connaissances » de l'UE sur la prévention de la radicalisation, similaire au RSR[81]. Celui-ci ne semble pas attaché à des possibilités de financement supplémentaires, mais guidera les chercheurs et chercheuses vers des possibilités de financement proposées dans le cadre de différents programmes de l'UE[82].

France

En France, le Comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR) régit la stratégie nationale de lutte contre le terrorisme[83]. Il réunit les ministres de l'Intérieur et de la Justice, entre autres[84], et est dirigé par le Premier ministre[85]. Le CIPDR finance directement certaines recherches. Le gouvernement français finance aussi des recherches en matière de lutte antiterroriste de manière indirecte, par le biais de l'Agence nationale de la recherche (ANR). Si les recherches financées par le CIPDR sont inextricablement liées à la stratégie française de lutte contre le terrorisme, la recherche

75 https://ec.europa.eu/transparency/regdoc/rep/1/2016/FR/COM-2016-379-F1-FR-MAIN-PART-1.PDF, p. 5
76 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0795&from=EN
77 *Ibid.*, p. 6
78 *Ibid.*, p. 4
79 https://ec.europa.eu/info/horizon-europe_en
80 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0795&from=EN, p. 4.
81 *Ibid.*, p. 9
82 *Ibid.*
83 http://www.justice.gouv.fr/art_pix/DP_CIPDR_23022018.pdf
84 https://www.cipdr.gouv.fr/pnpr/
85 http://www.justice.gouv.fr/art_pix/DP_CIPDR_23022018.pdf, p. 5

de l'ANR semble, quant à elle, moins destinée à étayer la prise de décisions politiques.

Le CIPDR a publié, en 2016, le deuxième Plan d'action contre la radicalisation et le terrorisme (PART), une politique actualisée de prévention de la radicalisation qui articule logiques sociale et de sécurité[86]. Le PART et son prédécesseur, le Plan de lutte antiterroriste (PLAT) de 2014, ont développé une politique de prévention autour de la détection, la formation et la prise en charge en milieux ouvert et fermé et le développement de la recherche[87]. Plus précisément, le PART s'articule autour de sept axes liés à la radicalisation, répartis en 80 mesures[88]. L'un des objectifs généraux poursuivis, associé à dix mesures, consistait à développer la recherche appliquée en mettant en place un réseau de recherche pour coordonner et partager les conclusions, en attribuant des bourses aux doctorants[89] et en finançant des initiatives privées diffusant un discours critique des idéologies de la radicalisation ou un discours ouvert des connaissances sur l'Islam[90].

Plus récemment, en 2018, le CIPDR a publié le Plan national de prévention de la radicalisation, qui a vocation à remplacer le PLAT et le PART[91]. Ce nouveau plan comprend une mesure spécifique consacrée à la recherche, sur 60 au total, qui s'attache à financer des doctorats[92] et à appuyer les candidatures françaises au système de financement Horizon 2020 de la Commission européenne (voir la section « Commission européenne » ci-dessus pour plus de détails sur le financement de la recherche en matière de lutte contre le terrorisme). Les résultats de ces financements du CIPDR en matière de recherche ne sont pas mentionnés explicitement, mais sont étroitement liés à la stratégie nationale et semblent donc poursuivre des objectifs à la fois axés sur la politique et orientés vers l'obtention de résultats.

L'ANR, de son côté, est placée sous la tutelle du ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation et finance, plus généralement, des recherches sur projets pour les opérateurs publics en coopération entre eux ou avec des entreprises[93]. L'ANR poursuit donc des objectifs davantage liés à la recherche pure qu'à un sujet précis et vise plutôt, par exemple, à financer des recherches pluridisciplinaires qu'à encourager les recherches dans un domaine particulier comme la lutte contre le terrorisme. Une recherche effectuée en avril 2021 sur les mots-clés « violent extremism » (extrémisme violent) et « counter-terrorism » (lutte contre le terrorisme) montre que l'ANR avait financé dix projets de recherche consacrés au premier entre 2011 et 2020[94], et trois projets liés au deuxième entre 2018 et 2020[95]. Ces recherches ont été indirectement financées par le gouvernement français au travers de l'ANR, mais ne semblent pas être explicitement destinées à étayer la prise de décisions politiques ou liées à la stratégie nationale de lutte contre le terrorisme.

86 *Ibid.*
87 *Ibid.*
88 https://www.cipdr.gouv.fr/announcement/second-plan-daction-contre-la-radicalisation-et-le-terrorisme-part/
89 https://www.gouvernement.fr/sites/default/files/document/document/2016/05/09.05.2016_dossier_de_presse_-_plan_daction_contre_la_radicalisation_et_le_terrorisme.pdf, p. 8
90 *Ibid.*, p. 9
91 http://www.justice.gouv.fr/art_pix/DP_CIPDR_23022018.pdf
92 *Ibid.*, p. 15
93 https://anr.fr/fr/lanr-et-la-recherche/missions/
94 https://anr.fr/en/funded-projects-and-impact/funded-projects/?q=violent+extremism&id=1781&L=1
95 https://anr.fr/en/search/?q=counter-terrorism&id=1817&L=1

Ghana

Peu d'attentats terroristes ont été perpétrés sur le territoire de la République du Ghana, qui n'a par conséquent pas mis en œuvre de stratégie nationale ou régionale de lutte contre le terrorisme[96]. L'État ghanéen a toutefois adopté une approche claire en matière de maintien de l'ordre et de renseignement. La loi de lutte antiterroriste, adoptée en 2008 pour se conformer aux obligations juridiques internationales faisant suite au 11 Septembre, est une « loi qui vise à combattre, supprimer et prévenir l'utilisation par les terroristes du territoire ghanéen comme plaque tournante »[97]. Cette loi punit les actes de terrorisme et, conformément à la Résolution 1373 du Conseil de sécurité des Nations Unies, crée de nouvelles infractions : le financement du terrorisme et les supports à caractère terroriste, la possession de biens associés au terrorisme, l'incitation au terrorisme et la promotion du terrorisme[98].

La loi confère des pouvoirs élargis de surveillance et de recherche des terroristes présumés à la police et au système judiciaire. Elle dispose, dans son article 24, que la police peut mener des fouilles corporelles et « entrer de force et par effraction » dans certains lieux si elle a des « motifs raisonnables » de soupçonner qu'ils renferment des biens utilisés à des fins terroristes[99]. De manière décisive, la police peut aussi effectuer ces fouilles sans mandat et sans arrestation préalable du suspect[100]. La loi octroie, par ailleurs, des pouvoirs de surveillance élargis à l'État, qui lui permettent d'intercepter des communications dans les cas où il existe des « raisons plausibles de soupçonner » que des actes de terrorisme sont en train d'être perpétrés. Elle a ouvert la voie à deux nouvelles évolutions de la stratégie ghanéenne en matière de lutte antiterroriste : premièrement, un amendement de 2012 à la loi prévoit (conformément aux bonnes pratiques internationales) des sanctions financières et le gel des avoirs des groupes désignés comme terroristes[101], et un contrôle de l'immigration entremêlé à la stratégie de lutte contre le terrorisme[102].

