SYNTHÈSE DE LA CONFÉRENCE EN LIGNE SUR LA LUTTE CONTRE LES COMMUNICATIONS TERRORISTES :

Propagande terroriste, provocation publique, recrutement et radicalisation

31 janvier – 1er février 2023

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Allocution de bienvenue de la présidente du Comité du Conseil de l'Europe de lutte contre le terrorisme (CDCT)

Mme Päivi Kairamo, Ambassadrice pour la coopération antiterroriste, Finlande, et présidente du CDCT

En tant que présidente du Comité du Conseil de l'Europe de lutte contre le terrorisme (CDCT) pour 2022-2023, j'ai l'honneur de présenter cette synthèse de la Conférence en ligne sur la lutte contre les communications terroristes.

Les terroristes modernes s'appuient fortement sur les médias et internet. La propagande est de longue date un élément clé des stratégies terroristes, qui visent à diffuser leur message de peur auprès de leur public cible, tout en incitant les individus à commettre de nouveaux actes de terrorisme.

Les terroristes et les extrémistes violents sont connus pour utiliser tous les moyens de communication dont ils disposent. Cela ajoute à la difficulté d'identifier et de contrôler un large éventail de médias et de sources. En effet, l'un des changements les plus notables dans le paysage terroriste de ces dernières années est le fait que les groupes et les réseaux en ligne sont devenus le principal moyen par lequel certains mouvements extrémistes violents communiquent avec d'autres, recrutent de nouveaux membres et inspirent de nouvelles attaques.

Aussi la mise en place de mécanismes efficaces de lutte contre les communications terroristes est-elle un volet essentiel de nos stratégies antiterroristes. La coopération internationale est, et restera, un aspect essentiel de notre travail. Nous devons disposer de mécanismes efficaces pour améliorer les échanges non seulement entre les autorités nationales et les services répressifs, mais aussi avec leurs homologues des plateformes technologiques et des fournisseurs de services en ligne. Nous jouons tous un rôle essentiel dans la prévention de la prolifération des communications terroristes, et nous soutenons les efforts visant à recueillir et partager des données et des informations essentielles sur les activités terroristes en ligne.

Cette conférence en ligne s'est tenue à un moment opportun pour avoir un débat approfondi sur ces sujets et combler certaines des lacunes dans la coordination entre les États et les organisations internationales, le secteur privé et le monde universitaire.

Dans notre lutte contre ce phénomène, nous ne devons pas perdre de vue la nécessité de respecter l'État de droit et les droits humains. Le fait de promouvoir ces valeurs et de les respecter dans nos propres politiques et actions est en lui-même un puissant contre-discours face au terrorisme.

Nous devons également nous rappeler que la lutte contre les communications terroristes ne se résume pas à empêcher que des attaques soient commises maintenant, mais suppose également d'entraver l'activité des terroristes sur le long terme. Le risque que des terroristes

mettent à profit le caractère opaque d'internet pour favoriser la prochaine vague d'attentats est réel. Nous devons mener une action coordonnée pour empêcher que ces projets ne se concrétisent.

À l'heure où nous réfléchissons à notre nouvelle Stratégie pour 2023-2027, le CDCT se félicite de l'occasion qui lui est donnée d'évoquer ces défis avec ses partenaires du monde entier.

Résumé

Avertissement : Les positions exprimées dans le présent résumé de la conférence ne reflètent pas la position officielle du Conseil de l'Europe.

Le Comité du Conseil de l'Europe de lutte contre le terrorisme (CDCT) a organisé une conférence en ligne sur le thème de « La lutte contre les communications terroristes : propagande terroriste, provocation publique, recrutement et radicalisation », au siège du Conseil de l'Europe les 31 janvier et 1er février 2023.

Le terrorisme moderne prend souvent une forme médiatique et de nombreux terroristes sont tout autant des propagandistes que des criminels violents. La vague actuelle du terrorisme s'est malheureusement nourrie de messages criminels postés dans un riche environnement médiatique, commettant des actes de violence horribles largement diffusés afin de contraindre et d'intimider les gouvernements et les citoyens. Les terroristes et les extrémistes violents ont utilisé à leurs fins des plateformes et des technologies en ligne pour le recrutement, l'entrainement, la radicalisation, la provocation publique, la propagande ou pour planifier, préparer et exécuter des attaques. Ce phénomène continue d'évoluer avec l'apparition de nouvelles plateformes et de nouveaux services, ce qui permet aux terroristes de trouver des moyens nouveaux et innovants d'exploiter les capacités offertes par ces technologies.

