Rapport sur les modèles émergents de détournement des technologies par les acteurs terroristes

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Rapport sur les modèles émergents de détournement des technologies par les acteurs terroristes

Conseil de l'Europe

Édition anglaise :

Report on the emerging patterns of misuse of technology by terrorist actors

Toute autre correspondance relative à ce document doit être adressée à la Direction générale Droits humains et État de droit, Conseil de l'Europe,
F-67075 Strasbourg Cedex,
Courriel dgi-cdct@coe.int

Conception de la couverture et mise en page : Division publications et identité visuelle, Conseil de l'Europe

Photo : Shutterstock

Imprimé dans les ateliers du Conseil de l'Europe

Table des matières

Liste des abréviations

CAO : conception assistée par ordinateur

CBRN : chimiques, biologiques, radiologiques ou nucléaires

CDCT : Comité du Conseil de l'Europe de lutte contre le terrorisme

EEI : engins explosifs improvisés

EIAO : l'État islamique en Afrique de l'Ouest

EIIIL : État islamique en Irak et au Levant

EIPK : l'État islamique – Province de Khorassan

GCTF : Global Counterterrorism Forum (Forum mondial de lutte contre le terrorisme)

GIFCT : Global Internet Forum to Counter Terrorism (Forum mondial de l'internet contre le terrorisme)

GNET : Global Network on Extremism and Technology (Réseau mondial sur l'extrémisme et la technologie)

IA : intelligence artificielle

LBC/FT : lutte contre le blanchiment de capitaux et le financement du terrorisme

LFT : lutte contre le financement du terrorisme

PKK : Parti des travailleurs du Kurdistan

Avant-propos

Les groupes et réseaux terroristes et extrémistes violents recourent de plus en plus aux nouvelles technologies pour mener à bien leurs activités criminelles en organisant, finançant, perpétrant et relayant en direct des attentats. De tels actes compromettent notre sécurité et mettent en péril notre mode de vie démocratique. Dans un monde où chaque avancée technologique peut être utilisée à mauvais escient par des terroristes et extrémistes violents, il est important d'identifier leurs modèles d'utilisation de ces technologies afin de mieux définir et mettre en œuvre des mesures efficaces. Tel est précisément l'objectif de cette publication. Cette dernière examine pourquoi et comment ces groupes et réseaux utilisent les technologies, et l'impact sur le paysage terroriste actuel. Elle formule des recommandations concrètes destinées aux praticiens ainsi qu'aux responsables politiques.

Cette publication a été élaborée dans le cadre de la Stratégie du Conseil de l'Europe contre le terrorisme (2023-2027), avec le soutien du ministère fédéral allemand des Affaires étrangères. Sous l'égide du Comité du Conseil de l'Europe de lutte contre le terrorisme (CDCT), M. David Wells a contribué à son élaboration en tant qu'expert indépendant. Nous remercions tout particulièrement les praticiens des États membres du Conseil de l'Europe, ainsi que les représentants de l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), du Groupe d'action financière (GAFI) et du Forum mondial de l'internet contre le terrorisme (Global Internet Forum to Counter Terrorism, GIFCT), dont les contributions ont permis de formuler les conclusions et les recommandations.

Résumé

Bien que depuis un certain temps, l'utilisation abusive des nouvelles technologies par des acteurs terroristes soit une préoccupation majeure, les capacités offertes par toute une série de technologies nouvelles et émergentes – y compris les plateformes de jeux, les systèmes aériens sans pilote (drones), l'intelligence artificielle (IA) et les armes imprimées en 3D – (et la disponibilité de ces technologies) ont encore renforcé ces craintes.

Une analyse de la manière dont les terroristes adoptent les nouvelles technologies et des raisons qui les poussent à le faire montre que, pour beaucoup d'entre eux, c'est le contexte qui dicte leurs actions, l'ampleur et la rapidité de l'innovation étant influencées par des facteurs internes (notamment stratégiques, structurels et individuels) et externes, en particulier les rapports, les ressources et l'impact de la lutte contre le terrorisme. Dès lors qu'ils sont combinés les uns aux autres, ces facteurs peuvent encourager ou inhiber l'adoption de nouvelles technologies par les acteurs terroristes, ce qui se traduit par des variations significatives s'agissant de l'adoption et de l'utilisation des principales technologies, qui sont sources de préoccupation.

Les acteurs terroristes présents en Europe ou ayant des effets sur celle-ci ont adopté (ou commencent à adopter) un grand nombre de ces technologies. Les plateformes de médias sociaux, les petites ou microplateformes, les sites web hébergés par des terroristes et les plateformes de jeux ou liées à des jeux tiennent une place essentielle dans le processus de radicalisation et de recrutement. Les technologies émergentes utilisées dans ce processus comprennent le web décentralisé, le *dark web* et, plus récemment, l'IA générative.

Bien que de nombreux attentats terroristes en Europe utilisent un *modus operandi* peu technologique, la technologie joue un rôle clé dans leur préparation, leur planification et leur promotion ultérieure. Le matériel de propagande et d'instruction – généralement stocké et partagé en ligne – joue un rôle prépondérant dans la définition des cibles et des méthodes d'agression. Par exemple, l'émergence de l'utilisation d'armes imprimées en 3D par des acteurs terroristes en Europe a été alimentée par du matériel pédagogique élaboré par une sous-culture active en ligne. D'autres sous-cultures d'extrême droite en ligne ont également encouragé la diffusion en direct d'attentats et le partage de manifestes en ligne.

Les acteurs terroristes en Europe utilisent une série d'activités licites et illicites pour financer leurs attentats et leurs activités de radicalisation et de recrutement, dont certaines (mais pas toutes) nécessitent l'utilisation de nouvelles technologies. Il s'agit notamment des systèmes de paiement mobile, des bourses et portefeuilles en ligne, du *crowdfunding*, des transferts de fonds en ligne de pair à pair et de la sollicitation de dons sur les plateformes de médias sociaux. Simultanément, les acteurs terroristes hors d'Europe – notamment EIIIL (État islamique en Irak et au Levant)/Daech – encouragent de plus en plus les dons par le biais d'actifs virtuels, ce qui a entraîné une augmentation de la présence d'actifs virtuels dans les arrestations et les poursuites liées au financement du terrorisme en Europe.

Les entretiens avec des experts nationaux, régionaux et internationaux ont permis de dégager des enseignements et des bonnes pratiques pour répondre à l'utilisation abusive des nouvelles technologies par les terroristes. Il s'agit notamment de réduire le délai entre l'exploitation des nouvelles technologies par les terroristes et les réactions antiterroristes (grâce à des exercices d'analyses prospectives et à un meilleur partage de l'information), d'accorder une importance cruciale aux approches multipartites, à l'identification et à la gestion des risques liés aux droits humains, et de tirer avantage d'une plus grande clarté stratégique, qui peut conduire à viser avant tout les résultats souhaités plutôt que de définir les étapes nécessaires pour les atteindre.

Introduction

La Stratégie du Conseil de l'Europe contre le terrorisme (2023-2027)1 a fait de l'augmentation des cas de détournement de la technologie à des fins terroristes l'un de ses principaux domaines d'intervention, indiquant que les terroristes exploitent les nouvelles technologies pour leur recrutement et la planification, le financement et l'exécution d'attentats. L'activité 1.4 de la stratégie prévoit l'établissement d'un rapport analytique sur les modèles émergents de détournement des technologies par les acteurs terroristes, afin d'aider les États membres à identifier les principaux modèles d'utilisation, les vulnérabilités et les risques associés à ces évolutions, et à mener les actions nécessaires pour surveiller, perturber et intercepter les activités terroristes. Lors de sa 12e réunion plénière tenue le 14 mai 2024, le Comité du Conseil de l'Europe de lutte contre le terrorisme (CDCT) a approuvé la première ébauche du rapport, et a chargé son consultant indépendant, David Wells, de produire un avant-projet de rapport pour présentation lors de sa 13e réunion plénière, en novembre 2024.

Le présent rapport s'appuie principalement sur une phase de recherches approfondies, comprenant notamment l'examen d'un large éventail de travaux universitaires et de rapports émanant de diverses institutions nationales, régionales et internationales (parmi lesquelles le Conseil de l'Europe), axés sur le terrorisme et les nouvelles technologies. Cette analyse documentaire a été complétée par des entretiens avec des experts de premier plan, membres de dix institutions nationales et internationales différentes, ayant chacun participé activement, à différents titres, à la lutte contre l'utilisation de la technologie par les terroristes. Ces entretiens non nominatifs ont été réalisés à distance et visaient à mieux appréhender l'efficacité des différentes contre-mesures mises en œuvre pour lutter contre le détournement de diverses nouvelles technologies et identifier les enseignements tirés et les bonnes pratiques afin d'éclairer les interventions futures.

La collecte et l'analyse des données ont été synthétisées dans le présent rapport qui, outre cette introduction, comprend une courte section décrivant le contexte plus large du terrorisme et des nouvelles technologies, ainsi que trois sections consacrées aux questions de fond suivantes :

- pourquoi les terroristes adoptent-ils les nouvelles technologies ?
- comment les nouvelles technologies influent-elles sur le paysage terroriste actuel que connaît l'Europe (et dont elle subit l'impact) ?
- quels enseignements tirer des réponses antiterroristes aux nouvelles technologies et quelles bonnes pratiques adopter ?

Une analyse des informations et des données recueillies dans le cadre des travaux de recherche et des entretiens a guidé l'élaboration d'un ensemble restreint de recommandations concernant les actions de suivi que pourraient entreprendre le Conseil de l'Europe et ses États membres pour renforcer la lutte contre le terrorisme et atténuer les risques encourus.

1. Comité du Conseil de l'Europe de lutte contre le terrorisme (CDCT), Stratégie du Conseil de l'Europe contre le terrorisme (2023-2027), CM2023(2), 8 février 2023.

Contexte

De tout temps, les terroristes ont détourné les technologies qui leur ont permis de démultiplier leur pouvoir, d'agir avec une force bien supérieure à leur taille réelle et d'instiller une peur sans commune mesure avec la menace réelle qu'ils représentaient. De l'invention de la dynamite au XIX[e] siècle[2] à l'expérimentation, encore tâtonnante, de l'IA générative en 2024[3], l'utilisation de la technologie par les terroristes (et la manière d'y répondre au mieux) a peut-être été le défi le plus constant de la lutte contre le terrorisme.

Ces dix dernières années, l'éventail des nouvelles technologies disponibles et les capacités qu'elles offrent se sont développés à un rythme effréné. Certes, beaucoup d'entre elles sont (ou pourraient être) très utiles aux gouvernements, y compris dans le domaine de la lutte contre le terrorisme, mais leur détournement réel ou potentiel par les terroristes et les acteurs extrémistes violents – et la rapidité de ce phénomène par rapport à l'intégration souvent lente des nouvelles technologies dans les interventions stratégiques et opérationnelles – constitue une préoccupation majeure pour les praticiens, les responsables politiques et le large panel d'entités impliquées dans la lutte contre le terrorisme aujourd'hui.