Deuxièmement, une législation plus stricte en matière de lutte contre le terrorisme a permis au gouvernement d'introduire un projet de loi sur l'interception des messages postaux et télécommunications début 2016, ce qui revêt son importance pour la lutte contre l'extrémisme violent en ligne. Ce projet de loi, baptisé « Spy Bill » (projet de loi autorisant la surveillance de masse), visait à autoriser légalement « l'interception de communications postales, électroniques et virtuelles aux fins de protection de la sécurité nationale dans le cadre de la lutte contre le crime organisé, y compris le terrorisme ». Ce projet de loi se démarquait par l'absence de redevabilité ou de contrôle, notamment parce que son article 4(3) autorisait le gouvernement à retarder de 48 heures toute ordonnance judiciaire ou mandat autorisant la surveillance. Couplée à l'absence de mécanisme

96 https://issafrica.org/iss-today/slow-progress-for-west-africas-latest-counter-terrorism-plan
97 https://heinonline.org/HOL/Page?handle=hein.journals/afjincol28&div=7&g_sent=1&casa_token=9lH5SXVmi30AAAAA:GB8E5gSXIg-UxFeFoW0D5MHaJkhBN0__swDI07Ot-ocLfkb60cbqF4qSyMCn3XTzQKg4-177Fw&collection=journals, p. 56
98 *Ibid.*, p. 57
99 https://acts.ghanajustice.com/actsofparliament/anti-terrorism-act-2008-act-762/, article 24
100 https://heinonline.org/HOL/Page?handle=hein.journals/afjincol28&div=7&g_sent=1&casa_token=9lH5SXVmi30AAAAA:GB8E5gSXIg-UxFeFoW0D5MHaJkhBN0__swDI07Ot-ocLfkb60cbqF4qSyMCn3XTzQKg4-177Fw&collection=journals, p. 58–9
101 https://www.mint.gov.gh/wp-content/uploads/2017/06/Anti-Terrorism-Reg-L.-I.-2181.pdf, articles 5 et 6
102 *Ibid.*, article 4

de supervision, cette disposition ouvrait la voie à d'éventuels abus et surveillances secrètes[103]. Le projet de loi a été retiré sous la pression de la société civile[104].

L'environnement antiterroriste répressif et propice aux abus du Ghana est la manifestation d'une tendance généralisée des États post-coloniaux ayant hérité des techniques policières paramilitaires des anciennes puissances coloniales – en l'espèce, les autorités coloniales britanniques[105]. Malgré une économie manufacturière et d'exportation riche en ressources et en pleine croissance, la dépendance économique néocoloniale permanente vis-à-vis des institutions occidentales (telles que le Fonds monétaire international) signifie que la corruption est généralisée et que les taux de pauvreté demeurent élevés[106].

Dans ce contexte, il n'est pas vraiment surprenant que la stratégie ghanéenne actuelle en matière de LEV ne comprenne pas d'éléments « intangibles » comme la recherche financée par des fonds publics. La recherche et les initiatives en matière de LEV sont, en règle générale, financées par des acteurs non étatiques, tels que des groupes régionaux, groupes de la société civile et gouvernements étrangers. Par exemple, un atelier de haut niveau traitant des causes profondes de l'extrémisme violent, organisé en 2016, a été financé par le Centre international Kofi Annan de formation au maintien de la paix, le Centre africain d'études et de recherche sur le terrorisme et le gouvernement espagnol[107]. De même, des activités de partage de connaissances en matière de lutte contre le terrorisme organisées en 2019 et 2020 ont été financées par la Direction exécutive du Comité contre le terrorisme des Nations Unies[108] et l'Office des Nations Unies contre la drogue et le crime, en collaboration avec le gouvernement allemand[109].

Japon

À l'instar du Ghana, l'approche nationale du Japon en matière de LEV est fondée sur la répression et le maintien de l'ordre. Le fait que les activités de renseignement menées sur le territoire national soient coordonnées en grande partie par les organismes chargés de l'application des lois – chargés à l'époque de lutter contre la menace communiste ostentatoire – est une caractéristique héritée de l'époque de la Guerre froide. La police préfectorale (supervisée par l'Agence de police nationale – APN) et l'Agence d'investigation de sécurité publique (l'agence japonaise de renseignement) dirigent la collecte de renseignements et les activités antiterroristes sur le territoire[110].

---

103 https://heinonline.org/HOL/Page?handle=hein.journals/afjincol28&div=7&g_sent=1&casa_token=9lH5SXVmi30AAAAA:GB8E5gSXIg-UxFeFoW0D5MHaJkhBN0__swDl07Ot-ocLfkb60cbqF4qSyMCn3XTzQKg4-177Fw&collection=journals, p. 60–61
104 https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Spy-Bill-withdrawn-from-Parliament-451805
105 https://journals.sagepub.com/doi/pdf/10.1177/1461355716638114
106 Voir Walter Rodney (2018) *How Europe Underdeveloped Africa* (Londres : Verso Books) ; https://www.imf.org/en/News/Articles/2015/09/14/01/49/pr15159 ; https://www.tandfonline.com/doi/abs/10.1080/01900692.2011.598272 ; https://www.unicef.org/ghana/media/531/file/The%20Ghana%20Poverty%20and%20Inequality%20Report.pdf
107 https://caert.org.dz/Reports/Final%20Report%20for%20CVE%20Workshop_7-8Nov2016.pdf
108 https://www.un.org/sc/ctc/news/2019/10/04/cted-conducts-follow-visit-republic-ghana/
109 https://www.unodc.org/westandcentralafrica/fr/2020-09-28-ghana-counter-terrorism.html
110 Ken Kotani (2013), « A Reconstruction of Japanese Intelligence: Issues and Prospects », in : Philip H. J. Davies et Kristian C. Gustafson (dir.), *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere* (Washington D.C. : Georgetown University Press), p. 181–99.

Les systèmes traditionnels de répression et de sécurité sont donc mobilisés pour répondre aux activités terroristes intérieures menées en ligne[111]. Les innovations technologiques constituent un signe distinctif de la recherche scientifique et du commerce d'exportation du Japon, et ceci se reflète également dans sa stratégie sécuritaire. Les pouvoirs publics japonais ont beaucoup investi dans la création de solutions d'intelligence artificielle, notamment des systèmes de reconnaissance faciale, d'authentification biométrique et de détection comportementale de grande échelle[112]. Ces solutions suggèrent un modèle de gouvernance axé sur la détection précoce et la prévention, appliqué à l'aide de tactiques répressives et sécuritaires traditionnelles.

En 2015, en réaction à une prise d'otages dans laquelle deux citoyens japonais ont été assassinés par l'État islamique en Syrie, le Japon a mis sur pied une unité de lutte antiterroriste, dont le personnel est issu de ses ministères des Affaires étrangères et de la Défense, de l'APN et du Bureau du Conseil des ministres chargé du renseignement et de la recherche[113]. Cette unité semble indiquer un renforcement progressif des capacités nationales en matière de renseignement et de sécurité. En effet, l'ancien Premier ministre Shinzo Abe a fait passer de force un projet de loi antiterroriste « brutal »[114] au Parlement à la fin du premier semestre 2017[115]. Ce projet de loi érige en infraction les préparatifs pour commettre 270 « infractions graves », y compris les sit-ins de protestation et la violation des droits d'auteur d'œuvres musicales, et son application s'étend aux médias sociaux[116]. Les défenseurs des droits de l'homme ont exprimé leurs inquiétudes vis-à-vis de cette loi, compte tenu de sa portée et des vastes pouvoirs de surveillance et de contrôle des activités en ligne qu'elle confère aux forces de l'ordre japonaises[117].