Compte tenu de ces défis, la Conférence a porté plus particulièrement sur les moyens de surveiller et de contrer les activités des groupes terroristes menées en ligne et hors ligne, notamment les efforts qu'ils déploient pour recruter et obtenir le soutien du public qu'ils ciblent ou pour se procurer les moyens et le savoir-faire nécessaires pour mener des attaques terroristes. Les autorités, les entreprises du secteur d'internet et d'autres acteurs mènent une lutte constante contre les contenus terroristes en ligne, du fait que les terroristes déclinent leur propagande sur plusieurs services, migrent vers des plateformes non réglementées et cryptées ou créent et hébergent leurs propres sites web.

La Conférence en ligne a bénéficié des connaissances d'experts, de praticiens et de décideurs hautement qualifiés dans ce domaine, ainsi que de représentants d'organisations régionales et internationales qui soutiennent les efforts mondiaux visant à résoudre ces problèmes. Les experts qui sont intervenus ont présenté leurs recherches de pointe sur les tendances et l'évolution du paysage des communications terroristes, tandis que les praticiens ont partagé leurs points de vue sur une série d'outils et de techniques disponibles pour contrer et empêcher la prolifération des terroristes et des extrémismes violents.

Ont également été évoquées lors de la Conférence certaines des questions clés liées à l'accès à des preuves électroniques et à leur obtention auprès d'entreprises d'internet privées à des fins d'enquêtes et de poursuites contre des personnes soupçonnées de terrorisme et d'extrémisme violent. Les mécanismes actuels visant à supprimer ou à restreindre l'accès aux contenus illicites ont été présentés et analysés, en tenant compte également de l'importance du respect des droits humains et des libertés fondamentales, en particulier de la liberté d'expression. Les droits humains ne doivent pas être considérés comme une entrave à ces efforts, mais comme un complément et un guide dans la lutte contre les communications terroristes en ligne et hors ligne.

L’accent a été mis également lors de la Conférence sur l’importance de renforcer la coopération internationale et le dialogue public-privé sur ces questions, en favorisant la compréhension mutuelle et l’échange de bonnes pratiques pour prévenir la propagande terroriste, la provocation publique, le recrutement et la radicalisation sous toutes ses formes et manifestations.

Session I : Radicalisation conduisant au terrorisme : Dimensions en ligne et hors ligne

La première session de la Conférence en ligne a porté sur certaines des questions relatives à la radicalisation menant au terrorisme et aux moyens par lesquels une personne peut être amenée à embrasser des idéologies terroristes et à mener des actions violentes ou à inspirer d'autres actes de terrorisme.

Si ce phénomène présente à la fois des dimensions en ligne et hors ligne, il a été suggéré que ces deux dimensions ne devraient pas être considérées comme des sphères entièrement séparées. Compte tenu de l'utilisation généralisée de dispositifs connectés à internet, les frontières entre les expériences en ligne et hors ligne sont de plus en plus floues, un phénomène que l'on peut également observer dans les communications terroristes.

En ce qui concerne plus particulièrement les dimensions en ligne du terrorisme et de l'extrémisme violent, il a été observé que les organisations utilisent un large éventail de plateformes en ligne, telles que des applications de messagerie, des médias sociaux ou même des plateformes de jeux vidéo, créant et diffusant une vaste gamme de contenus, y compris des images, des vidéos, des enregistrements audio, des textes, etc. De nombreux groupes terroristes ont également cherché à posséder et à exploiter leur propre site web incluant des forums et des espaces de discussion.

Cependant, les recherches suggèrent qu'il est rare que la radicalisation se fasse exclusivement par des moyens en ligne. Ainsi, les espaces hors ligne jouent toujours un rôle important dans la radicalisation terroriste, car les interactions en personne avec la famille, les amis et les connaissances demeurent un moyen courant de radicalisation menant au terrorisme et à l'extrémisme violent. En outre, il a été noté que les formes traditionnelles de communication (telles que les lettres écrites ou les documents papier), bien qu'elles puissent être peu pratiques, plus lentes et avoir une portée plus limitée, sont également plus difficiles à contrôler et à intercepter.