Le Conseil de sécurité de l'Organisation des Nations Unies a reconnu cette évolution pour la première fois dans sa Résolution 2129, adoptée en 2013, dans laquelle il prend acte « du lien qui existe entre le terrorisme et les technologies de l'information et des communications, en particulier [i]nternet », et de l'usage qui est fait de ces technologies pour « recruter, inciter à commettre, financer et planifier » des actes de terrorisme[4]. Ce cadre, et notamment l'accent spécifique mis sur l'utilisation d'internet par les terroristes, a donné lieu à un ensemble d'initiatives et d'activités ultérieures, dont plusieurs résolutions du Conseil de sécurité[5], certains éléments de la Stratégie du Conseil de l'Europe contre le terrorisme (2018-2022)[6] (y compris son rapport ultérieur sur les menaces terroristes émergentes en Europe[7]), des initiatives publiques et privées telles que le Forum mondial de l'internet contre le terrorisme (Global Internet Forum to Counter Terrorism-GIFCT) et des actions d'organisations de la société civile (dont l'Appel de Christchurch), ainsi que les recommandations de Zurich et Londres du Forum mondial de lutte contre le terrorisme (Global Counterterrorism Forum-GCTF) sur la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne[8].

Plus récemment, cette approche a été étendue aux défis posés par l'utilisation à mauvais escient de diverses technologies nouvelles et émergentes[9]. L'exploitation de ces technologies par des terroristes et des extrémistes violents est parfois déjà effective et a des répercussions opérationnelles (en Europe et ailleurs). Il s'agit notamment du recours aux actifs virtuels et au financement participatif pour se procurer des fonds et les faire circuler, des activités de radicalisation et de recrutement menées par les terroristes sur des plateformes de jeux et des plateformes connexes, de l'utilisation de systèmes autonomes sans pilote (communément appelés « drones ») pour effectuer des reconnaissances, filmer de la propagande et commettre des attentats, ainsi que de l'utilisation d'armes imprimées en 3D dans le cadre de plusieurs projets terroristes. Pour ce qui est d'autres applications – comme l'utilisation abusive de l'IA générative et des réalités virtuelles ou augmentées à des fins de propagande ou opérationnelles, ou les risques potentiels posés par les activités cyberterroristes – la priorité a été donnée à l'anticipation, en raison des inquiétudes suscitées par les conséquences possibles (ou à très court terme) d'un détournement de ces technologies.

2. Hammes T. X.,« Terror and technology : from dynamite to drones », *War on the Rocks*, 4 septembre 2020.
3. Wells D., « The next paradigm-shattering threat ? Right-sizing the potential impacts of generative AI on terrorism », Middle East Institute, 18 mars 2024.
4. La Résolution 2129 (S/RES/2129) a été adoptée par le Conseil de sécurité des Nations Unies le 17 décembre 2013. Le texte intégral est disponible ici.
5. Il s'agit notamment de résolutions énonçant des exigences relatives à la collecte d'éléments de preuve numériques (par exemple la Résolution 2396 (2017)), à la lutte contre la propagande terroriste (Résolution 2354 (2017)) et à la lutte contre le financement du terrorisme (Résolution 2462 (2019)).
6. Voir par exemple l'activité 1.2 « Prévenir et combattre l'incitation publique, la propagande, la radicalisation, le recrutement et la formation en lien avec le terrorisme sur internet », Stratégie du Conseil de l'Europe contre le terrorisme (2018-2022), CM(2018)86, CDCT, 4 juillet 2018.
7. Le rapport est disponible ici.
8. Les recommandations sont publiées sur le site internet du GCTF, ainsi que la Boîte à outils, développée ultérieurement (afin de rendre opérationnelles les recommandations).
9. Voir par exemple la Déclaration de Delhi sur la lutte contre l'utilisation des technologies nouvelles et émergentes à des fins terroristes du Comité contre le terrorisme du Conseil de sécurité des Nations Unies, 29 octobre 2022.

Parallèlement à l'utilisation à mauvais escient des nouvelles technologies, les terroristes et les extrémistes violents exploitent également toute une panoplie de technologies existantes et éprouvées pour mener à bien leurs activités. Ainsi, dans certains cas, ils se sont tournés vers des solutions simples et peu technologiques pour échapper à la vigilance des autorités, comme les attaques au couteau, l'utilisation de véhicules en tant qu'armes, ou encore l'utilisation de hawalas et de mules pour les transactions financières, la première étant particulièrement répandue en Europe. Dans les régions ou les pays les plus touchés actuellement par le terrorisme – notamment dans de nombreuses régions d'Afrique –, les approches « rudimentaires » constituent souvent la solution par défaut. Les activités de recrutement et de radicalisation se déroulent fréquemment hors ligne, et les armes conventionnelles vieillissantes ainsi que les engins explosifs improvisés (EEI) sont les principaux moyens utilisés pour commettre les attaques.

L'une des explications possibles de cette divergence manifeste entre le rôle nuancé et contextuel joué par les nouvelles technologies dans les activités terroristes et l'importance accordée aux technologies nouvelles et émergentes par les autorités nationales, régionales et internationales – aussi bien en ce qui concerne leur évaluation du risque terroriste que leur intégration des nouvelles technologies dans leur réponse – est la « course technologique » (*technological treadmill*) évoquée par le spécialiste du terrorisme Bruce Hoffman[10]. Compte tenu des risques et des avantages que présentent simultanément les nouvelles technologies, les terroristes et les acteurs de la lutte contre le terrorisme se sentent obligés d'innover et d'adopter en permanence de nouvelles technologies, sous peine d'être dépassés par leurs adversaires sur le plan technologique.

Cette pression peut être purement hypothétique, mais elle peut aussi se fonder sur des expériences du passé qui, s'agissant des acteurs de la lutte contre le terrorisme et les nouvelles technologies, ne sont pas nécessairement positives. À titre d'exemple, bon nombre des cadres politiques et opérationnels dans lesquels opèrent les professionnels de cette lutte, en particulier dans le contexte européen, ont été mis en place en réponse à la montée en puissance rapide du prétendu « État islamique en Irak et au Levant » (EIIL/Daech) et à l'exode, à partir des années 2012 et 2013, de combattants terroristes étrangers vers les zones de conflit au Moyen-Orient. Le détournement d'internet par les terroristes a souvent été au cœur de cette mobilisation, l'EIIL/Daech utilisant diverses plateformes et applications internet traditionnelles pour radicaliser et recruter des milliers d'individus[11] et occuper une place de premier plan à l'ordre du jour politique et médiatique mondial.

Le fait que les autorités n'aient pas su anticiper la maîtrise rapide du cyberespace par l'EIIL/Daech – mais surtout le temps nécessaire à la mise au point d'une réponse globale – peut expliquer la crainte légitime des professionnels de la lutte contre le terrorisme de sous-estimer les risques posés par l'utilisation à mauvais escient d'autres technologies émergentes par les terroristes. En juillet 2024, un cadre de Microsoft a bien résumé cet état d'esprit (qui s'applique également à divers autres contextes politiques), déclarant que le plus grand danger n'est pas tant que le monde en fasse trop pour résoudre ces problèmes, mais qu'il en fasse trop peu : non que les gouvernements agissent trop vite mais qu'ils soient trop lents à réagir[12].

L'essor de l'EIIL/Daech s'est également traduit par une augmentation rapide du nombre de pays et de régions touchés par le terrorisme, avec la création d'une organisation d'envergure mondiale ayant la capacité de mener des opérations extérieures et la possibilité d'établir de nouvelles synergies potentielles entre un groupe hétérogène de combattants terroristes étrangers[13] dans les zones de conflit. Dans le même temps, on observe une tendance de plus en plus marquée à l'internationalisation de la menace terroriste croissante d'extrême droite, avec notamment l'échange de tactiques et de techniques. Il est dès lors plus difficile pour les responsables politiques et les praticiens de partir du principe (ou d'espérer) que des tendances, problématiques ou modes opératoires particuliers se limiteront à des contextes nationaux ou régionaux spécifiques.

Par conséquent, l'émergence de nouvelles technologies susceptibles d'être utilisées à des fins terroristes, ou l'expérimentation de nouvelles technologies par des acteurs terroristes dans un pays ou une région donné ont souvent conduit les autorités nationales, régionales et internationales à consacrer des ressources considérables pour s'efforcer de comprendre dans quelle mesure ces exemples d'utilisation de la technologie par des terroristes sont réalistes ou reproductibles, et d'identifier des réponses potentielles.

10. Hoffman B., *Inside Terrorism*, Columbia University Press, New York, 2006, p. 252-253.
11. Barrett R. *et al.*, « Foreign fighters in Syria », The Soufan Center, New York, juin 2014.
12. Smith B., « Protecting the public from abusive AI-generated content », Microsoft, 30 juillet 2024.
13. D'après certaines estimations, des combattants terroristes étrangers originaires de plus de 110 pays ont rejoint les rangs de l'EIIL/Daech. Voir par exemple Barrett R., « Beyond the caliphate : foreign fighters and the threat of returnees », The Soufan Center, New York, octobre 2017.

Pourquoi les terroristes adoptent-ils les nouvelles technologies ?

Malgré ces craintes légitimes, l'adoption de nouvelles technologies par les acteurs terroristes continue de dépendre du contexte. En effet, le rythme auquel les terroristes procèdent et les types de technologies détournées varient nettement d'un pays ou d'une région à l'autre. Afin d'aider les États membres du Conseil de l'Europe à adopter une approche plus contextuelle et nuancée de l'évaluation des risques posés par les technologies nouvelles et émergentes, cette section tentera d'analyser la façon dont les terroristes innovent (en utilisant notamment de nouvelles technologies) et les raisons pour lesquelles ils le font, et d'identifier les facteurs qui ont déterminé le caractère limité, fragmentaire ou généralisé de l'adoption de technologies spécifiques. Deux études de cas illustrant la manière dont ce cadre analytique peut être appliqué dans la pratique concluront cette partie.

Aperçu de l'innovation dont font preuve les terroristes

Au cours des vingt dernières années, les scientifiques se sont penchés sur la meilleure façon d'appréhender et de catégoriser l'innovation terroriste. L'un d'entre eux, Adam Dolnik, s'est attaché à définir « l'innovation », qu'il a décrite comme « l'introduction d'une nouvelle méthode ou technologie ou l'amélioration d'une capacité déjà existante ». Cette définition peut englober à la fois l'innovation radicale (l'utilisation de tactiques ou de technologies totalement nouvelles) et l'innovation incrémentale (l'amélioration ou la modification d'une tactique)[14]. D'autres, dont Gill *et al.*[15], ont également insisté sur la distinction qu'il convient d'établir entre la créativité – c'est-à-dire l'identification de solutions à des problèmes – et l'innovation, qui est la mise en œuvre effective de ces stratégies. Cette distinction est essentielle car, si la créativité est un processus difficile en soi à encourager et à promouvoir (dans toute organisation ou tout mouvement), l'application des solutions identifiées au cours de ce processus peut souvent s'avérer encore plus complexe. C'est également la partie du processus que les opérations antiterroristes peuvent le plus facilement perturber.