En ce qui concerne les activités de lutte contre le terrorisme international, l'approche adoptée par le Japon se distingue considérablement de sa stratégie de criminalisation mise en œuvre à l'échelle nationale. Ses efforts sont régionaux, coopératifs et fondés sur le renforcement des capacités. L'Association des nations de l'Asie du Sud-Est (ANASE), le forum par lequel passe une grande partie des efforts menés par le Japon pour lutter contre le terrorisme à l'étranger[118], a publié plusieurs déclarations. Celles-ci engagent les signataires à « prévenir, empêcher et combattre le

111 https://www.mofa.go.jp/files/000156881.pdf, section consacrée aux « Mesures nationales de lutte contre le terrorisme » (« Domestic Counter-Terrorism Measures »)

112 Gouvernement du Japon, « All is Ready for a Safe and Secure Tokyo Games », https://www.japan.go.jp/tomodachi/2019/autumn-winter2019/tokyo2020.html ; NEC Corporation (2015), « NEC Becomes a Gold Partner for the Tokyo 2020 Olympic and Paralympic Games ». https://www.nec.com/en/press/201502/global_20150219_01.html ; Kyodo News (29 janvier 2018), « Kanagawa police eye AI-assisted predictive policing before Olympics », https://english.kyodonews.net/news/2018/01/5890d824baaf-kanagawa-police-eye-ai-assisted-predictive-policing-before-olympics.html.

113 https://www.voanews.com/east-asia/japan-launches-anti-terrorism-unit-ahead-summit-olympics

114 B. Allen-Ebrahimian (16 juin 2017) « Japan Just Passed a 'Brutal,' 'Defective' Anti-Terror Law », *Foreign Affairs*, https://foreignpolicy.com/2017/06/16/japan-just-passed-a-brutal-defective-anti-terror-law/

115 Le projet de loi a été adopté « de façon inhabituelle, sans être soumis au vote de la Commission des affaires judiciaires de la Chambre haute ». Fédération des barreaux du Japon (15 juin 2017), « Statement on the Enactment of the Bill to Revise the Act on Punishment of Organized Crimes and Control of Crime Proceeds, including the Criminalization of Conspiracy », https://www.nichibenren.or.jp/en/document/statements/170615.html.

116 J. McCurry (15 juin 2017) « Japan passes 'brutal' counter-terror law despite fears over civil liberties », *The Guardian*, https://www.theguardian.com/world/2017/jun/15/japan-passes-brutal-new-terror-law-which-opponents-fear-will-quash-freedoms ; J. Adelstein (15 juin 2017) « Japan's Terrible Anti-Terror Law Just Made 'The Minority Report' Reality », *The Daily Beast*, http://www.thedailybeast.com/japans-terrible-anti-terror-law-just-made-the-minority-report-reality

117 Fédération des barreaux du Japon, « Statement on the Enactment of the Bill »

118 « Japan: Extremism & Counter Extremism », Counter-Extremism Project, https://www.counterextremism.com/countries/japan.

terrorisme international grâce à l'échange d'informations, le partage de renseignements et le renforcement des capacités », établissant ainsi un précédent en matière de coopération régionale pour la LEV et le terrorisme[119]. Le Japon a accueilli le Dialogue ANASE-Japon sur la lutte contre le terrorisme à deux reprises, et dirigé des discussions bilatérales avec différents acteurs mondiaux[120]. Par exemple, fin 2019, le Japon et le Royaume-Uni ont échangé sur « la situation actuelle en matière de terrorisme international, les mesures à prendre à l'échelle nationale pour lutter contre le terrorisme, ainsi que la coopération actuelle en vue du renforcement des capacités de lutte antiterroriste, en particulier dans les pays tiers [*sic*] »[121].

Dans ce contexte, rien ne prouve que le gouvernement japonais finance des recherches en matière de LEV aux côtés de la société civile ou de partenaires universitaires sur les activités extrémistes violentes intérieures commises en ligne. En accord avec la distinction entre ses approches nationale et internationale, toutefois, le Japon a financé des recherches et des ateliers en conjonction avec les Nations Unies. Il a par exemple publié, en association avec l'Office des Nations Unies contre la drogue et le crime, des directives internationales visant à prévenir le recrutement et l'exploitation d'enfants par les groupes extrémistes violents[122], et a créé un partenariat avec ONU Femmes pour comprendre les dynamiques sexospécifiques de l'extrémisme violent[123]. Ces activités rehaussent l'image internationale du Japon comme étant un pays coopératif et progressiste en matière de gouvernance relative à la LEV. Mais il devrait, pour protéger efficacement les libertés et la vie privée de ses citoyens, commander des recherches et façonner des politiques en gardant à l'esprit ces préoccupations.

Nouvelle-Zélande

La réponse globale de la Nouvelle-Zélande à la lutte contre le terrorisme implique une coordination entre différents ministères du gouvernement, les communautés et des organisations du secteur privé. La gouvernance de haut niveau est assurée par le Comité du Cabinet chargé des relations extérieures et de la sécurité et par le Conseil de la sécurité et du renseignement. La stratégie globale de la Nouvelle-Zélande est présentée dans son Plan stratégique de lutte contre le terrorisme publié en février 2020[124]. L'attentat de Christchurch en mars 2019 a conduit la Nouvelle-Zélande à adopter différentes réponses en matière de lutte antiterroriste, telles que l'Appel de Christchurch, à vocation internationale, et le rapport de la Commission royale, à vocation nationale, qui aborde régulièrement la question de la recherche.

119 « ASEAN-Japan Joint Declaration for Cooperation to Combat International Terrorism », ANASE. https://asean.org/?static_post=asean-japan-joint-declaration-for-cooperation-to-combat-international-terrorism-2.
120 « Japan: Extremism & Counter Extremism »
121 Ministère des Affaires étrangères du Japon (4 décembre 2019), « The 4th Japan-the UK Counter-Terrorism Dialogue », https://www.mofa.go.jp/fp/is_sc/page1e_000297.html.
122 https://www.unodc.org/unodc/en/frontpage/2019/March/unodc--japan-gather-countries-from-asia--the-middle-east-and-north-africa-to-protect-children-affected-by-terrorism-and-violent-extremism.html
123 https://thediplomat.com/2018/03/japan-helps-explore-the-gender-dynamics-of-violent-extremism/
124 Gouvernement de la Nouvelle-Zélande, Comité des fonctionnaires chargés de coordonner la sécurité intérieure et extérieure, Comité de coordination de la lutte contre le terrorisme (février 2020) « Countering terrorism and violent extremism national strategy overview », https://dpmc.govt.nz/sites/default/files/2020-02/2019-20%20CT%20Strategy-all-final.pdf CT Strategy-all-final.pdf