Cette première session a également mis en évidence certains des principaux aspects sociaux et psychologiques de la radicalisation, notamment en ce qui concerne l'idée d'un « continuum » de la radicalisation. La radicalisation, tant en ligne qu'hors ligne, peut être considérée comme un processus qui repose sur de multiples facteurs individuels et contextuels. Au niveau individuel, certains indicateurs de vulnérabilité générale à la radicalisation ont été analysés, tels qu'un faible contrôle des impulsions ou des antécédents criminels. D'après des recherches similaires dans le domaine de la santé publique, bien qu'il puisse exister une vulnérabilité sous-jacente, les individus ont moins de risques de se radicaliser si certains facteurs contextuels ne sont pas également présents. Des recherches supplémentaires sont nécessaires pour mieux comprendre ce qui caractérise un tel contexte si l'on veut prévenir globalement la radicalisation conduisant au terrorisme.

Lors de cette session, la question de la radicalisation a également été envisagée d'un point de vue national, en examinant le contexte spécifique de la radicalisation en ligne et hors ligne. En particulier, les intervenants ont souligné certaines différences essentielles dans les stratégies de radicalisation de plusieurs organisations, notamment l'EIIL (Daech), Al-Qaïda et ses groupes affiliés, Al-Chabab et diverses organisations violentes d'extrême droite. Certains de ces groupes

ciblent spécifiquement les jeunes et les enfants, qui peuvent être particulièrement vulnérables lorsqu'ils sont exposés à des contenus terroristes en ligne.

Les intervenants ont également évoqué les efforts nationaux de prévention et d'intervention pour lutter contre les communications terroristes et prévenir la radicalisation, soulignant la nécessité d'une coopération entre les acteurs publics et privés, la société civile et les organisations internationales et régionales. Il a largement été reconnu que l'éducation, en particulier en termes d'éducation aux médias, constitue une première ligne de défense importante contre la radicalisation.

Session II : Narratifs terroristes et incitation publique à commettre des attaques terroristes : Prévention et réponse

La deuxième session de la Conférence visait à comprendre la manière dont le discours terroriste et l'incitation publique à commettre des attaques violentes sont diffusés et quelles mesures peuvent être prises pour les prévenir et y répondre, en examinant les stratégies d'approche et le discours des organisations terroristes et extrémistes violentes telles que l'EIIL (Daech), Al-Qaïda et ses affiliés ainsi que des groupes d'extrême droite violents.

Il a été souligné que pratiquement toutes les organisations terroristes/d'extrémisme violent et leurs sympathisants ont une activité de communication stratégique. Toutefois, certaines distinctions importantes peuvent être faites : d'une part, il existe une production médiatique « au niveau organisationnel » (par exemple de la part de l'EIIL (Daech) ou d'Al-Qaïda), caractérisée par une structure hiérarchique et des niveaux élevés de logistique et de planification : d'autre part, il y a la communication « au sein de la société » (émanant par exemple de divers réseaux violents d'extrême droite), qui est généralement plus nébuleuse et novatrice, en particulier lorsqu'il s'agit d'utiliser les nouvelles technologies.

En outre, plusieurs intervenant ont également souligné que les contre-discours constituent un outil important pour prévenir les communications terroristes et y répondre. Les campagnes de communication stratégique telles que celles de la Cellule de communication de la Coalition internationale contre Daech visent à contrer les communications terroristes tout en favorisant la cohésion sociale et en rapprochant les communautés. D'une manière générale, les intervenants ont souligné les défis que pose l'adaptation des stratégies de lutte contre les communications terroristes à l'évolution du paysage terroriste et aux spécificités régionales.

Cette session a également offert une vue d'ensemble de certains outils actuels permettant de surveiller et répondre à la prolifération de contenus terroristes en ligne. En particulier, les réseaux en ligne étant exploités pour inspirer ou encourager les attaques terroristes, il a été souligné que les fournisseurs de services en ligne jouent un rôle crucial.