D'autres spécialistes encore ont étudié les différents types d'innovation liés au terrorisme. Martha Crenshaw les a qualifiés de tactiques (adoption de nouvelles technologies pour atteindre des objectifs immuables), de stratégiques (identification de nouveaux objectifs) et d'organisationnels (structure organisationnelle ou processus de recrutement)[16]. Cette chercheuse a également fait valoir que l'objectif ultime de l'innovation terroriste est de maintenir l'effet de surprise, compte tenu de l'adaptation des acteurs étatiques aux actions des groupes terroristes. Cela est d'autant plus important que, selon certains experts, 90 % des organisations terroristes périclitent ou disparaissent au cours de leur première année d'existence[17] ; les 10 % restants doivent notamment leur survie à leur capacité d'adaptation, d'innovation et de créativité face aux puissances étatiques plus importantes qu'ils combattent[18].

14. Dolnik A., « Understanding terrorist innovation : technology, tactics and global trends », *Routledge Contemporary Terrorism Series*, Londres et New York, 2009.
15. Gill P. *et al.*, « Malevolent creativity in terrorist organisations », *The Journal of Creative Behaviour*, 4 juin 2013.
16. Crenshaw M., « Theories of terrorism : instrumental and organizational approaches », *Journal of Strategic Studies*, 24 janvier 2008.
17. Depuis l'affirmation largement reprise de David Rapoport en 1992, des études plus récentes ont examiné ces données et conclu que le chiffre réel se situait probablement autour de 50 %. Voir par exemple Phillips B. J., « Do 90 percent of terrorist groups last less than a year ? Updating the conventional wisdom », *Terrorism and Political Violence*, septembre 2017.
18. Gill P. *et al.*, « Malevolent creativity in terrorist organisations », *Journal of Creative Behaviour*, 2013.

L'adoption de nouvelles technologies n'est qu'un élément de cette approche de l'innovation. Les nouvelles technologies contribuent à l'innovation tant radicale qu'incrémentale au niveau tactique et ouvrent la voie à l'innovation stratégique et organisationnelle. Malgré le nombre important de recherches consacrées à la créativité et à l'innovation dont font preuve les terroristes (y compris au rôle de la technologie), l'accent a surtout été mis sur l'aspect tactique, et plus particulièrement sur les méthodes utilisées pour commettre les attentats. Depuis peu, l'importance d'autres innovations tactiques est de plus en plus reconnue[19], en particulier celles auxquelles ont recours les acteurs terroristes en réponse aux contre-mesures mises en œuvre par les autorités et le secteur privé sur les grandes plateformes de réseaux sociaux qui les ont souvent poussés à innover sur différentes plateformes en ligne de moindre envergure[20].

Étant donné le rôle avéré qu'a joué la technologie dans la réalisation, par les terroristes, de nouveaux objectifs organisationnels (par exemple l'utilisation par l'EIIL/Daech des réseaux sociaux et des applications cryptées pour recruter à l'échelle mondiale) et, dans une moindre mesure, stratégiques, il est essentiel de se pencher sur les facteurs qui sont des moteurs ou des freins à cette innovation. Dès lors, le présent rapport s'appuiera sur ces modèles pour créer un cadre qui contribuera à l'émergence d'une compréhension commune des raisons pour lesquelles les terroristes ont ou n'ont pas adopté diverses nouvelles technologies.

Pour commencer, il est utile d'examiner les différentes fonctions que doivent remplir les terroristes et les groupes terroristes pour opérer avec succès. Ces fonctions se résument globalement à trois domaines d'action :

- les ressources : ce domaine peut englober chaque aspect du cycle financier, à savoir la levée de fonds, leur circulation, leur stockage et leur dépense, y compris l'acquisition de l'équipement et du matériel nécessaires aux deuxième et troisième domaines d'action ;
- la communication : il s'agit à la fois de la communication interne (pour assurer la coordination et donner des instructions) et de la communication externe (à des fins de recrutement, de polarisation et de publicité) ;
- les attentats : cela va de la mise au point d'un projet et des opérations de reconnaissance à la conduite des attentats proprement dits, en passant par l'utilisation future de ces attaques à des fins de publicité ou de propagande.

Ces trois domaines d'action sont bien sûr étroitement liés. Ainsi, des groupes terroristes ont eu recours à des drones pour effectuer des reconnaissances et mener des attentats, mais aussi à des fins de propagande, ce qui leur a permis de collecter des fonds[21]. La communication externe post-attentat (par exemple la couverture médiatique de l'attaque et/ou la propagande associée) peut également orienter la levée de fonds ou le recrutement (de manière positive ou négative), et inspirer la commission d'attentats par des sympathisants ou des partisans. Ces chevauchements et interconnexions témoignent de la nécessité d'aborder l'utilisation de la technologie par les terroristes de manière globale, plutôt que de s'attacher à l'emploi d'une technologie spécifique dans un domaine d'action précis. Ils montrent aussi à quel point il peut être complexe de comprendre comment et pourquoi les terroristes adoptent une technologie particulière.

Facteurs internes de l'innovation terroriste

Les facteurs qui influent sur l'innovation terroriste peuvent être à la fois internes et externes, et présentent un niveau élevé d'interaction. On distingue de nombreux facteurs internes interconnectés, regroupés ici par souci de concision.

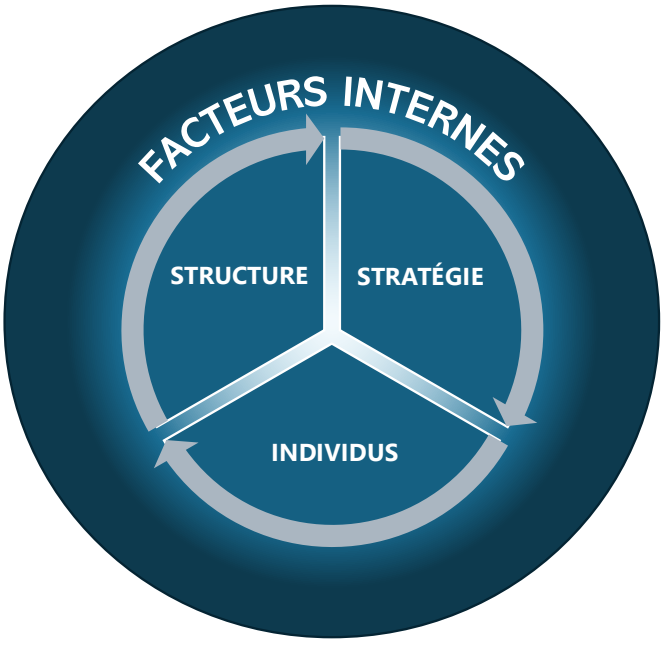
- **Les facteurs stratégiques :** ils comprennent la compatibilité générale entre les objectifs stratégiques ou les idéologies de l'organisation ou du mouvement et l'adoption d'une innovation particulière (y compris l'utilisation de la technologie). Un aspect essentiel de cette adéquation tient à l'équilibre ou à la hiérarchisation des différentes priorités, dont la rapidité, l'efficacité, le coût et la probabilité de détection. Les acteurs terroristes, en particulier, doivent mettre en balance la discrétion (pour éviter toute intervention/mesure préventive), d'une part, et la pertinence et l'impact (qui supposent de sacrifier la discrétion), d'autre part[22]. À titre d'exemple, après le 11 septembre 2001, Al-Qaida a généralement privilégié la discrétion dans son approche de nouvelles recrues potentielles et la prévention de toute intervention

19. Kfir I., « Terrorist innovation and online propaganda in the post-Caliphate period », Social Science Research Network, 4 novembre 2019.
20. Amarasingam A., Maher S. et Winter C., « How Telegram disruption impacts jihadist platform migration », Centre for Research and Evidence on Security Threats, 8 janvier 2021.
21. Direction exécutive du Comité contre le terrorisme (DECT) des Nations Unies, « Greater efforts needed to address the potential risks posed by terrorist use of unmanned aerial systems », mai 2019.
22. Kfir I., *op. cit.*

de l'État par le biais d'une procédure de vérification approfondie[23] au détriment de l'impact potentiel que pourrait avoir un nombre plus important de recrues. En revanche, à partir des années 2013-2014, l'EIIL/Daech a opté pour une plus grande ouverture aux nouvelles recrues (en personne et en ligne), au risque de compromettre la clandestinité de ses activités et de s'exposer davantage à la pénétration des services de renseignement, mais aussi de maximiser son champ d'action potentiel.

- **Les facteurs structurels :** ces choix stratégiques ont souvent une incidence sur le type de structure utilisé par un groupe ou un mouvement terroriste, ce qui, à son tour, influe sur la mesure dans laquelle et la manière dont il innovera. Il ressort des recherches menées que les groupes hiérarchiques et structurés ne font pas intrinsèquement preuve de créativité, les groupes salafistes-djihadistes étant souvent de nature conservatrice[24], mais qu'en même temps ils ont toujours privilégié l'innovation tactique dans leur méthodologie d'attaque (et ont même été à l'avant-garde dans ce domaine). En revanche, en ce qui concerne les mouvements terroristes moins structurés ou dépourvus de structure, en particulier ceux qui s'appuient sur des communautés en ligne plutôt que physiques (y compris le modèle de « résistance sans chef » de l'extrême droite), l'innovation peut être insufflée par la base, et les rendre ainsi plus réactifs aux changements opportunistes.
- **Les facteurs individuels :** indépendamment de la structure, un large éventail de facteurs individuels influe également sur l'innovation. Traditionnellement, les universitaires et les services de l'État se sont beaucoup intéressés au rôle des dirigeants au sein des organisations terroristes[25], notamment à leur attitude face au changement et à l'innovation, ainsi qu'à leur capacité à tirer des enseignements de leurs expériences passées et de celles des autres. Mais ces facteurs s'appliquent également aux acteurs terroristes isolés ainsi qu'à ceux liés à des mouvements aux contours plus flous. La créativité, le niveau d'expertise, le degré d'attachement à une technologie spécifique ou de confiance dans celle-ci et l'âge sont d'autres caractéristiques qui revêtent une importance particulière pour l'innovation dans le contexte technologique.

Figure 1 – Facteurs internes qui influent sur l'innovation terroriste



23. Joscelyn T., « Spying on al Qaeda », *Long War Journal*, 10 mai 2012.
24. Winter C., Maher S., Jawad al-Tamimi A., « Understanding Salafi-Jihadist attitudes towards innovation », Centre international d'études sur la radicalisation, 19 janvier 2021.
25. Long A., « Assessing the success of leadership targeting », *CTC Sentinel*, novembre 2010.