Le sommet de l'Appel de Christchurch, organisé par la communauté internationale suite à l'attaque terroriste commise en mars 2019 contre deux mosquées, a réuni des dirigeants mondiaux et des représentants de sociétés Internet à Paris pour lutter contre l'usage d'Internet par les terroristes[125]. Cet événement, coprésidé par la Première ministre de Nouvelle-Zélande, Jacinda Ardern, et par le Président français, Emmanuel Macron[126], a défini une stratégie en quatre phases pour lutter contre les contenus à caractère extrémiste, l'une consistant à « comprendre, recenser et analyser la recherche (existante ou, à défaut, identifier les lacunes dans ce domaine) relative à l'extrémisme violent en ligne »[127], compte tenu du manque de recherche et de l'absence de progrès en matière de cartographie et de compréhension de ce phénomène[128]. En signant l'Appel à l'action de Christchurch, les États ont accepté d'accélérer la recherche et le développement d'outils visant à prévenir, détecter et supprimer la mise en ligne de contenus à caractère terroriste et extrémiste, en s'appuyant sur l'expertise d'universitaires, de chercheurs et chercheuses et de la société civile[129]. En soi, l'Appel de Christchurch pourrait être considéré comme un élargissement de la portée de la démarche axée sur la communauté et la société civile de la Nouvelle-Zélande, par comparaison aux modèles plus traditionnels adoptés par d'autres pays signataires comme le Royaume-Uni ou la France.

En ce qui concerne le financement de la lutte contre le terrorisme spécifiquement axé sur la Nouvelle-Zélande, la Commission royale d'enquête, dans son rapport publié le 8 décembre 2020[130] sur l'attentat terroriste perpétré contre deux mosquées de Christchurch le 15 mars 2019[131], a émis 44 recommandations à l'intention du gouvernement. La recommandation n° 16 du rapport traite du financement de la recherche indépendante sur les causes du terrorisme et de l'extrémisme violent et sur les mesures de prévention y afférentes[132]. La recherche décrite semble être destinée à étayer la prise de décisions politiques ; en effet, selon les dispositions relatives au financement, l'agence nationale de sécurité et de renseignement (proposée) devrait bénéficier d'un crédit pluriannuel pour le financement de la recherche, et former un panel de représentants chargés de sélectionner les priorités de recherche et les bénéficiaires de subventions[133]. Le rapport a également recommandé la création d'un réseau de partage d'informations sur la LEV et le terrorisme, formé par les services du gouvernement central et des autorités locales, les communautés, la société civile, le secteur privé et la recherche[134]. Le gouvernement a officiellement accepté toutes les recommandations du rapport. Leur mise en œuvre semble toutefois être à la traîne ; dans un discours du 8 décembre 2020, Jacinda Ardern s'est excusée au nom du gouvernement pour ses manquements en matière de mise en

125 https://www.gov.uk/government/news/pm-joins-christchurch-call-to-action-on-online-terror
126 *Ibid.*
127 https://www.orfonline.org/research/one-year-since-the-christchurch-call-to-action-a-review/
128 https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/actualites-et-evenements/article/appel-de-christchurch-pour-supprimer-les-contenus-terroristes-et-extremistes
129 *Ibid.*
130 https://christchurchattack.royalcommission.nz/the-report/download-report/download-the-report/
131 https://christchurchattack.royalcommission.nz/assets/Report-Volumes-and-Parts/Ko-to-tatou-kainga-tenei-Volume-1-v2.pdf
132 https://christchurchattack.royalcommission.nz/assets/Report-Volumes-and-Parts/Ko-to-tatou-kainga-tenei-Volume-1-v2.pdf, p. 26
133 *Ibid.*
134 *Ibid.*, p. 27

œuvre[135]. La Première ministre n'a pas mentionné dans son discours les implications de la recherche financée directement, mais a déclaré que le gouvernement mettrait immédiatement en application certaines recommandations, tandis que d'autres seraient envisagées en partenariat avec le parlement et les citoyens[136]. Il est évident que la recherche financée sera destinée à étayer la prise de décisions politiques et qu'elle supposera de tisser des liens étroits avec les agences de sécurité nationale si elle est menée conformément aux recommandations de la Commission royale. Les mesures proposées dans le rapport de cette dernière semblent donc concerner à la fois les structures conventionnelles de sécurité et de renseignement et les initiatives réunissant représentants de la société civile, universitaires et responsables politiques dans la stratégie nationale de lutte contre le terrorisme.

Royaume-Uni

Au Royaume-Uni, le ministère de l'Intérieur est responsable des lois et politiques de lutte contre le terrorisme, et le Conseil de sécurité nationale (NSC), présidé par le Premier ministre, est le principal forum de discussion sur les objectifs du gouvernement en matière de sécurité nationale[137]. Le NSC détermine par ailleurs les priorités du quartier-général des communications du gouvernement (GCHQ)[138]. Le gouvernement britannique finance à la fois directement et indirectement la recherche en matière de lutte antiterroriste, au travers de ces différents organes. Il n'est pas surprenant que le financement soit (essentiellement) indirect et que les conclusions de recherche soient publiées par le biais d'agences indépendantes, compte tenu de la stratégie traditionnelle adoptée par le pays en matière de LEV. Quatre types de financement de la recherche en matière de lutte antiterroriste cohabitent au Royaume-Uni, classés ci-dessous du plus direct au moins direct.

Le Fonds de stabilité, de sécurité et de résolution des conflits (CSSF), créé en 2015 pour assurer une réponse gouvernementale plus intégrée à la fragilité et au conflit, est un fond annuel transversal de 1,26 milliard de livres sterling financé par le ministère de l'intérieur et le Bureau du Conseil des ministres[139]. Le Fonds pour les programmes de lutte antiterroriste (CTPF), créé dans le cadre du CSSF, opérait au travers notamment d'un programme intitulé « Enablers Programme ». Celui-ci avait pour objectif d'appuyer la recherche visant à améliorer les connaissances du gouvernement en matière de terrorisme et d'extrémisme violent[140]. Si la nature des recherches menées n'est pas précisée sur le site du Fonds, on peut imaginer qu'elles sont liées à la lutte contre le terrorisme, puisque ce programme est conçu pour soutenir la mise en œuvre de certains aspects des éléments de CONTEST relatifs à l'étranger[141].

135 https://www.tvnz.co.nz/one-news/new-zealand/full-statement-jacinda-ardern-apologises-agrees-all-recommendations-in-christchurch-attack-report
136 *Ibid.*
137 https://www.gov.uk/government/groups/national-security-council
138 https://www.gchq.gov.uk/section/mission/overview
139 https://www.gov.uk/government/organisations/conflict-stability-and-security-fund/about
140 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875951/CTPF_Enablers_Programme_Summary.odt
141 *Ibid.*

CONTEST, la Stratégie de lutte antiterroriste britannique, mise à jour en 2018 par le ministère de l'Intérieur[142], mentionne plusieurs fois la recherche, en lien notamment avec l'un de ses axes de travail stratégiques éprouvés, « Prevent »[143]. Prevent est étayée par « un processus continu de recherche et d'évaluation »[144]. Encore une fois, celui-ci n'est pas décrit en détail mais passe, par exemple, par une collaboration avec des instituts de recherche et des universitaires pour mieux comprendre comment les terroristes utilisent Internet pour radicaliser des individus vulnérables[145]. La Stratégie précise par ailleurs que la lutte antiterroriste se fonde sur « la science, la technologie, l'analyse et la recherche »[146] et décrit le projet du ministère de l'Intérieur visant à « renforcer sa collaboration avec le monde universitaire et le secteur privé, afin d'avoir accès aux dernières technologies, à des conseils et à des solutions en matière de lutte antiterroriste et de les exploiter »[147].