La coopération entre les secteurs privé et public a été reconnue comme un aspect

déterminant de la riposte aux communications terroristes. Le règlement de l'Union européenne sur les contenus à caractère terroriste en ligne constitue un changement législatif majeur dans ce domaine. Il instaure l'obligation, pour les fournisseurs de services d'hébergement, de lutter contre la prolifération des contenus à caractère terroriste tout en cherchant un équilibre effectif avec la liberté d'expression en ligne. Ce règlement prévoit un mécanisme de réponse rapide aux menaces imminentes, notamment le retrait du contenu à caractère terroriste de leurs plateformes dans un délai d'une heure, tout en exigeant certaines garanties et mesures, telles que des injonctions de conservation et la nécessité de prévoir des recours juridiques pour les contenus retirés par erreur. En vertu du règlement, les fournisseurs de services d'hébergement sont également tenus de mettre en place plusieurs mesures techniques ou opérationnelles proactives telles que l'affectation de personnel à la modération des contenus et la mise en place de moyens d'identifier et de supprimer des contenus.

En outre, afin d'identifier et de supprimer de tels contenus, les fournisseurs de services en ligne peuvent combiner des technologies de modération automatisée des contenus, capables de détecter des violations potentielles des politiques, avec un contrôle humain. Sachant que les terroristes et les extrémistes violents sont capables d'adapter leurs stratégies de communication pour contourner ces efforts de modération, les équipes chargées de la modération des contenus doivent constamment mettre à jour leurs politiques et leur approche afin de rester efficaces.

Session III : Prévenir et entraver le recrutement de terroristes

La troisième session de la Conférence a été consacrée aux défis liés aux activités visant à prévenir et entraver le recrutement pour le terrorisme et l'extrémisme violent.

Lors de cette session, l'accent a été mis en particulier sur la question de la manipulation de jeunes aux fins du recrutement dans des milieux terroristes et extrémistes violents, une question d'autant plus cruciale qu'internet permet maintenant aux terroristes et aux extrémistes violents d'atteindre, d'influencer et de recruter plus facilement des jeunes dans le monde entier.

Diverses stratégies de recrutement de terroristes ont été recensées, variant souvent en fonction de l'axe idéologique principal du mouvement (comme les groupes misogynes violents, les mouvements inspirés par l'EIIL (Daech) ou l'extrémisme d'extrême droite violent). En outre, il a été démontré que les groupes terroristes et extrémistes violents ont recours à une manipulation des médias à la fois sophistiquée et coordonnée, évitant souvent de manière stratégique les efforts de modération des contenus sur les plateformes traditionnelles tout en migrant vers des sites alternatifs dont les politiques en matière de contenus extrémistes violents sont plus faibles, voire inexistantes.

Un phénomène récent notable est celui de certains mouvements qui ont donné à leurs actions en ligne un caractère ludique, en appliquant des concepts de jeu à des contextes non liés au jeu. Il s'agit, par exemple, d'appeler les sympathisants et les agresseurs potentiels à obtenir de

nouveaux « scores élevés » en matière de violence dans le monde réel. Ces éléments peuvent avoir pour effet de stimuler l'engagement et servir de source d'inspiration pour la reproduction d'attaques. S'il a été souligné que les jeux vidéo et leur culture ne sont pas problématiques en eux-mêmes, il convient cependant d'examiner l'ampleur et la prévalence de l'utilisation abusive des espaces de jeu par des extrémistes à des fins de radicalisation conduisant au terrorisme.

Ces problèmes sont aggravés par la fluidité notable des frontières entre le monde en ligne et la réalité pour les jeunes et par le caractère souvent virtuel de l'engagement en ligne. Ainsi, il peut être difficile de faire la différence entre des convictions profondément ancrées et un jeu de rôle virtuel ou de délimiter clairement le *trolling* et les idéologies extrémistes réelles.

Lors de cette session, des initiatives internationales visant à prévenir le recrutement de terroristes ont été présentées. Pour résoudre ces problèmes, les spécialistes de la lutte contre le terrorisme, les décideurs politiques et les chercheurs doivent travailler en étroite collaboration avec les plateformes en ligne, y compris les médias sociaux et les services de jeux, afin de limiter la capacité des extrémistes à exploiter ces espaces.