Facteurs externes de l'innovation terroriste

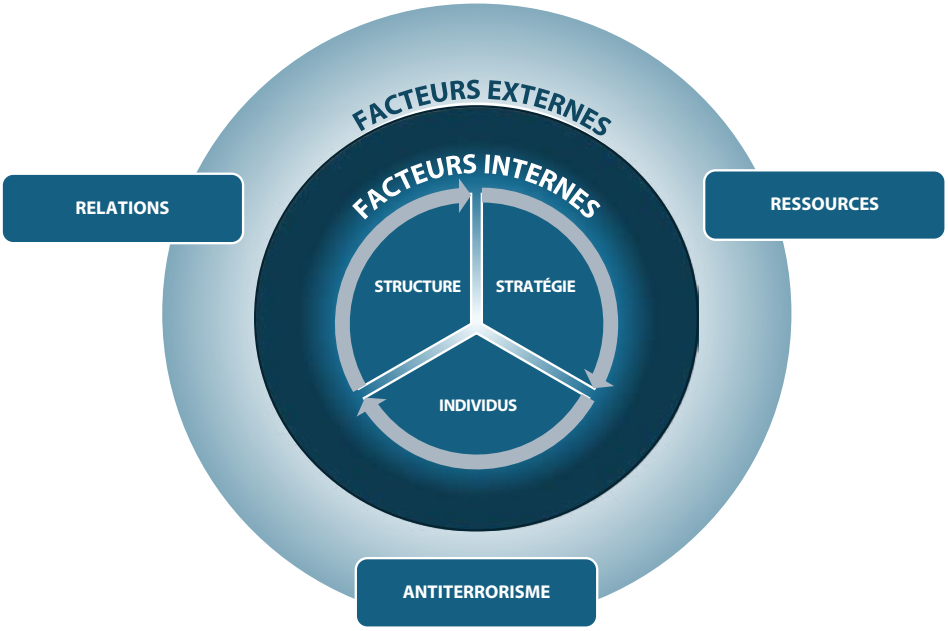
Ces facteurs internes sont bien sûr étroitement liés et recoupent divers facteurs externes, dont ceux qui suivent.

- **Les relations** : les relations entretenues par différents acteurs terroristes ont toujours été un moteur à l'innovation au service de leur cause car elles favorisent le partage de technologies, de techniques et de connaissances des mesures antiterroristes. Ce type de relation directe a été illustré par le déplacement en Colombie, effectué en 2001 par trois membres présumés de l'Armée républicaine irlandaise (IRA), qui ont ensuite été déclarés coupables d'avoir formé les Forces armées révolutionnaires de Colombie (FARC) au maniement des explosifs[26]. Plus récemment, internet a facilité l'accès à ce type d'informations sans nécessiter (ou risquer) l'établissement d'une relation directe entre différents acteurs terroristes. Ainsi, il est désormais possible d'accéder à du matériel d'instruction[27], sur le web de surface et le *dark web* (en particulier en ce qui concerne la fabrication d'engins explosifs improvisés), mais aussi à des enseignements plus généraux tirés des succès et échecs d'autres opérations terroristes, et notamment de comprendre pourquoi et comment des projets d'attentats ont pu être repérés et déjoués. Cet aspect est particulièrement important dans le contexte des attaques commises par des acteurs isolés, qui se caractérisent souvent par l'absence de liens directs, personnels et opérationnels entre l'assaillant et d'autres membres du mouvement. Enfin, les relations entre les groupes terroristes et les autorités peuvent également être un facteur clé d'innovation car elles permettent le partage de technologies, mais aussi de connaissances et d'autres ressources. Les recherches concernant l'utilisation de drones par des groupes armés non étatiques ont particulièrement mis en évidence cet élément, et montré que la plupart des groupes qui ont utilisé de tels équipements avec succès ont des liens avec des acteurs étatiques[28].
- **Les ressources :** une large gamme de ressources influe sur l'innovation terroriste fondée sur les nouvelles technologies. L'argent est la ressource la plus critique, dans la mesure où elle conditionne d'autres éléments essentiels à l'innovation terroriste, comme l'acquisition de matériel, mais aussi le recrutement et le versement des salaires aux membres du groupe terroriste. Toutefois, l'accès à des fonds ne garantit pas à lui seul l'accès aux ressources indispensables à la réussite de l'innovation avec les nouvelles technologies, compte tenu notamment du niveau et du type d'expertise qui peuvent s'avérer nécessaires. Ainsi, la stratégie de longue haleine mais finalement infructueuse d'Al-Qaida pour mener des attaques terroristes chimiques, biologiques, radiologiques ou nucléaires (CBRN), qui s'est traduite par le recrutement de scientifiques, la construction de laboratoires et des tentatives avortées de production ou d'acquisition de matériaux CBRN dans différents pays, en est un bon exemple[29]. Cette question plus générale de l'accessibilité d'une technologie particulière et de l'expertise technique nécessaire à son adoption a été présentée par les scientifiques comme un facteur clé dans la manière dont les terroristes abordent l'innovation technologique, en particulier en ce qui concerne sa complexité et son coût relatifs[30].
- **La lutte contre le terrorisme :** enfin, et c'est peut-être le point le plus important, toute innovation terroriste s'inscrit dans le prolongement des mesures nationales, régionales ou internationales antiterroristes et de prévention ou de lutte contre l'extrémisme violent, qui varient toutes en termes d'approches adoptées et d'efficacité. Les terroristes qui évoluent dans des environnements opérationnels permissifs disposent d'une plus grande liberté d'innovation que ceux qui sont confrontés à des acteurs efficaces de la lutte antiterroriste. Dans le même temps, ils ont souvent moins besoin d'innover, compte tenu de leur facilité d'accès à des armes et des explosifs, et de leur capacité à se procurer, à stocker et à faire circuler des fonds sans entrave. L'environnement de la lutte contre le terrorisme peut également influer sur le choix des cibles visées par les attentats, le renforcement de la prévention situationnelle pouvant avoir pour effet d'orienter les terroristes vers des cibles plus faciles, ne nécessitant que des méthodes simples et peu technologiques. Ainsi, malgré le durcissement progressif des mesures de sécurité dans les aéroports du monde entier en réponse aux attentats et aux projets terroristes, ces infrastructures demeurent une cible récurrente, mais les terroristes se concentrent désormais sur les zones non sécurisées[31].

26. Taylor, L., « Colombia revokes amnesty it granted to alleged IRA bomb-making trio », *The Guardian*, 16 décembre 2022.
27. Europol, « Crackdown on material designed to 'educate' future terrorists », 21 décembre 2023.
28. Voir par exemple Rassler, D., « Going the distance : the emergence of long-range stand-off terrorism », *CTC Sentinel*, février 2024.
29. Mowatt-Larssen, R., « Al Qaeda's pursuit of weapons of mass destruction », *Foreign Policy*, 25 janvier 2010.
30. Veilleux-Lepage Y., Damon C. et Archambault E., « Learning from foes : how racially and ethnically motivated violent extremists embrace and mimic Islamic State's use of emerging technologies », Réseau mondial sur l'extrémisme et la technologie (GNET), 7 juin 2022.
31. Voir par exemple les attentats commis en 2016 dans les aéroports de Bruxelles et d'Istanbul, qui visaient les passagers en attente de passer les contrôles de sécurité et ceux situés à l'extérieur des terminaux.

La perturbation d'activités et les poursuites menées avec succès par les services antiterroristes peuvent également permettre aux acteurs terroristes de se familiariser avec les techniques d'enquête utilisées par les autorités pour détecter et déjouer leurs projets d'attentats, ce qui les incite à innover davantage pour s'y soustraire. Cette efficacité des mesures antiterroristes peut être liée aux vulnérabilités des technologies existantes employées par les acteurs terroristes (par exemple certains systèmes ou plateformes de communication accessibles aux services de renseignement et aux services répressifs) ou à des vulnérabilités plus générales liées à leur mode opératoire, et susceptibles d'être corrigées par l'utilisation de nouvelles technologies (par exemple le recours au cryptage[32] ou aux applications de cartographie hors ligne pour éviter d'être suivi par les forces de l'ordre). Il est bien entendu très difficile de prouver qu'une stratégie ou une mesure antiterroriste particulière est la cause directe d'une innovation terroriste spécifique (ou même qu'une telle mesure a permis d'éviter un passage à l'acte). Cependant, force est de constater que les actions antiterroristes suscitent des réactions, positives ou négatives, de la part des terroristes, notamment en termes d'innovation et d'utilisation de nouvelles technologies.

Figure 2 – Facteurs internes et externes ayant une incidence sur l'innovation terroriste



32. Mascellino A., « End-to-end encryption sparks concerns among EU law enforcement », *Infosecurity Magazine*, 23 avril 2024.

Adoption des nouvelles technologies par les terroristes : études de cas

Pour mieux comprendre l'impact de ces différents facteurs sur l'exploitation des nouvelles technologies par les terroristes, le présent document analysera deux études de cas illustrant l'adoption à plus ou moins grande échelle, et à des rythmes différents, de nouvelles technologies présentant des avantages manifestes pour les acteurs terroristes.

Étude de cas n° 1 : l'utilisation à mauvais escient des systèmes autonomes sans pilote (drones)

Des inquiétudes quant aux possibilités d'utilisation malveillante de systèmes autonomes sans pilote par des acteurs terroristes en Europe ont vu le jour depuis que l'EIIL/Daech est parvenu à armer des drones en Irak et en Syrie en 2016 et 2017, en combinant des engins disponibles dans le commerce, des composants de faible technicité et d'autres accessoires technologiques[33]. Au plus fort de son activité, le programme de drones de l'EIIL/Daech aurait été à l'origine de plus d'une centaine d'attentats en Irak en un mois[34], ce qui a amené des responsables de l'Union européenne (UE) à mettre en garde à plusieurs reprises contre les risques d'utilisation de ce type d'engins pour mener des attaques sur des villes européennes[35]. Bien que la technologie des drones soit de plus en plus accessible et abordable, et que la propagande terroriste fasse souvent référence à son recours pour cibler l'Europe (notamment lors des jeux Olympiques de Paris de 2024)[36], les acteurs terroristes n'ont pas encore adopté les systèmes autonomes sans pilote en Europe ou pour cibler l'Europe. Plusieurs facteurs internes et externes permettent d'en expliquer les raisons (à ce jour). Il convient de noter que la Türkiye a également été témoin de l'utilisation de parapentes/paramoteurs par des acteurs terroristes lors de l'attaque contre le commissariat de police de Tece dans le district de Mezitli de la province de Mersin à l'automne 2024. Bien qu'ils diffèrent à bien des égards des drones, ils représentent un autre vecteur d'attaque aérienne que les acteurs terroristes pourraient chercher à exploiter à l'avenir, compte tenu de leur coût relativement faible et de leur facilité d'obtention et d'assemblage.

Facteurs internes

Du point de vue du risque stratégique, les drones restent moins prisés que d'autres méthodes d'attaque, notamment en raison de leur rapport coût-efficacité (compte tenu des difficultés considérables à les armer de manière fiable) et de la crainte que l'achat de drones ou de composants connexes ou la réalisation de vols d'entraînement n'éveillent l'attention des autorités. Sur le plan structurel, les groupes hiérarchiques sont davantage enclins à favoriser l'innovation à long terme dans les méthodes d'attaque, alors que ce sont des acteurs isolés et de petites cellules, généralement dépourvus de cette structure formelle, qui dominent le contexte actuel de la menace en Europe. En effet, un spécialiste de la lutte antiterroriste d'un État membre du Conseil de l'Europe a récemment déclaré que les groupes terroristes dotés de programmes de drones constituaient sa plus grande préoccupation car ils disposent de ressources, d'une expertise et de fonds dédiés, et bénéficient de réseaux qui leur facilitent l'accès à des composants ou à de tels engins vendus dans le commerce[37]. Cependant, certains facteurs individuels laissent présager une possible adoption des systèmes autonomes sans pilote à l'avenir, le paysage terroriste européen étant généralement dominé par des jeunes susceptibles d'avoir une bonne maîtrise des technologies et d'être déjà familiarisés avec celle des drones.