Le Centre de recherche et d'étude sur les menaces pour la sécurité (CREST), le « pôle des sciences comportementales et sociales pour la sécurité nationale », est financé par le gouvernement britannique de manière moins explicite[148]. Le CREST a bénéficié de fonds publics à la fois directs et indirects, de la part des agences britanniques de renseignement et de sécurité, du ministère de l'Intérieur[149] et du Conseil de recherche économique et sociale (ESRC), qui fait partie de l'organisme public chargé d'appuyer la recherche et l'échange de connaissances dans les établissements d'enseignement supérieur en Angleterre[150]. Depuis octobre 2015, le CREST a reçu près de 12,5 millions de livres sterling[151] pour amener six universités partenaires du pays à « réaliser un portefeuille d'activités interdisciplinaires et d'envergure mondiale qui maximise la valeur des sciences sociales dans la lutte contre les menaces pour la sécurité intérieure »[152]. La subvention la plus récente prévoit également que sept étudiants en doctorat seront formés par le CREST[153]. Les projets du Centre sont diversifiés, abordant des sujets tels que « Comprendre et combattre les comportements en ligne » ou l'évaluation de l'efficacité de la LEV[154]. Les liens étroits unissant le CREST et ses partenaires universitaires, et non le gouvernement britannique, apparaissent clairement dans les rapports publiés. Le fait que le CREST bénéficie de fonds directs du ministère de l'Intérieur (et indirects du gouvernement par le biais de l'ESRC) signifie toutefois qu'on ne peut ignorer ses liens avec le gouvernement britannique et sa politique de lutte antiterroriste.

Le ministère de l'Intérieur travaille en étroite collaboration avec le Centre national de cybersécurité (NCSC), l'autorité indépendante du pays en matière de cybersécurité[155]. Le NCSC n'a pas de mission spécifique liée à la LEV, mais fait partie du GCHQ, dont les priorités

142 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf
143 *Ibid.*, p. 9
144 *Ibid.*, p. 32
145 *Ibid.*, p. 33
146 *Ibid.*, p. 8
147 *Ibid.*, p. 80
148 https://www.lancaster.ac.uk/people-profiles/paul-j-taylor
149 https://crestresearch.ac.uk/about/
150 https://www.ukri.org/about-us/who-we-are/
151 https://gtr.ukri.org/projects?ref=ES%2FN009614%2F1#/tabOverview ; https://gtr.ukri.org/projects?ref=ES%2FV002775%2F1
152 https://www.ukri.org/news/uk-hub-for-research-into-security-threats-awarded-5-3m-funding/ ; https://gtr.ukri.org/projects?ref=ES%2FN009614%2F1#/tabOverview
153 https://gtr.ukri.org/projects?ref=ES%2FV002775%2F1
154 https://crestresearch.ac.uk/projects/
155 https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

sont alignées sur celles du Conseil de sécurité nationale et de la Stratégie nationale de sécurité[156], pour lesquels la lutte antiterroriste joue un rôle central. Le NCSC finance des recherches doctorales liées aux questions de cybersécurité depuis 2012[157], au travers de 19 universités reconnues comme des Centres universitaires d'excellence en matière de recherche sur la cybersécurité[158]. Ces universités sont reconnues à la fois par le NCSC et le Conseil de recherche en ingénierie et sciences physiques, une source indirecte de financement public. Tout comme la France, Le Royaume-Uni finance les recherches doctorales dans le domaine de la lutte antiterroriste, mais de façon plus indirecte. Si ce lien peut sembler légèrement ténu, il s'agit d'une source de financement bien établie pour les futur·e·s chercheurs et chercheuses, qui peut également servir de voie d'accès direct à un emploi au sein du NCSC ou du GCHQ[159], alimentant la politique britannique de lutte contre le terrorisme.

Direction exécutive du Comité contre le terrorisme des Nations Unies

La Direction exécutive du Comité contre le terrorisme des Nations Unies (UN CTED) a été créée par la Résolution 1535 (2004) du Conseil de sécurité des Nations Unies comme organe spécialisé ayant pour mandat de soutenir le Comité contre le terrorisme du Conseil de sécurité (CTC)[160]. Elle avait pour but initial d'évaluer la mise en œuvre par les États membres des Nations Unies des résolutions du Conseil de sécurité en matière de lutte contre le terrorisme et d'appuyer leurs efforts par le dialogue.

En 2015, l'UN CTED a créé son Réseau mondial de recherche dans le domaine de la lutte antiterroriste (GRN). Le GRN réunit plus de 100 instituts de recherche dans le monde, et a pour objectifs d'informer l'UN CTED sur les tendances émergentes en matière de terrorisme et d'identifier et partager les bonnes pratiques en matière de mise en œuvre par les États membres des résolutions du Conseil de sécurité pertinentes[161]. La valeur du GRN a été reconnue dans une résolution (2395) de l'ONU de 2017, tout comme l'ont été les rapports de l'UN CTED avec les spécialistes compétents de différentes universités et groupes de réflexion[162]. Bien que l'on ne sache pas exactement si la recherche partagée par le GRN est financée par l'UN CTED ou un autre organe de l'ONU, cet organisme publie régulièrement des rapports en ligne et des analyses longues, par exemple sur l'impact de la pandémie de coronavirus sur le terrorisme, la lutte antiterroriste et la LEV[163], ainsi que des avis de tendance. Ces avis sont publiés pour « améliorer la prise de conscience, de la part du CTC comme des agences des Nations Unies et responsables

156 https://www.gchq.gov.uk/section/mission/overview
157 https://www.ncsc.gov.uk/information/academic-centres-excellence-phd-student-scheme
158 https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research
159 https://www.ncsc.gov.uk/information/academic-centres-excellence-phd-student-scheme
160 N. Chowdhury Fink (2012) « Meeting the challenge: A guide to United Nations counterterrorism activities », Institut international de la paix : p .45, https://www.ipinst.org/wp-content/uploads/publications/ebook_guide_to_un_counterterrorism.pdf
161 https://spark.adobe.com/page/hMGmYTiTbbEag/
162 https://www.un.org/sc/ctc/news/2021/01/05/virtual-roundtable-global-research-network-20-years-research-emerging-threats-trends-developments-terrorism-counter-terrorism/
163 https://www.un.org/sc/ctc/wp-content/uploads/2020/06/CTED-Paper%E2%80%93-The-impact-of-the-COVID-19-pandemic-on-counter-terrorism-and-countering-violent-extremism.pdf

politiques »[164], et contiennent les recherches menées par le GRN[165]. Tout comme la recherche financée par la Commission européenne, celle du GRN poursuit des objectifs axés sur la politique et orientés vers l'obtention de résultats.