Des modèles d'intervention spécifiques tels que la Méthode de redirection ont été cités comme étant potentiellement efficaces à cet égard. Il s'agit d'un modèle d'intervention visant à rediriger les utilisateurs vulnérables vers des contenus plus sûrs et non extrémistes, tels que des services de santé mentale, des services de conseil de crise ou d'autres sites proposant des messages de substitution convaincants et crédibles.

Dans cet esprit, la Conférence a également souligné la contribution du Groupe de travail sur la lutte contre l'extrémisme violent (LEV) du Forum mondial de lutte contre le terrorisme (FMLT), qui travaille sur ces questions depuis de nombreuses années, notamment sur des textes clés tels que les recommandations de Zurich-Londres du Forum mondial de lutte contre le terrorisme (GCTF) sur la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne.

Cependant, des solutions plus durables pour prévenir le recrutement peuvent nécessiter des systèmes d'intervention précoce et une prévention primaire renforcée. Il peut être nécessaire de déployer des efforts plus importants pour améliorer la culture, la formation et l'éducation au numérique, qui peuvent améliorer et renforcer la résilience des communautés face au terrorisme.

Session IV : Prévention de la prolifération d'éléments matériels relatifs à l'entraînement terroriste

Cette quatrième session a porté sur les moyens et les méthodes utilisés par les terroristes et les extrémistes violents pour diffuser du matériel didactique et des conseils aux recrues potentielles, aux membres actuels et aux acteurs isolés potentiels.

En examinant différents types de matériels didactiques, il a été observé que ceux-ci peuvent varier selon le niveau d'organisation d'un groupe terroriste ou extrémiste violent particulier. Sur la base du rapport de taxonomie des données de partage de hachages du GIFCT, les matériels d'entraînement au terrorisme peuvent être distingués d'autres types de matériels, tels que les *matériels idéologiques* conçus pour promouvoir la vision du monde d'un mouvement particulier, les *matériels d'inspiration* destinés à renforcer ou à radicaliser davantage les sympathisants.

Bien que de nombreux groupes terroristes produisent des documents combinant tout ou partie de ces éléments, les intervenants se sont intéressés plus particulièrement à cette dernière catégorie de contenus didactiques, qui peuvent fournir à leurs lecteurs des connaissances spécifiques sur la manière de préparer et de mener des attaques terroristes. Les matériels didactiques peuvent ainsi apporter de dangereuses instructions étape par étape sur des questions telles que la façon d'effectuer la reconnaissance de cibles potentielles, de préparer ou d'utiliser divers types d'explosifs et d'armes ou de garantir le secret des opérations.

En ce qui concerne la modération de ce type de contenus par les plateformes internet, il a été noté que les matériels didactiques peuvent poser un problème particulier et qu'ils doivent être analysés et contextualisés correctement. Cela s'explique par le volume important des contenus didactiques en ligne qui peuvent être utiles aux terroristes et aux extrémistes violents, mais qui ne sont pas explicitement de nature terroriste (comme des instructions générales sur le maniement des armes ou divers types de textes politiques).

De plus, bon nombre de matériels didactiques fournissent des conseils sur les aspects non violents du terrorisme, par exemple sur la façon d'entrer en contact avec des sympathisants potentiels et des recrues en ligne, celle d'obtenir et de distribuer des ressources financières ou encore celle de fabriquer ou falsifier des documents aux fins de voyages à destination ou en provenance des territoires contrôlés par l'EIIL/Daech.

La session a bénéficié de l'expertise de l'Équipe d'enquêteurs des Nations Unies chargée d'amener l'EIIL/Daech à répondre de ses crimes (UNITAD), qui a pour mandat d'aider les autorités nationales à amener traduire les membres de l'EIIL/Daech en justice pour leurs crimes en recueillant, préservant et conservant des éléments de preuve conformément aux normes internationales. Il est notoire que l'EIIL/Daech a utilisé internet pour diffuser une grande variété de matériels d'entraînement et d'instruction à ses adeptes dans le monde entier, et il a été observé que l'EIIL/Daech (ainsi que certains groupes affiliés à Al-Qaïda) ont longtemps considéré internet comme un terrain d'entraînement virtuel ou une extension du champ de bataille lui-même. Ces groupes ont produit des guides sur des thèmes tels que la guerre électronique, les interrogatoires, les enlèvements, la

fabrication de tunnels ou les engins explosifs improvisés, ainsi que sur la façon d'acquérir du matériel pour construire des armes chimiques, biologiques, radiologiques ou nucléaires (CBRN) improvisées.