33. Rassler D., « The Islamic State and drones : supply, scale and future threats », Combatting Terrorism Center at West Point, juillet 2018.
34. Sullivan B., « The Islamic State conducted hundreds of drone strikes in less than a month », *Vice*, 21 février 2017.
35. Martin N., « EU : terrorists could use drones for attacks », *Deutsche Welle*, 8 mars 2019.
36. Courtney-Guy S., « ISIS warns of Eiffel Tower drone attack in chilling Paris Olympics threat », *Metro*, 10 juin 2024.
37. Cité dans UNOCT AROS Programme & Conflict Armament Research, « Global report on the acquisition, weaponization and deployment of unmanned aircraft systems by non-State armed groups for terrorism-related purposes », mars 2024.

Facteurs externes

En ce qui concerne les facteurs externes, les acteurs terroristes établis en Europe (ou qui ciblent ce continent) ont maintes occasions de tirer indirectement des enseignements de l'expérience d'autres acteurs non étatiques qui sont parvenus à armer des drones. Pour l'heure, les éléments attestant de l'existence de relations directes entre des acteurs terroristes établis en Europe et des groupes ou des individus possédant ce type d'expertise essentielle pour accélérer l'armement des drones en Europe semblent très limités. Cependant, des inquiétudes légitimes ont été exprimées quant à la propagation de méthodes et de technologies depuis les zones de conflit actuelles[38]. Bien que les compétences et le savoir-faire relatifs à l'utilisation des drones et les contre-mesures visant à empêcher leur détournement soient probablement déjà disponibles, les ressources peuvent être un frein à l'adoption de cette technologie, étant donné son coût relatif par rapport aux méthodes couramment utilisées aujourd'hui dans les attaques autofinancées.

Enfin, la mise en place en Europe d'approches antiterroristes globales et dans l'ensemble efficaces a rendu l'environnement opérationnel difficile pour les groupes ou les individus qui cherchent à innover en recourant à l'armement de drones. Ainsi, l'utilisation de drones à proximité d'infrastructures critiques et en particulier en milieu urbain fait déjà l'objet de restrictions, et des initiatives de partage d'informations ont été lancées à l'échelle de l'UE, tandis que différents moyens technologiques de contrer les menaces que représentent les drones sont actuellement à l'essai[39]. Si l'efficacité concrète de certaines de ces mesures et des activités programmatiques et politiques visant à relever ces défis[40] suscite des interrogations, celles-ci peuvent avoir influé sur la vision qu'ont les acteurs terroristes de la probabilité d'une détection précoce et d'une perturbation de leurs activités faisant appel à l'utilisation de drones.

De toute évidence, ces facteurs internes et externes, ainsi que les calculs stratégiques plus larges des acteurs terroristes en Europe, sont appelés à évoluer. La baisse du coût des drones, la disponibilité accrue de matériel didactique quant à leur armement fiable, la multiplication de la propagande terroriste encourageant leur utilisation dans l'environnement européen ou les attaques de drones très médiatisées dans d'autres contextes sont autant d'éléments susceptibles d'induire des changements. Toutefois, le cadre susmentionné s'avère utile pour évaluer la probabilité d'un recours aux drones (ou à d'autres technologies) par les acteurs terroristes ainsi que pour identifier les obstacles à leur adoption qui peuvent être surveillés afin de déterminer les risques et les défis à venir.

Étude de cas n° 2 : les actifs virtuels

Depuis la création du bitcoin en 2009, les cryptomonnaies et autres actifs virtuels ont été massivement utilisés par divers acteurs criminels, en raison du niveau d'anonymat qu'ils semblent offrir et de l'absence initiale d'obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) destinées à attirer l'attention des autorités gouvernementales sur les transactions suspectes. Compte tenu de ces avantages opérationnels manifestes, et de la nature transnationale de nombreux mouvements terroristes qui impliquent la circulation de fonds à l'échelle internationale, la coalition de lutte contre le terrorisme redoute depuis longtemps une adoption rapide des actifs virtuels par les terroristes. Ainsi, dès 2014[41], le Canada a pris des mesures pour parer aux risques de BC/FT associés aux monnaies virtuelles.

Ces dix dernières années ont été marquées par une légère augmentation progressive de la présence d'actifs virtuels dans les enquêtes antiterroristes, en particulier depuis trois ou quatre ans. Ce phénomène n'a toutefois pas eu le type d'impact envisagé notamment par la marine américaine en 2014, qui estimait que l'introduction des monnaies virtuelles façonnerait probablement le financement de la menace en renforçant l'opacité, la rapidité des transactions et l'efficacité globale des attaques terroristes[42].

Facteurs internes

Bien que les actifs virtuels semblent généralement adaptés aux objectifs stratégiques et aux idéologies de la plupart des acteurs terroristes opérant en Europe, leur efficacité reste sujette à caution. Cela tient à leur volatilité, c'est-à-dire à la variation rapide et régulière de leur valeur (en particulier pour les monnaies qui

38. Bell S., « West must adapt as drones become weapon of choice for military 'underdogs' and terror groups », *Sky News*, 3 février 2024.
39. Commission européenne, Communication de la Commission au Conseil et au Parlement européen relative à la lutte contre les menaces potentielles posées par les drones, 18 octobre 2023.
40. Unmanned Airspace, « European Commission announces funding for the EUR 71 million E-CUAS programme », 17 mai 2024.
41. Canadian Broadcasting Company, « Budget 2014 : bitcoin, charities face scrutiny to prevent money laundering », *Yahoo News*, 12 février 2014.
42. Cohen B., « US Navy Preparing Bitcoin Battalion », *Bitcoin Magazine*, 24 avril 2014.

privilégient l'anonymat grâce à un « grand livre » privé)[43], mais aussi aux difficultés rencontrées par certaines juridictions pour convertir les actifs virtuels en monnaie fiduciaire et à la capacité avérée des acteurs publics et privés de suivre à la trace les transactions afin de remonter jusqu'aux utilisateurs. D'un point de vue structurel, le paysage terroriste en Europe semble également propice à l'adoption d'actifs virtuels, l'absence de groupes hiérarchiques bien établis encourageant une approche insufflée par la base et émanant d'individus agissant seuls. Cependant, un pourcentage non négligeable d'attaques terroristes en Europe relève de l'initiative d'acteurs isolés, et ces dernières sont donc autofinancées[44], en faisant appel à des méthodes éprouvées telles que les structures commerciales légales, la collecte de dons, les cotisations de membres et les activités criminelles[45]. En revanche, la majeure partie des opérations identifiées à ce jour dans lesquelles les actifs virtuels jouent un rôle important (et, de fait, la plupart des individus ont été arrêtés en 2022 pour financement d'activités terroristes) ont une dimension extérieure, les fonds étant transférés à des organisations terroristes établies hors de l'Union européenne et ne servant pas à financer des activités ou des attentats ciblant l'Europe[46].

Ainsi, cette évolution progressive vers l'utilisation d'actifs virtuels a été essentiellement motivée par des facteurs externes (à savoir la volonté d'innover manifestée par des acteurs terroristes externes), principalement après que des groupes terroristes comme l'EIIL/Daech et ses affiliés ont fait part de leur intérêt et de leur capacité à recevoir des fonds en cryptomonnaies. Enfin, en raison de leur jeunesse, de leur bonne maîtrise de la technologie et de la généralisation croissante de toute une gamme d'actifs virtuels, il est probable que les acteurs terroristes aient été exposés à l'utilisation (et aux avantages/inconvénients) de ces derniers dans la vie de tous les jours ; d'où la difficulté à déterminer si la présence d'actifs virtuels découverte lors d'enquêtes antiterroristes est due à leur utilisation à des fins terroristes, ou simplement parce que les acteurs terroristes ont recours à ce type d'actifs dans le cadre d'activités non liées au terrorisme.

Facteurs externes

Compte tenu de la généralisation des actifs virtuels et de leur utilisation durable par une multitude d'acteurs criminels, un large éventail de sources et de relations directes ou indirectes peut favoriser l'innovation parmi les acteurs terroristes. Du fait de l'adoption relativement limitée de ces moyens par les acteurs terroristes, et de la grande diversité des normes et des approches selon les actifs virtuels et les transactions concernés, les acteurs terroristes ne disposent peut-être pas d'une « bonne pratique » évidente qu'ils pourraient suivre, de sorte qu'ils auront probablement des approches divergentes vis-à-vis des actifs virtuels. Les ressources semblent constituer un facteur moins déterminant pour les acteurs terroristes établis en Europe, la barrière d'entrée sur le marché des actifs virtuels étant nettement plus basse que par le passé (en termes de savoir-faire technique). Cependant, le problème est plus important pour les acteurs terroristes qui pourraient être destinataires d'actifs virtuels provenant de personnes situées en Europe, en raison des difficultés liées aux procédures d'échanges, à la fluctuation des devises (tant virtuelles que « physiques ») et à la conversion de cryptoactifs en monnaie fiduciaire[47], l'infrastructure mondiale connexe étant encore relativement instable.

Enfin, les actions de lutte contre le terrorisme restent un frein important à l'utilisation des actifs virtuels, étant donné l'issue positive des poursuites engagées dans ce domaine (et d'autres poursuites pénales) dans de nombreuses juridictions, qui démontre la traçabilité de bon nombre desdits actifs, et la possibilité de remonter jusqu'à l'utilisateur final des transactions malveillantes. En effet, selon un rapport établi en juin 2023 par le Groupe Egmont de cellules de renseignement financier (CRF), un groupe terroriste a cessé de recourir aux actifs virtuels pour collecter des fonds à la suite d'actions fructueuses menées par les pouvoirs publics pour identifier et poursuivre les donateurs[48].

Outre ces facteurs internes et externes spécifiques, le contexte général dans lequel opèrent les acteurs terroristes en Europe depuis cinq à six ans contribue à expliquer leur adoption relativement limitée des actifs virtuels. La prédominance d'un terrorisme d'acteurs isolés ou de petites cellules de nature essentiellement interne est due à la fois à la défaite territoriale de l'EIIL/Daech (l'organisation terroriste extérieure auparavant dominante qui recrutait et mobilisait des acteurs terroristes européens) et à la montée d'une menace terroriste d'extrême droite qui privilégie le modèle de « résistance sans chef ». Les tendances récentes qui indiquent que

43. Alexander A. et MacDonald T., « Examining Digital Currency Usage by Terrorists in Syria », *CTC Sentinel*, mars 2022.
44. Reimer S. et Redhead M., « A new normal : countering the financing of self-activating terrorism in Europe », RUSI Europe, mai 2021.
45. Europol, « European Union terrorism situation and trend report », Office des publications de l'Union européenne, Luxembourg,octobre 2023.
46. *Ibid*.
47. Alexander A. et MacDonald T., « Examining digital currency usage by terrorists in Syria », *CTC Sentinel*, mars 2022.
48. Groupe Egmont de cellules de renseignement financier, groupe de travail Échange d'informations, « Report on abuse of virtual assets for terrorist financing purposes », juin 2023.

les groupes ou les conflits extérieurs jouent un rôle de plus en plus important dans la menace terroriste, dont plusieurs projets d'attentats en Europe liés à l'État islamique – Province de Khorassan (EIPK)[49], laissent présager une évolution de la situation, avec la possibilité d'acheminer des fonds aussi bien vers que depuis l'Europe (au moyen de méthodes conventionnelles ou virtuelles), notamment pour soutenir des attaques plus ciblées.