Le Programme des Nations Unies pour le développement, bien que non directement relié à l'UN CTED, a également publié en 2016 un plan d'action pour lutter contre la radicalisation et l'extrémisme violent axé sur deux programmes, dont l'un relatif à « la recherche, [à] la politique et [au] plaidoyer »[166]. Ce programme de recherche « sera piloté par le Centre d'Oslo pour la gouvernance [des Nations Unies] et mené en collaboration avec les pôles régionaux et en partenariat avec des instituts universitaires et de recherche »[167]. Le programme aborde également le rôle du réseau de recherche RESOLVE, distinct du GRN, qui vise à fournir « aux programmes et politiques de lutte contre l'extrémisme violent une base de données probantes »[168], et organise une conférence annuelle à l'occasion de laquelle les recherches internationales en matière de LEV sont présentées. Si aucune mention n'est faite des sources de financement associées, les conclusions de recherche devraient, encore une fois, être axées sur les politiques, comme le suggère le nom du programme.

États-Unis

Les activités et le budget national alloué à la LEV ont été réduits sous l'administration Trump. Le groupe de travail chargé de la lutte contre l'extrémisme violent, créé en 2011, sous l'administration Obama, pour unifier les efforts et activités des différentes agences, a été restructuré en 2017[169], puis démantelé fin 2018[170]. Le financement des activités impliquant les communautés et la société civile, telles que Life After Hate, une initiative aidant les individus souhaitant quitter les groupes suprémacistes blancs et néonazis[171], a été suspendu.

Malgré ces coupes budgétaires, le niveau de financement en matière de LEV destiné aux autorités chargées de l'application de la loi – en particulier le ministère de l'Intérieur (DHS) – a triplé, passant de 764 000 dollars US à 2 340 000 dollars US[172]. La Direction des sciences et technologies du DHS a commandé plusieurs feuilles de route en matière de recherche pour faire l'état des lieux de la recherche en cours en matière de LEV et des parties prenantes concernées, et formuler des recommandations concernant de futurs axes de recherche[173]. La recherche du gouvernement fédéral en matière de LEV porte principalement sur « les questions sociales,

164 https://www.un.org/sc/ctc/wp-content/uploads/2020/04/CTED_Trends_Alert_Extreme_Right-Wing_Terrorism.pdf, p. 2
165 *Ibid.*
166 https://www.undp.org/content/dam/norway/undp-ogc/documents/Discussion%20Paper%20-%20Preventing%20Violent%20Extremism%20by%20Promoting%20Inclusive%20%20Development.pdf, p. 33
167 *Ibid.*
168 *Ibid.*, p. 34
169 J. Ainsley *et al.* (3 février 2017), « Exclusive: Trump to focus counter-extremism program solely on Islam – sources ». *Reuters*, https://www.reuters.com/article/idUSKBN15G5VO?feedType=RSS&feedName=topNews&utm_source=twitter&utm_medium=Social.
170 P. Beinart (29 octobre 2018), « Trump Shut Programs to Counter Violent Extremism », *The Atlantic*, https://www.theatlantic.com/ideas/archive/2018/10/trump-shut-countering-violent-extremism-program/574237/.
171 Life After Hate, « About Us ». https://www.lifeafterhate.org/about-us-page.
172 https://www.brennancenter.org/our-work/analysis-opinion/countering-violent-extremism-programs-trump-era
173 Voir : https://www.dhs.gov/science-and-technology/developing-local-capabilities et plus particulièrement https://www.dhs.gov/sites/default/files/publications/861_OPSR_TP_CVE-Developing-Research-Roadmap_Oct2017.pdf

psychologiques, économiques, juridiques, politiques et culturelles émergentes », ainsi que sur les « facteurs de risque conduisant à l'extrémisme violent, de façon à aider les partenaires à créer des programmes de LEV plus efficaces et efficients »[174].

Si certains observateurs avancent que la politique de LEV de l'administration Trump « aurait pu être bien pire », mentionnant l'élargissement des financements de la recherche par le DHS comme une évolution positive[175], il est évident que ces programmes de recherche ont ciblé des communautés spécifiques et intensifié les mesures de répression et de surveillance en leur sein. Le Brennan Center for Justice, un institut de droit et de politiques publiques, a analysé les subventions octroyées par l'administration Trump dans le domaine de la LEV. Il conclut que « au moins 85 % des subventions et plus de la moitié des programmes actuels de LEV ciblent explicitement des groupes minoritaires, tels que les musulmans, la communauté LGBTQ, les militants Black Lives Matter, les migrants et les réfugiés »[176]. Plus de la moitié des programmes ciblent les établissements scolaires et les écoliers, dès l'âge de cinq ans[177]. Bon nombre de subventions en matière de LEV ont été remises aux forces de l'ordre opérant dans des zones à forte concentration ethnique, tels que « Minneapolis et ses enclaves somaliennes ; le bureau du shérif du comté d'Alameda, dont la compétence s'étend à Oakland, en Californie »[178].

L'utilisation de fonds fédéraux pour ce type d'activités est insidieuse. Sous couvert de recherche et de sensibilisation communautaire, les forces de l'ordre peuvent en effet « recueillir des renseignements dans le but de repérer les cibles potentielles d'opérations d'infiltration ou d'identifier de potentiels informateurs à recruter »[179], ce qui ne va pas sans rappeler Prevent, le programme controversé mis en œuvre au Royaume-Uni qui a impulsé la surveillance des communautés musulmanes britanniques[180]. Ces activités ont contribué au profilage racial de certaines communautés, créant ainsi un climat de peur et de répression de la liberté d'expression et du droit à la vie privée.

La nouvelle administration Biden n'a pas encore dévoilé sa stratégie en matière de LEV. Il ne serait pas étonnant que sa stratégie de lutte contre le terrorisme soit caractérisée par la même approche militariste à l'étranger favorisée par Obama, dont il était le vice-président[181]. Si Biden tient à revenir sur les politiques racistes mises en place par Trump, il pourrait commencer par abandonner le programme de subventions relatives à la LEV. Les fonds préalablement utilisés pour mener des recherches néfastes dans le domaine de la LEV pourraient être détournés vers les communautés négligées et sous-financées de manière chronique pour répondre à leurs besoins fondamentaux.

174 https://www.dhs.gov/sites/default/files/publications/861_OPSR_TP_CVE-Developing-Research-Roadmap_Oct2017.pdf, p. 11
175 https://www.brookings.edu/blog/order-from-chaos/2020/04/07/on-cve-the-trump-administration-could-have-been-worse/
176 https://www.brennancenter.org/our-work/analysis-opinion/countering-violent-extremism-programs-trump-era
177 https://www.brennancenter.org/our-work/research-reports/countering-violent-extremism-trump-era
178 https://theintercept.com/2018/06/15/cve-grants-muslim-surveillance-brennan-center/
179 *Ibid.*
180 Voir le rapport précédent du GNET, « Recherche relative aux contenus à caractère extrémiste sur les médias sociaux : enjeux et opportunités de la protection des données et de l'éthique de la recherche » https://gnet-research.org/wp-content/uploads/2021/01/GNET-Researching-Extremist-Content-Social-Media-Ethics-FRENCH.pdf, p. 36–41
181 https://www.cfr.org/election2020/candidate-tracker, section « Counterterrorism »

Pertinence politique, recherche et État : questions éthiques fondamentales

Trois catégories d'intervenants prennent part à l'élaboration et à l'exécution des politiques de LEV : les chercheurs et chercheuses, les responsables politiques/praticien·ne·s et le secteur des technologies. L'enquête menée par Lydia Khalil, reproduite dans ce rapport, porte sur la collaboration entre la recherche et le secteur des technologies, et conclut à l'existence de degrés variables de collaboration avec les entreprises. Nous étudierons, dans la présente sous-section, la collaboration de la recherche avec les professionnels de la LEV et les responsables politiques, et analyserons certains des enjeux éthiques implicites qui découlent des rapports entre la recherche et le législateur.