Il s'est avéré difficile de retirer complètement ces matériels d'internet, ce qui représente un risque important et permanent. En outre, il a été souligné que si les groupes terroristes et extrémistes violents ont souvent élaboré des matériels didactiques adaptés à leur idéologie et à leurs objectifs spécifiques, il y a eu également un certain degré de pollinisation croisée dans la mesure où divers acteurs terroristes et extrémistes violents ont utilisé de tels matériels pour incorporer des idées et des pratiques d'autres mouvements dans leur *modus operandi*.

Session V : La criminalistique numérique et les preuves électroniques dans la lutte contre le contenu terroriste en ligne

Étant donné que les mouvements terroristes et extrémistes violents dépendent de plus en plus d'un vaste écosystème de plateformes en ligne, cette session a été consacrée à la compréhension des principaux défis et des utilisations potentielles concernant l'identification, la collecte et la conservation des preuves électroniques.

Les contenus terroristes en ligne et les métadonnées qui y sont associées sont de plus en plus utilisés à des fins d'enquêtes criminelles. Les praticiens des services répressifs ont souligné l'importance des preuves électroniques dans les affaires de terrorisme national et international, insistant sur la nécessité de mettre en place et de renforcer les capacités techniques de collecte, de conservation et d'analyse des données électroniques afin de mener à bien les enquêtes et les poursuites relatives aux infractions terroristes.

Toutefois, les services répressifs sont confrontés à plusieurs défis importants à cet égard, notamment en raison de la grande quantité de données à traiter, de la variété des dispositifs ou applications (ainsi que des applications cryptées) et du nombre de langues pouvant être impliquées. Il a été reconnu que de nombreux services répressifs ne disposent pas d'une expertise et d'outils médico-légaux suffisants pour collecter, stocker et conserver correctement des données électroniques provenant d'un éventail aussi large de sources potentielles.

Les organisations et les réseaux terroristes adaptent en permanence leurs stratégies de communication à mesure que la technologie évolue et migrent vers des plateformes cryptées ou fermées pour éviter d'être détectés. Il est ainsi devenu très difficile pour les entreprises technologiques d'avoir accès aux données sur les services en ligne, en particulier lorsque ces plateformes sont exploitées ou détenues dans un ou plusieurs pays étrangers. Cette situation requiert souvent des autorités répressives qu'elles travaillent avec des partenaires et des intermédiaires internationaux pour avoir accès à des preuves et des données électroniques essentielles. Une autre difficulté peut venir des différences entre les cadres juridiques, de l'absence de politiques normalisées dans le secteur numérique, de la longueur des procédures formelles et du manque subjectif de réactivité aux demandes de conservation

et de divulgation. En l'absence de systèmes harmonisés et efficaces, certaines autorités nationales ont plutôt recherché des arrangements ponctuels ou une coopération volontaire directe de la part des fournisseurs de services en ligne, même dans des circonstances où il existe des mécanismes de coopération judiciaire ou d'entraide judiciaire.

Un certain nombre d'initiatives internationales et régionales visent à répondre à ces problèmes. En particulier, l'Organisation pour la sécurité et la coopération en Europe (OSCE) a proposé aux services répressifs un certain nombre de formations aux médias et à l'information. Plusieurs projets ont produit des résultats tels que le guide pratique pour les demandes transfrontalières de preuves électroniques, élaboré conjointement avec l'Office des Nations Unies contre la drogue et le crime.

En outre, des initiatives telles que le projet SIRIUS d'EUROPOL sont conçues pour aider les services répressifs et les autorités judiciaires à améliorer l'accès aux preuves électroniques lors des enquêtes pénales. Ce projet est en outre soutenu par une série de recommandations formulées à l'intention des autorités répressives et des fournisseurs de services en ligne, qui figurent dans le rapport de situation SIRIUS sur les preuves numériques dans l'UE.