49. Clarke C. P. et Webber L., « ISKP goes global : the world is not ready to confront a new international terror threat », *Foreign Affairs*, 1er août 2024.

Impact des nouvelles technologies sur le paysage terroriste actuel en Europe (et sur l'Europe)

Après avoir analysé la façon dont les terroristes innovent en utilisant la technologie sur un plan général – et deux études de cas examinant ce processus dans la pratique – il est important de comprendre comment ces différents facteurs, et leur interaction, ont influé sur le paysage terroriste que connaît l'Europe (et dont elle subit l'impact). Étant donné les dangers d'une généralisation de la situation entre différents pays confrontés à divers types de menaces et cherchent à y répondre avec des ressources et des approches variables, ce chapitre s'efforcera d'être aussi précis et concis que possible, notamment en présentant des exemples ou des études de cas fondés sur divers contextes nationaux. Il dégagera toutefois certaines tendances régionales plus larges afin de permettre de mieux comprendre l'état actuel de la menace.

Communication terroriste et radicalisation

Partage de contenus terroristes

Bien que les moteurs de la radicalisation vers le terrorisme restent complexes et touchent les individus dans leur vie aussi bien en ligne qu'hors ligne, l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) a fait valoir que l'utilisation de la technologie et d'internet (y compris les plateformes de réseaux sociaux, les applications de messagerie instantanée, les forums en ligne et les plateformes de jeux vidéo) continue de jouer un rôle crucial dans le processus de radicalisation et de recrutement des individus et dans la diffusion de matériel de propagande[50].

Dans le contexte européen, si les modalités de stockage et de diffusion de la propagande terroriste varient en fonction de l'idéologie du groupe ou du mouvement qui en est à l'origine, certains points communs essentiels subsistent en ce qui concerne les types de nouvelles technologies exploitées et les méthodes utilisées à cette fin. Il s'agit notamment de technologies et de méthodes relativement bien établies. En particulier, les terroristes et les extrémistes violents cherchent toujours à tirer parti des principales plateformes de réseaux sociaux, car elles leur permettent de diffuser leur propagande auprès d'un public aussi large que possible et leur offrent les meilleures chances d'atteindre la « viralité ».

Toutefois, grâce aux efforts conjoints des pouvoirs publics, de la société civile et des plateformes elles-mêmes, les terroristes ont désormais plus de mal à essaimer sur ces grandes plateformes. Par exemple, le règlement de l'Union européenne relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne exige des fournisseurs de services d'hébergement qu'ils retirent les contenus à caractère terroriste dans un délai d'une heure une fois qu'ils ont été alertés par une autorité compétente[51], les sanctions en cas de non-respect pouvant atteindre jusqu'à 4 % du chiffre d'affaires (pour l'exercice précédent) de la plateforme concernée. Ce dispositif est appuyé par l'unité de signalement des contenus sur internet d'Europol, qui organise trimestriellement des « journées d'action de signalement » afin d'identifier les contenus à caractère terroriste diffusés en ligne, puis de renvoyer les URL qui y sont associées aux fournisseurs de services en ligne pour qu'ils les suppriment[52].

50. Europol, « European Union terrorism situation and trend report 2023 », Offices des publications de l'Union européenne, Luxembourg, octobre 2023.
51. Pour plus d'informations, voir le Règlement (UE) 2021/784 du Parlement européen et du Conseil relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne », adopté le 29 avril 2021.
52. Voir par exemple Europol, « Crackdown on material designed to 'educate' future terrorists », 21 décembre 2023.

De leur côté, de nombreuses plateformes s'emploient à détecter et à supprimer de manière proactive les contenus qui ne respectent pas leurs propres conditions générales d'utilisation, y compris les contenus à caractère terroriste. Trente-deux entreprises du secteur des technologies sont aujourd'hui membres du GIFCT[53], qui leur donne accès (et leur permet de contribuer) à une base de données de partage de hachages. Celle-ci contient l'« empreinte numérique » unique de chaque contenu terroriste repéré par le GIFCT et ses membres, ce qui permet à ces derniers de supprimer le contenu en question ou d'empêcher son téléchargement sur leur plateforme. Grâce à cette base de données, et à diverses autres techniques d'apprentissage automatique utilisées par différentes plateformes[54], il est désormais difficile de publier des contenus terroristes avérés sur la plupart des grandes plateformes. Ainsi, sur les millions de messages à caractère terroriste supprimés par Facebook, environ 98 % ont été détectés de manière proactive par la plateforme[55].

Ces facteurs externes (c'est-à-dire les efforts de lutte contre le terrorisme) ont sans nul doute fortement influé sur la propension des acteurs terroristes à innover en utilisant de nouvelles technologies dans le cadre de leurs activités de radicalisation et de recrutement. De ce fait, les terroristes ont désormais recours à une gamme de plus en plus diversifiée de plateformes et d'applications pour créer, stocker et partager des contenus à caractère terroriste. Tech against Terrorism a repéré de tels contenus sur 187 plateformes en ligne différentes entre novembre 2020 et janvier 2023, 78 d'entre elles étant de petits fournisseurs de services d'hébergement ou des microplateformes[56].

Les petites plateformes disposent généralement de ressources plus limitées pour modérer les contenus de toute nature (et sont parfois opposées au concept de modération des contenus). De plus, elles sont moins susceptibles d'avoir établi des relations de travail avec les services répressifs. Cette situation peut, là encore, être liée à des problèmes de ressources, au caractère inédit ou limité de l'activité terroriste sur la plateforme, à la juridiction compétente en matière d'hébergement et de gestion de la plateforme, ou encore aux inclinations idéologiques de ses propriétaires. C'est ainsi que des acteurs terroristes ont été en mesure de maintenir leur présence en ligne, même si elle s'adresse à un public plus restreint.

Ces petites plateformes posent certes des problèmes notables, notamment en ce qui concerne le partage de fichiers et le stockage de contenus. Cependant, subsiste un écosystème d'applications et de plateformes en ligne plus importantes qui sont détournées depuis un certain temps par les acteurs terroristes, et dont les mesures de modération des contenus et les relations avec les forces de l'ordre n'ont pas suffi à dissuader leur utilisation à des fins terroristes. L'exemple le plus notoire est Telegram, qui a été largement utilisé par les acteurs terroristes de diverses convictions idéologiques durant ces dix dernières années[57]. Avec plus de 900 millions d'utilisateurs et utilisatrices mensuels, Telegram est l'un des dix réseaux sociaux les plus populaires au monde[58]. Plus récemment, X (anciennement Twitter) a assoupli ses règles de modération des contenus, a autorisé des types de contenus auparavant interdits sur la plateforme (et dans certains cas les promeut), et a rétabli des comptes d'extrême droite précédemment supprimés de Twitter pour incitation à la violence[59]. Par conséquent, X est à nouveau un refuge pour les terroristes et extrémistes violents de tout le spectre idéologique.

Parallèlement à l'utilisation de plateformes ou d'applications hébergées par d'autres entreprises, certains terroristes ont également développé leurs propres sites internet pour héberger des contenus à caractère terroriste. Sur une période de deux ans, Tech against Terrorism a recensé près de 300 sites exploités par des terroristes ou des extrémistes violents. Ces sites offrent un espace stable et accessible pour héberger du matériel de propagande, recruter de nouveaux membres et lever des fonds[60], et sont également utilisés pour proposer des contenus didactiques qui enfreindraient les conditions générales d'utilisation de la plupart des plateformes en ligne.

Europol s'est attelé à la menace que représentent les sites internet gérés par des terroristes, dans le cadre d'une enquête conjointe qui a conduit, en juin 2024, à la saisie de quatre serveurs en Roumanie, Ukraine et Islande, et au signalement de 13 sites à leurs fournisseurs de services en vue de leur suppression[61]. Les services répressifs nationaux ont également ciblé les personnes agissant en qualité d'administrateurs des sites web. Ainsi, un Britannique responsable de la gestion de deux sites d'extrême droite (mais pas de la création des

53. Pour une liste complète des membres, voir le site internet du GIFCT (consulté le 7 août 2024).
54. Macdonald S, Mattheis A. et Wells D., « Utiliser l'intelligence artificielle et l'apprentissage automatique pour identifier les contenus terroristes en ligne », Tech Against Terrorism Europe, 17 janvier 2024.
55. *Ibid*.
56. « Patterns of online terrorist exploitation : TCAP insights », Tech against Terrorism, avril 2023.
57. Tan R., « Terrorists love for Telegram, explained », *Vox*, 30 juin 2017.
58. Dean B., « How many people use Telegram? » *Backlinko*, 17 juillet 2024.
59. Ingram D., « Verified pro-Nazi X accounts flourish under Elon Musk », *NBC News*, 16 avril 2024.
60. « Terrorist operated websites : explainer », Tech against Terrorism (consulté le 7 août 2024).
61. Europol, « Europol-coordinated operation tackles the threat of terrorist-operated websites », 14 juin 2024.

contenus hébergés) a été condamné à sept ans de prison au début du mois d'août 2024 pour quatre chefs d'accusation de diffusion de publications à caractère terroriste[62].

Plateformes de jeux et plateformes connexes

Les plateformes de jeux et les plateformes connexes constituent un autre écosystème en ligne de plus en plus préoccupant en termes de recrutement et de radicalisation. Ce virage manifeste vers des espaces en ligne différents semble avoir été motivé par des facteurs internes, en particulier la nature non hiérarchique de l'écosystème terroriste en Europe et sa relative jeunesse, ainsi que par les pressions exercées par les acteurs de la lutte contre le terrorisme évoquées précédemment. Un autre facteur externe joue un rôle dans l'apprentissage des terroristes : l'influence des relations indirectes, en particulier la diffusion en temps réel, très médiatisée, des attaques terroristes de Christchurch et de Buffalo, s'inspirant du visuel des jeux vidéo de tir à la première personne[63].

Le terrorisme peut interférer ou interagir de diverses manières avec l'univers des jeux[64]. Il s'agit aussi bien des jeux grand public, qui ont généralement une composante en ligne permettant la communication entre pairs ou de groupe, que des communautés ou canaux de jeux en ligne qui permettent aux joueurs et joueuses de diffuser en direct leurs activités et de discuter avec leurs contacts et une communauté plus large (notamment Steam, Twitch, DLive et Discord). Bien qu'à l'origine ces applications aient été développées à des fins purement ludiques, elles ont évolué et se rapprochent davantage des réseaux sociaux traditionnels ou des plateformes de commerce électronique dont elles reprennent certaines fonctionnalités[65], sans pour autant disposer des mêmes capacités de modération des contenus ou entretenir les mêmes relations avec les services répressifs.