Avant les attentats à la bombe perpétrés en juillet 2005 à Londres, la stratégie de lutte antiterroriste se concentrait sur les menaces pour la sécurité posées par le terrorisme international, et en particulier certains groupes comme Al-Qaïda. C'est à cette époque que le Royaume-Uni a commencé à s'intéresser aux menaces posées par l'extrémisme « d'origine intérieure » et le terrorisme intérieur, compte tenu du fait que trois des quatre kamikazes était nés sur le territoire britannique. La stratégie Prevent, lancée en 2003 par le ministère de l'Intérieur britannique, ciblait des individus jugés « vulnérables » à la radicalisation et intervenait dans le parcours dit de radicalisation avant que toute activité criminelle ne puisse avoir lieu[182].

Cette stratégie était particulièrement remarquable pour son approche « pansociétale » : les institutions civiques telles que les écoles, les garderies agréées, l'enseignement supérieur, les prisons, les services de probation, les services de santé, les services sociaux et les services d'immigration étaient tous impliqués dans la stratégie. Ces institutions étaient tenues d'anticiper, de surveiller et d'intervenir dans les possibles cas de radicalisation en identifiant certains marqueurs évocateurs de la radicalisation, et de les signaler. Cette démarche a entraîné un transfert de la stratégie de répression et de lutte contre le terrorisme des dispositifs traditionnels de sécurité et de renseignement vers les espaces communautaires et différents organismes publics. L'approche adoptée dans le cadre de la stratégie Prevent sous l'égide du Royaume-Uni a depuis été mise en œuvre dans de nombreux pays occidentaux[183].

Cette approche pansociétale et pluri-institutionnelle de la lutte antiterroriste a fini par être décrite par le terme LEV. La LEV se traduit par différentes activités « sur le terrain » destinées à intervenir dans le parcours de radicalisation, étayées et sous-tendues par une conception idéologique, psychologique ou culturelle de la radicalisation[184]. Les projets d'engagement communautaire, tels que les programmes éducatifs ou de mentorat – souvent destinés aux jeunes ou à certaines communautés – et les programmes conçus pour renforcer la confiance envers la police et l'engagement avec celle-ci sont caractéristiques des stratégies de LEV[185].

182 Gouvernement britannique, « Prevent Strategy », juin 2011, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf
183 https://www.tandfonline.com/doi/pdf/10.1080/09546553.2020.1727450?needAccess=true, note 18
184 https://www.tandfonline.com/doi/pdf/10.1080/09546553.2020.1727450?needAccess=true, p. 3
185 *Ibid.*, p. 5 et https://www.tandfonline.com/doi/full/10.1080/18335330.2015.1028772?casa_token=4VBOXUOQT3UAAAAA%3ABeegdWY62rzDh376WJQuY3Ssw6Z99i4QiU6NZkRWzkypPQ4OQ5Q9PkBzslOXsdnrAVFp07xAQE4

Les activités du Bureau pour la prévention de la violence ciblée et du terrorisme du ministère de l'Intérieur américain (TVTP, anciennement Groupe de travail chargé de la lutte contre l'extrémisme violent) résument bien les principes de la stratégie de LEV. Elles sont en effet axées sur des « mesures proactives » visant à prévenir le terrorisme et les actes de violence ciblée et destinées aux communautés[186]. Ces mesures viseraient à « autonomiser les communautés et les individus » et à développer leur résilience face aux « messages violents et au recrutement ». Elles se traduisent notamment par la mise en place de services de sensibilisation du public, d'engagement communautaire et de soutien[187].

De manière décisive, la stratégie de LEV et les cadres de prévention s'articulent autour d'un paradigme d'évaluation et de gestion de la menace. Selon le TVTP, cela suppose d'assurer la participation « d'enseignants, de psychologues, de chefs spirituels, de membres du personnel médical et des forces de l'ordre, entre autres » à la lutte antiterroriste, dans le cadre d'une approche pansociétale[188]. Cette approche a été très critiquée par les groupes de défense des droits humains, préoccupés par la façon dont cette forme de surveillance et de répression communautaires enracine des hypothèses préjudiciables, selon lesquelles les communautés et groupes raciaux sont « vulnérables » à la radicalisation et à la violence, tout en créant un climat de peur et d'hostilité au sein des communautés[189]. En accordant la priorité à l'évaluation et à la gestion de la menace, la stratégie de LEV dépend du soutien de dispositifs répressifs et de sécurité « forts » pour criminaliser certains comportements.

Nous avons examiné, dans le paysage politique élaboré plus haut, le rôle des financements fédéraux aux États-Unis, destinés à mettre en œuvre cette approche pansociétale avec l'aide des forces de l'ordre, des responsables politiques et des universitaires. Nous avons vu que « au moins 85 % des subventions et plus de la moitié des programmes actuels de LEV ciblent explicitement des groupes minoritaires, tels que les musulmans, la communauté LGBTQ, les militants Black Lives Matter, les migrants et les réfugiés »[190]. Plus de la moitié des programmes ciblent les établissements scolaires et les écoliers, dès l'âge de cinq ans[191]. Bon nombre de subventions en matière de LEV ont été remises aux forces de l'ordre opérant dans des zones à forte concentration ethnique, tels que « Minneapolis et ses enclaves somaliennes ; le bureau du shérif du comté d'Alameda, dont la compétence s'étend à Oakland, en Californie »[192].

Une subvention relative à la LET, octroyée aux services de police de la ville de Seattle est un exemple particulièrement frappant de collaboration entre les forces de l'ordre, les agences fédérales et les universitaires. Cette subvention, d'un montant de 409 389 dollars US, a servi à financer les heures supplémentaires consacrées par des policiers à l'élaboration et à l'exécution de « plans de police de proximité » qui articulent « engagement communautaire, données sur la criminalité et services de police ». Ces plans ciblent les « communautés afro-américaines, est-africaines, philippines, coréennes, latinas,

186 Voir : https://www.dhs.gov/tvtp
187 *Ibid.*
188 https://www.dhs.gov/tvtp, section « Local Prevention Frameworks »
189 Voir, par exemple : Liberty : https://www.libertyhumanrights.org.uk/fundamental/prevent/
190 https://www.brennancenter.org/our-work/analysis-opinion/countering-violent-extremism-programs-trump-era
191 https://www.brennancenter.org/our-work/research-reports/countering-violent-extremism-trump-era
192 https://theintercept.com/2018/06/15/cve-grants-muslim-surveillance-brennan-center/

musulmanes/arabes sikhs, amérindiennes et du Sud-Est asiatique » de Seattle, en particulier les femmes réfugiées et leurs familles, les enfants de 5 à 18 ans et les « populations en difficulté »[193]. Cette subvention assure la collaboration des forces de l'ordre de Seattle avec un centre de réhabilitation, des établissements scolaires, la ville et des organisations spirituelles et communautaires, ainsi que des chercheurs et chercheuses de l'Université de Seattle. Les chercheurs et chercheuses « évalueront le programme par le biais d'enquêtes communautaires mesurant 'la manière dont la police est perçue' » et d'autres facteurs.