Il est nécessaire d'améliorer la transparence et la coopération entre les différents acteurs publics et privés dans ce domaine, en particulier en vue de la mise au point de mécanismes et d'outils efficaces pour recueillir, conserver et analyser les preuves électroniques tout en préservant la chaîne de conservation en vue de leur utilisation devant un tribunal.

Session VI : Renforcer les mécanismes des droits humains et de l'État de droit dans la lutte contre les contenus terroristes en ligne

Lors de cette dernière session de la Conférence, les intervenants ont évoqué l'importance de renforcer les mécanismes des droits humains et de l'État de droit dans la lutte contre les contenus terroristes en ligne. Cet aspect demeure un défi pour de nombreux gouvernements et entreprises d'internet, eu égard à la nécessité de trouver un équilibre entre les droits humains, la lutte contre le terrorisme et un internet libre, ouvert et sécurisé.

Les discours radicaux et extrémistes sont généralement protégés par les lois sur la liberté d'expression et ne peuvent être restreints par les États que dans des circonstances exceptionnelles, nécessaires et proportionnées. Les contenus en ligne sont toutefois généralement soumis à des règles de modération privées, à des normes collectives ou à des conditions d'utilisation qui sont définies par les plateformes en ligne elles-mêmes. Ces conditions d'utilisation définissent des obligations, des limites et des conditions pour l'utilisation de la plateforme qui vont au-delà des dispositions légales applicables et elles s'appliquent généralement à tous les utilisateurs, indépendamment de la juridiction réelle de l'utilisateur.

Les intervenants ont fait observer que ces questions peuvent être rendues plus

complexes du fait du rôle émergent que les entreprises privées peuvent jouer dans la lutte contre le terrorisme et de l'absence d'une délimitation claire des tâches et responsabilités qui leur incombent. Certains des défis auxquels les entreprises technologiques sont confrontées découlent donc de difficultés persistantes au sein du cadre international de la lutte contre le terrorisme. Si le terrorisme peut être bien défini par les cadres juridiques nationaux ou régionaux, il existe des différences significatives entre les juridictions en ce qui concerne des concepts fondamentaux tels que le « terrorisme » et l'« extrémisme violent ». Les entreprises privées peuvent avoir du mal à déterminer clairement quels contenus doivent être interdits, supprimés et conservés. Bien que de nombreuses entreprises s'appuient sur les listes internationales du terrorisme pour guider leurs actions, cette approche peut présenter des risques importants, car ces listes peuvent ne pas être à jour par rapport aux menaces terroristes actuelles ou être utilisées de manière abusive par certains États pour restreindre le comportement légitime de communautés minoritaires ou de certaines catégories protégées, telles que les journalistes, les défenseurs des droits humains ou les organisations de la société civile.

Les entreprises du secteur privé, à la différence des organismes publics, ne sont pas directement liées par la législation sur les droits humains. Des instruments tels que les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme constituent un ensemble essentiel de normes non contraignantes qui peuvent guider l'action du secteur privé dans ce domaine.

Des initiatives clés telles que l'Appel de Christchurch et son Réseau consultatif, lancés conjointement par la Nouvelle-Zélande et la France, soutiennent les efforts visant à lutter contre le terrorisme et l'extrémisme violent tout en promouvant les droits humains. Le Réseau consultatif contribue à garantir que les groupes de la société civile, le monde universitaire et les organisations de défense des droits humains jouent un rôle actif dans l'élaboration de réponses aux contenus terroristes en ligne. En outre, le Forum mondial de l'Internet pour la lutte contre le terrorisme (GIFCT), organisation à but non lucratif et initiative technologique, s'est employé à faire en sorte que les droits humains soient une composante essentielle et complémentaire de son travail, en exigeant des entreprises qui en sont membres qu'elles respectent les valeurs des droits humains tout en empêchant les terroristes et les extrémistes violents d'exploiter leurs services numériques.

Les participants ont évoqué la nécessité de mettre en place des garanties appropriées et efficaces pour que les individus puissent faire valoir leurs droits humains lorsque des contenus sont retirés ou ciblés de manière abusive. Ainsi, pour fonder la lutte contre les contenus terroristes sur une approche claire basée sur les droits humains, il est nécessaire de renforcer et d'améliorer les cadres juridiques internationaux actuels applicables aux entreprises privées.