Les craintes liées à ces vulnérabilités possibles ont été renforcées par l'utilisation répétée de l'imagerie ou de la terminologie des jeux dans la propagande terroriste[66] (notamment par l'EIIL/Daech) – qui laisse penser que les groupes ou mouvements terroristes ont pris conscience de l'affinité entre leur public potentiel et le monde du jeu en ligne – ainsi que par la ludification des activités terroristes proprement dites, en particulier au sein de la communauté d'extrême droite[67]. Les acteurs extrémistes violents ont également développé leurs propres jeux vidéo ou personnalisé certains niveaux de jeux existants, afin notamment d'offrir à leurs adeptes la possibilité de reproduire d'anciennes attaques terroristes[68].

En 2021, Europol a qualifié de « tendance croissante »[69] la prévalence de la propagande d'extrême droite sur les plateformes, les forums et les chaînes de jeux, et d'autres services répressifs (tant en Europe qu'au-delà)[70] ont souvent aussi fait état de ce risque, en particulier dans le contexte de l'exposition des enfants à des contenus à caractère terroriste. Malgré ces fragilités potentielles, l'intérêt manifeste que portent les acteurs terroristes à l'écosystème des jeux et la reconnaissance massive du nombre important d'attitudes et de comportements haineux et violents sur les plateformes de jeux[71], on compte relativement peu d'exemples concrets et opérationnels d'utilisation de plateformes de jeux ou de plateformes connexes pour mener des actions de radicalisation et de recrutement. Cependant, le sujet demeure extrêmement préoccupant, compte tenu des données constantes montrant que les enfants sont la cible de groupes terroristes de différentes idéologies dans toute l'Europe, et de la popularité actuelle des plateformes de jeux ou connexes auprès de cette tranche d'âge.

62. Ministère public britannique (Crown Prosecution Service), « Far-right extremist jailed for running racist websites used by international terrorists », 2 août 2024.
63. Schlegel L. et Amarasingam A., « Examining the intersection between gaming and violent extremism », Bureau de lutte contre le terrorisme des Nations Unies, 6 octobre 2022.
64. Pour un aperçu de certaines de ces préoccupations et des nouvelles réponses qui y sont apportées, voir Comité du Conseil de l'Europe de lutte contre le terrorisme, « Conference summary : the abuse of livestreaming, gaming and virtual reality services and platforms by terrorist actors », novembre 2023.
65. Lakhani S., « Video gaming and (violent) extremism : an exploration of the current landscape, trends and threats », Réseau européen de sensibilisation à la radicalisation (RSR), 1er octobre 2021.
66. Dass R. et Singh J., « How IS exploits gamification of violence in bid to appeal to youths online during the pandemic », *M today*, 9 juin 2021.
67. Pour plus de détail, voir Lakhani S., White J. et Wallner C., « The gamification of (violent) extremism : an exploration of emerging trends, future threat scenarios and potential P/CVE solutions », Réseau européen de sensibilisation à la radicalisation (RSR), 7 septembre 2022.
68. « State of play : trends in terrorist and violent extremist use of the Internet 2022 », Tech against Terrorism, 19 janvier 2023.
69. Europol, « European Union terrorism situation and Trend Report 2021 », Office des publications de l'Union européenne, Luxembourg,14 juillet 2022.
70. Voir par exemple « Online gaming platforms such as Roblox used as 'Trojan horse' for extremist recruitment of children, AFP warns », *The Guardian*, 3 décembre 2023.
71. Schlegel L. et Amarasingam A., « Examining the intersection between gaming and violent extremism », Bureau de lutte contre le terrorisme des Nations Unies, 6 octobre 2022.

Technologies émergentes

Parallèlement à cette évolution relativement progressive de la manière d'utiliser la technologie pour mener des actions de recrutement et de radicalisation, les terroristes et les extrémistes violents ont également commencé à expérimenter des technologies plus récentes. Ils se sont notamment tournés vers le web décentralisé (DWeb)[72] et le *dark web* pour partager et stocker de la propagande.

Les terroristes ont aussi commencé à utiliser l'IA générative pour créer du matériel de propagande[73] qui leur offre la possibilité de générer rapidement des contenus à caractère terroriste dans divers formats, styles et langues, et leur donne potentiellement l'opportunité de cibler plus efficacement différents groupes démographiques et catégories de population. D'aucuns craignent également que les agents conversationnels d'IA générative puissent être utilisés pour « externaliser » le processus de radicalisation[74], ces agents étant alors programmés pour renforcer les idéologies terroristes et promouvoir la désinformation, et ce, au besoin, dans plusieurs langues, 24 heures sur 24. Ce risque n'est pas purement hypothétique, puisqu'un agent conversationnel a incité une personne mentalement instable à commettre un attentat visant la Reine d'Angleterre en décembre 2021 (bien qu'il n'ait pas été programmé à cette fin)[75].

La mesure dans laquelle les terroristes utilisent l'IA générative, et d'autres technologies émergentes comme le métavers, pour mener des actions de radicalisation et de recrutement dépendra à nouveau des facteurs internes et externes décrits précédemment dans le présent rapport et, bien entendu, de la vitesse de développement de la technologie (et de fait, de son accessibilité et de l'efficacité). Pour contrer tout détournement, il conviendra peut-être aussi de s'intéresser non plus uniquement aux plateformes sur lesquelles les terroristes partagent et diffusent leur propagande et leurs contenus, mais aussi à la manière dont ces contenus sont créés et à l'endroit où ils le sont. Plus généralement, étant donné le rôle central de la technologie dans la radicalisation et le recrutement pour le terrorisme, les États membres devraient chercher à anticiper les innovations à venir en ce qui concerne la nature et les modalités d'utilisation des technologies.

Attaques terroristes

Modes opératoires actuels et matériel d'instruction

La technologie a toujours joué un rôle majeur en ce qu'elle permet aux terroristes de planifier, de mener et de faire connaître leurs attaques au public. Au cours des dix années ou presque qui ont suivi les attentats du 11 septembre 2001, les attaques relativement complexes, souvent perpétrées à l'aide d'EEI et d'armes à feu, ont continué de représenter la principale menace terroriste, les moyens de transport et les espaces publics étant visés dans l'espoir de faire un grand nombre de victimes.

À l'inverse, l'utilisation de méthodes simples et peu technologiques caractérise peut-être mieux la menace terroriste actuelle qui pèse sur l'Europe. Les trois derniers rapports d'Europol sur la situation et les tendances en matière de terrorisme dans l'Union européenne (TE-SAT) mettent en avant la prédominance de modes opératoires rudimentaires, notamment les attaques à l'arme blanche ou à la voiture bélier et les incendies criminels[76], parallèlement à un nombre moins élevé d'attentats ou de projets impliquant des EEI et des armes à feu.

L'évolution de ce contexte de menace au cours de la dernière décennie résulte de la conjonction d'une série de facteurs internes et externes. Il s'agit notamment du tournant dans la stratégie d'Al-Qaida – marqué notamment par son appel au « djihad open source » qui encourage les attaques locales et auto-initiées par le biais de son magazine *Inspire*[77] – et par la suite de l'EIIL/Daech, qui a appelé ses adeptes à commettre des attentats dans leur pays plutôt qu'à se rendre en Irak et en Syrie. Ces deux changements stratégiques ont été motivés dans une large mesure par les actions de lutte contre le terrorisme, qui ont compliqué la tâche des deux groupes pour planifier et diriger des attentats terroristes en dehors de leur sphère d'influence directe, y compris en Europe, ainsi que par la prise de conscience de la capacité des autorités à détecter et à déjouer des complots terroristes plus sophistiqués et plus complexes. Enfin, les acteurs terroristes d'extrême droite sont également parvenus à tirer des enseignements de ces tendances et ont, d'une certaine manière, modifié leurs méthodes d'attaque en conséquence.

72. Bodo L. et Trauthig I. K., « Emergent technologies and extremists : the DWeb as a new internet reality », GNET, 1er août 2022.
73. Borgonovo F., Bolpagni A. et Rizieri Lucini S., « AI-powered jihadist news broadcasts : a new trend in pro-IS propaganda? » GNET, 9 mai 2024.
74. Jowitt T., « Terrorism tsar warns of AI chatbot radicalisation risk », Silicon, 5 janvier 2024.
75. Vaughan H., « AI chat bot 'encouraged' Windsor Castle intruder in 'Star Wars-inspired plot to kill Queen' », *Sky News*, 5 juillet 2023.
76. Europol, « European Union terrorism situation and trend report 2021 », Office des publications de l'Union européenne, Luxembourg, 22 juin 2021.
77. Black I., « Inspire magazine : the self-help manual for al-Qaida terrorists », *The Guardian*, 24 mai 2013.

Bien que de nombreux attentats et projets d'attentats actuels utilisent un mode opératoire à faible technicité, cela ne signifie pas pour autant que leur planification ou la diffusion de la propagande à la suite d'une attaque réussie ne font pas appel à des technologies plus élaborées. Les communications au sein de groupes pour planifier des attaques et mener d'autres activités sont désormais généralement cryptées, ce qui pose des problèmes considérables aux autorités gouvernementales qui cherchent à les intercepter et à les comprendre.

S'agissant des acteurs isolés, ils puisent généralement leur inspiration idéologique et opérationnelle dans le matériel de propagande et d'instruction disponible en ligne. Toutefois, ces derniers temps, de plus en plus d'éléments semblent indiquer un retour au type de projets commis sur ordre, si répandus lorsque l'EIIL/Daech était à son apogée dans les années 2015-2016, mais cette fois-ci en lien avec l'EIPK. Après les attentats liés à ce groupe, déjoués par les autorités en Autriche, en France, en Allemagne, en Espagne et en Türkiye, force est de constater que l'EIPK représente la plus grande menace terroriste extérieure pour l'Europe. Certains États membres du Conseil de l'Europe ont avancé des parallèles avec le scénario de la menace terroriste émanant de l'EIIL/Daech de 2015 à 2017[78].

Étant donné le caractère récent de bon nombre de ces complots (dont la plupart ont été fomentés en 2024), il est difficile de déterminer dans quelle mesure ils ont été ordonnés ou inspirés par l'EIPK, ainsi que la technologie (le cas échéant) employée par ce dernier pour communiquer avec les assaillants en Europe, et le rôle probable joué par la technologie dans la planification de ces attentats. Cependant, compte tenu du succès qu'a connu dans le passé le modèle du « planificateur virtuel »[79] et de la zone de sécurité relative dont jouit l'EIPK (qui peut s'avérer un moteur essentiel de l'innovation terroriste), il est possible qu'à l'avenir les attentats ou les projets liés à cette mouvance utilisent un mode opératoire plus sophistiqué, notamment sur le plan de la technologie mise en œuvre à cet effet.

La forte présence en ligne de matériel didactique est un autre aspect essentiel de la contribution de la technologie au paysage actuel de la menace. Ces « guides pratiques » peuvent couvrir un large éventail d'activités, dont la fabrication d'armes artisanales et de bombes, le ciblage d'infrastructures critiques ou la manière de passer sous le radar lors de la préparation d'un attentat terroriste[80].