Cet exemple de partenariat entre la recherche et un programme répressif ciblant directement certains groupes particuliers montre le côté dangereux de la collaboration entre la recherche et les responsables politiques et les professionnel·le·s de la LEV. Il soulève des questions éthiques épineuses portant sur la complicité avec une surveillance problématique de la part de l'État, la répression policière et la poursuite du profilage racial, contribuant à une présence policière excessive auprès des groupes racialisés.

Richard Jackson, fondateur et rédacteur en chef de la revue *Critical Studies on Terrorism*, écrit que la « guerre contre le terrorisme » lancée au lendemain des attentats du 11 septembre 2001 aux États-Unis a « tué et blessé plus d'un million de personnes (…), causé des souffrances incalculables à des millions d'autres (…) et est l'un des outils de domination hégémonique des États occidentaux les plus efficaces de notre époque ». Il poursuit en déclarant que « le régime mondial de lutte contre le terrorisme est, dans sa philosophie, ses pratiques et ses effets, intrinsèquement violent et oppressif, et réduit l'espérance de vie » et que, « dans ces conditions, (…) on pourrait affirmer que la collaboration directe avec le dispositif étatique de lutte contre le terrorisme est comparable à la collaboration des professionnels médicaux avec des tortionnaires dans le but d'améliorer le bien-être des prisonniers »[194].

La recherche financée ou menée en partenariat avec les agences étatiques, telle que celle financée par le DHS et menée en partenariat l'Université et les services de police de Seattle, a une portée très limitée. Jackson écrit, de son point de vue d'éminent professeur critique spécialisé dans le terrorisme, que les « universitaires [critiques spécialisés dans le terrorisme] ont lancé l'alerte il y a plusieurs années et continuent d'émettre des critiques et des propositions alternatives, sans effet mesurable ; en gros, [ils] n'ont pas voix au chapitre dans le système actuel de lutte antiterroriste ». Il poursuit, en affirmant que les chercheurs et chercheuses consulté·e·s et invité·e·s à conseiller le gouvernement sont en réalité « principalement (…) utilisés par l'État pour donner une légitimité à des actions déjà décidées et consolider sa réputation publique »[195]. Puisque le champ d'action des enquêtes menées dans le cadre de partenariats entre les universités et le gouvernement se borne à fournir une légitimité intellectuelle aux pratiques de l'État, l'analyse critique indépendante du régime antiterroriste ou de certaines actions pratiquées en son sein est de plus en plus éloignée du centre de pouvoir et de décision de l'État.

193 https://www.dhs.gov/sites/default/files/publications/EMW-2016-CA-APP-00236%20Full%20Application.pdf
194 https://www.tandfonline.com/doi/pdf/10.1080/17539153.2016.1147771?needAccess=true, pp.121–2
195 *Ibid.*, p. 123

Certaines réponses à l'enquête mentionnée plus haut indiquent que les processus de validation en matière éthique et les questions relatives au respect de la vie privée, comme le respect des lois d'application du Règlement général sur la protection des données (RGPD) et des conditions d'utilisation des sociétés de médias sociaux, ont été des obstacles majeurs pour la recherche en matière de LEV. Ces obstacles, qui causent des retards importants dans la recherche et l'obtention de données ont, d'après l'analyse des résultats de l'enquête, « forcé de nombreux chercheurs et de nombreuses chercheuses à recourir à des données secondaires ».

Compte tenu de ce climat de recherche, où les analyses de sources primaires sont difficiles à produire et peuvent servir à légitimer des pratiques étatiques néfastes en matière de lutte contre le terrorisme, comment la recherche sur la LEV peut-elle avoir une pertinence pour les politiques tout en demeurant éthique ? Tout d'abord, la recherche en matière de LEV pourrait se fonder sur un mode d'enquête différent. Selon Jackson, la recherche qui vise à avoir une pertinence pour les politiques de manière orthodoxe « nous incite à poser certains types de questions et à chercher certains types de questions. Elle formule la question posée dans une optique de « résolution de problèmes », qui la conduit à se conformer avec la façon dont les responsables politiques articulent le « problème » et définissent l'éventail de solutions[196]. Un programme de recherche éthique qui accorde moins d'importance au paradigme « solutionniste » pourrait enquêter sur l'incidence de la lutte contre le terrorisme et de la LEV sur les communautés racialisées et marginalisées, et formuler des recommandations stratégiques visant à modifier les politiques en conséquence. Cela permettrait d'œuvrer pour comprendre la recherche ayant une pertinence politique comme une recherche qui ne se contente pas de légitimer les politiques de l'État, mais qui a une pertinence directe pour les communautés qu'elle cible.

Deuxièmement, la recherche qui apporte un éclairage sur les explications historiques, structurelles et sociétales – et non individuelles, idéologiques et raciales – de la violence contre les citoyens et l'État pourrait constituer le deuxième volet d'un programme de recherche éthique en matière de LEV. En élargissant le champ d'enquête pour prendre en compte la violence contre les communautés traditionnellement comprises comme étant « vulnérables à la radicalisation », la recherche en matière de LEV peut plaider en faveur de politiques cherchant à réparer les violences historiques et structurelles. Par exemple, en appréhendant le régime de détention et de déportation comme un préjudice institutionnel contre certaines communautés, la recherche en matière de LEV peut commencer à plaider pour le démantèlement de ces institutions et l'élaboration de politiques de gestion migratoire.

Enfin, la recherche en matière de LEV pourrait plaider, par le biais d'un programme de recherche axé sur les personnes touchées par les stratégies de lutte antiterroriste et destiné à améliorer leur sort, en faveur de l'abandon de l'approche pansociétale qui encourage une présence policière excessive dans ces communautés. Elle pourrait, de cette façon, effectuer des recherches sur l'incidence des politiques qui améliorent le sort des communautés, relatives

196 *Ibid.*

par exemple aux investissements dans le logement, aux services d'appui à la santé mentale, aux soins de santé et à l'emploi. La recherche en matière de LEV peut, en plaidant en faveur de ce type de besoins fondamentaux, en réduisant la présence policière dans les communautés et en assurant la compréhension de la violence structurelle, faire pression pour l'instauration d'interventions différentes dans le cycle de la violence.

COORDONNÉES

Pour toute question, demande d'information et demande de copies supplémentaires du présent rapport, contacter :

ICSR
King's College London
Strand
Londres WC2R 2LS
Royaume-Uni

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter : **@GNET_research**

Ce rapport peut, comme toutes les autres publications du GNET, être téléchargé gratuitement à partir du site Internet du GNET : www.gnet-research.org.

© GNET