Principaux enseignements de la Conférence

Bien qu'ayant couvert un large éventail de sujets interdépendants, cette Conférence n'a pu explorer en profondeur un domaine complexe et difficile. Il est possible d'en tirer quelques enseignements clés afin d'orienter les actions et événements futurs du CDCT dans ces domaines :

- Les terroristes ont fait preuve d'innovation en utilisant diverses plateformes de communication en ligne pour diffuser leur idéologie, inspirer ou encourager les attaques terroristes et fournir des matériels didactiques aux attaquants. Les terroristes et les extrémistes violents déploient toute une série de stratégies de communication basées en grande partie sur les spécificités de leur organisation, de leur idéologie et de leur public cible. En particulier dans les mouvements terroristes décentralisés ou post-organisationnels où les attaques menées par un acteur isolé sont devenues la norme, une grande partie de ces matériels visent à encourager des individus à commettre des attaques violentes et à leur en donner les moyens.
- Si cette propagande peut viser à radicaliser des individus vers le terrorisme, la radicalisation est souvent un processus complexe et non linéaire qui peut dépendre de multiples facteurs individuels et contextuels. Afin de prévenir et d'enrayer la radicalisation de manière globale, il est important de comprendre et d'identifier les risques liés aux caractéristiques et circonstances individuelles ainsi qu'aux facteurs locaux. Les dimensions en ligne et hors ligne de la radicalisation conduisant au terrorisme ne doivent pas être considérées comme étant distinctes, mais plutôt comme étant complémentaires et interdépendantes. Bien que les espaces en ligne puissent permettre aux terroristes et aux extrémistes violents d'atteindre un public plus large, les espaces hors ligne et les interactions en personne jouent encore un rôle essentiel dans la radicalisation terroriste.
- Les jeunes sont de plus en plus la cible des terroristes et des extrémistes violents, soit pour gagner des adeptes et des sympathisants à leur idéologie et leur cause, soit pour les recruter directement. De nombreuses stratégies de communication terroriste sont conçues pour attirer un public jeune, par exemple en utilisant des éléments de la culture pop, des jeux vidéo ou des mèmes dans leurs communications. Des mesures de prévention spécifiques sont nécessaires pour renforcer la résilience du secteur de la jeunesse, notamment par l'éducation et la formation aux médias.
- Les systèmes d'alerte précoce et les mécanismes de réaction visant à surveiller, conserver ou supprimer de tels contenus en ligne des plateformes internet devraient être régulièrement mis à jour et révisés, en coopération avec les organismes nationaux et internationaux, selon le cas, et en tenant compte des principales évolutions et modalités de l'utilisation abusive d'internet par des terroristes.
- L'identification précise des contenus terroristes en ligne peut être vitale pour les enquêtes et éventuellement les poursuites concernant toute une série d'infractions terroristes. Si la suppression de ces contenus est essentielle pour limiter la diffusion de la propagande terroriste, il est également nécessaire de collecter et de conserver correctement ces contenus afin qu'ils puissent servir de preuves dans le cadre de procédures pénales. Cependant, l'accès à des preuves électroniques, en particulier au-delà des frontières, dépend à la fois de la coopération internationale entre les États et de la coopération avec les fournisseurs de services en ligne. Afin de faciliter et d'améliorer le processus de demande de divulgation ou de conservation des données,

il est nécessaire que les acteurs clés de toutes les parties soient correctement formés et informés sur les principales questions techniques et juridiques d'intérêt mutuel.

- L'absence de définitions harmonisées du contenu à caractère terroriste et extrémiste violent pose depuis longtemps un certain nombre de problèmes. Les États et les fournisseurs de services en ligne doivent élaborer des normes appropriées qui tiennent dûment compte de leurs responsabilités et rôles respectifs, conformément aux principes des droits humains et de l'État de droit. Des garanties et des systèmes efficaces devraient être élaborés et mis en œuvre afin de lutter contre les contenus terroristes en ligne tout en préservant le caractère libre, ouvert et sûr d'internet.