La menace posée par ce type de matériel est sérieuse et ne date pas d'hier, puisqu'elle remonte aux premiers manuels de fabrication d'explosifs, en passant par l'*Anarchist Cookbook* (le manuel de l'anarchiste) et le roman *Turner Diaries* (les carnets de Turner)[81]. Plus récemment, Al-Qaida dans la péninsule arabique a lancé en janvier 2010 son magazine *Inspire*, qui propose une multitude de matériels d'instruction, à commencer par son article tristement célèbre « Fabriquez une bombe dans la cuisine de votre maman » qui a ensuite inspiré la fabrication des engins explosifs utilisés lors de l'attentat terroriste du marathon de Boston en 2013[82]. L'éthique stratégique de ce magazine, décrite par les scientifiques comme la volonté de réduire les obstacles à l'engagement dans des activités terroristes dans le but de favoriser une culture du « faire soi-même » pour susciter des comportements terroristes[83], a ensuite été adoptée par l'EIIL/Daech et divers autres groupes ou mouvements terroristes, y compris d'extrême droite.

Ce matériel d'instruction est stocké et diffusé sur différentes plateformes, notamment sur le *dark web* et sur Telegram, en particulier au sein du collectif Terrorgram, un réseau Telegram néofasciste qui a récemment été interdit au Royaume-Uni en tant qu'organisation terroriste[84].

Armes imprimées en 3D

Le matériel didactique relatif à la production d'armes imprimées en 3D est un domaine de préoccupation particulier. Depuis que Defense Distributed a publié, en 2013, les fichiers numériques de la première arme à feu au monde quasi entièrement imprimée en 3D, la conception, la fiabilité et l'efficacité de ces armes se sont

78. Conseil de sécurité des Nations Unies, « Trente-quatrième rapport de l'Équipe d'appui analytique et de surveillance des sanctions, présenté en application de la résolution 2734 (2024) », 22 juillet 2024.
79. Gartenstein-Ross D., Clarke C. P. et Shear M., « Terrorists and technological Innovation », *Lawfare*, 2 février 2020.
80. Europol, « Terrorist 'how to' guides – focus of latest Europol Referral Action Day », 3 juillet 2020.
81. Reed A. et Ingram H. J., « Explaining the role of instructional material in AQAP's inspire and ISIS' Rumiyah », Europol, 26 mai 2017.
82. Esposito R., « Exclusive : government doc shows how closely Boston Marathon bombers followed al Qaeda plans », *NBC News*, 26 avril 2013.
83. Lemieux A. F. *et al*.,« Inspire magazine : a critical analysis of its significance and potential impact through the lens of the information, motivation, and behavioural skills model », *Terrorism and Political Violence*, 14 janvier 2014.
84. Farrell-Mozlloy J., « The proscription of Terrogram as a terrorist organisation in the UK : insights from the independent reviewer of terrorist legislation », *Vox-Pol*, 26 juin 2024.

rapidement améliorées[85], grâce à l'innovation et à l'expérimentation poussées d'un réseau en ligne d'acteurs malveillants et d'amateurs d'armes à feu[86].

Sans surprise, ces avancées ont également suscité l'intérêt des acteurs terroristes, y compris en Europe, où les mesures de lutte contre le terrorisme et de répression au sens large sont telles qu'il est généralement difficile pour les acteurs malveillants de se procurer de manière fiable des armes à feu. C'est l'un des facteurs qui expliquent la prédominance des engins explosifs improvisés et, plus récemment, des attaques terroristes au couteau ou à la voiture bélier en Europe[87].

Dans le même temps, un certain nombre d'autres facteurs internes et externes ont stimulé cet intérêt, en particulier dans les milieux d'extrême droite. Il s'agit notamment de la présence massive d'individus jeunes et très connectés au sein d'un mouvement peu structuré, et des possibilités d'apprendre les uns des autres dans le cadre des relations directes et indirectes offertes par ces communautés en ligne. Ainsi, l'exemple donné par l'auteur de l'attentat de Halle en 2019, dont l'arsenal comprenait des éléments imprimés en 3D, a pu être source d'inspiration.

Ces facteurs, associés à la baisse du coût des imprimantes 3D, ont fait grimper en flèche la menace terroriste posée par les armes imprimées en 3D, en particulier au cours des cinq années qui ont suivi l'attentat de Halle. Des arrestations ou des saisies ont été effectuées dans toute l'Europe, notamment en Allemagne, en Islande, aux Pays-Bas, en Espagne, en Suède, au Royaume-Uni et en Finlande[88]. Dans ce dernier exemple, lors de l'arrestation des quatre membres d'un groupuscule d'extrême droite qui projetait des attaques à caractère raciste et contre des infrastructures critiques, la police a mis la main sur des armes semi-automatiques et d'autres pièces d'armement fabriquées à l'aide d'une imprimante 3D. La condamnation ultérieure de ces hommes pour plusieurs infractions terroristes et relatives à l'utilisation d'armes à feu était la première condamnation pour terrorisme lié à l'idéologie d'extrême droite en Finlande[89].

Parmi les armes saisies par la police finlandaise figuraient quatre FGC-9, un pistolet hybride semi-automatique considéré comme l'une des armes à feu artisanales semi-automatiques les plus faciles à fabriquer pour un coût d'environ 500 dollars des États-Unis, et qui ne nécessite aucune pièce d'arme à feu réglementée, échappant ainsi à la législation européenne en la matière[90]. En effet, selon un rapport récemment établi dans le cadre du Projet INSIGHT, financé par l'UE, les armes à feu imprimées en 3D pourraient constituer le plus grand défi pour les contrôles nationaux et internationaux des armes légères[91].

Dans le même temps, les manuels, les fichiers de conception assistée par ordinateur (CAO) et les instructions relatives à la conception et à la fabrication d'armes telles que le FGC-9 sont facilement accessibles sur des plateformes en ligne[92]. Les risques posés par les armes imprimées en 3D sont donc à la fois d'ordre technologique et profondément liés à la facilité d'accès à du matériel d'instruction tant sur le web de surface, via toute la gamme de services en ligne (d'où la nécessité d'une modération efficace du contenu), que sur le *dark web*.

Un autre sujet d'inquiétude tient à la conjonction potentielle des risques posés par l'impression 3D et une autre menace terroriste liée à la technologie, à savoir les drones. En effet, en septembre 2023, un étudiant britannique a été reconnu coupable de préparation d'actes terroristes après la saisie à son domicile d'un drone et d'une imprimante 3D capable de servir à la fabrication de ses composants. Le suspect, qui a ensuite été condamné à la réclusion à perpétuité, projetait d'équiper le drone d'armes chimiques[93]. Comme nous l'avons vu dans l'étude de cas n° 1, malgré l'adoption à ce jour relativement limitée des systèmes autonomes sans pilote dans le contexte européen, les drones n'en demeurent pas moins un vecteur d'attaque jugé très préoccupant par les services de lutte contre le terrorisme.

85. Veilleux-Lepage Y., « Printing terror : an empirical overview of the use of 3D-printed firearms by right-wing extremists », CTC Sentinel, juin 2024.
86. Red Team Working Group, « Risks and challenges in online communities for 3D-printed firearms among extremists and terrorists », GIFCT 20 septembre 2023.
87. Voir, par exemple, Pauwels A., « Prevention of gun-, knife-, bomb- and arson-based killings by single terrorists », dans *Handbook of Terrorism Prevention and Preparedness*, Centre international pour la lutte contre le terrorisme (ICCT), 2021.
88. Vallance C., « 3D printed guns : warnings over growing threat of 3D firearms », *BBC News*, 9 novembre 2022.
89. « Finnish neo-Nazis used 3D printer to make guns in preparation for 'race war' », *The Guardian*, 31 octobre 2023.
90. Dass R., « 3D-printed weapons and the far-right : the Finnish accelerationist cell », GNET, 6 octobre 2023.
91. Schroeder M *et al*., « Privately made firearms in the European Union », Projet Insight, Small Arm Survey, décembre 2023.
92. Dass R., *op. cit*., GNET, 6 octobre 2023.
93. Page T., « Mohamed Al Bared : student jailed for life for building IS drone », *BBC News*, 22 décembre 2023.

Publicité

Enfin, la technologie joue un rôle de plus en plus important dans la capacité des terroristes à médiatiser leurs attaques, y compris en temps réel. Là encore, une série de facteurs internes sont à l'origine de cette évolution. Sur le plan stratégique, la capacité de l'EIIL/Daech à revendiquer rapidement la responsabilité des actes commis, directement ou, dans le contexte européen, par le biais de vidéos ou de déclarations produites et parfois diffusées par le ou les assaillants, lui a permis de renforcer sa promesse de « rester et s'étendre ». Sur le plan organisationnel, le modèle de « résistance sans chef » privilégié par l'extrême droite a également encouragé l'innovation insufflée par la base, s'agissant entre autres du contenu associé aux attaques (les événements diffusés en direct et, souvent, des manifestes) mais aussi des modalités et du lieu de sa diffusion.

Vu de l'extérieur, les dernières actions menées par l'extrême droite ont souvent montré ouvertement dans quelle mesure les acteurs terroristes peuvent apprendre et s'inspirer les uns des autres, notamment en faisant référence à des attentats commis précédemment et à leurs auteurs, en reproduisant l'imagerie et en recourant à des méthodes similaires. La popularité des attaques terroristes diffusées en direct témoigne également des ressources dont disposent les assaillants solitaires en Europe, en termes à la fois de facilité d'accès à la technologie nécessaire pour assurer la retransmission en direct, mais aussi de familiarité avec ce concept (et ses avantages) dans des situations sans lien avec le terrorisme, en raison de leur âge et du temps qu'ils passent en ligne. Enfin, les mesures antiterroristes, qui ont limité l'accès des acteurs terroristes aux grandes plateformes de réseaux sociaux, ont contraint ces derniers à rechercher des moyens plus novateurs d'atteindre la viralité et de maximiser l'impact de leurs attaques.

Financement du terrorisme

Tendances actuelles

Le financement des activités terroristes en Europe (et depuis l'Europe) a également été soumis à certains des mêmes facteurs internes et externes (en particulier les pressions dues à la mise en œuvre de mesures de LBC/FT) et à l'évolution plus générale du paysage de la menace terroriste. Le financement du terrorisme est également de plus en plus tributaire d'une multitude de technologies.

Après le 11 septembre 2001, les services répressifs étaient surtout préoccupés par les mouvements de fonds opérés par les dirigeants d'Al-Qaida vers les cellules opérationnelles à travers le monde, selon le modèle établi pour les attentats du 11 septembre 2001 eux-mêmes. Toutefois, il ressort des recherches menées ultérieurement que ce modèle a atteint son apogée à cette date, en raison, du moins en partie, de la pression antiterroriste qui s'en est suivie. Al-Qaida s'est alors détourné des attaques dirigées, financées (et planifiées) par des acteurs terroristes situés en dehors de l'Europe au profit d'une activité de propagande susceptible d'inciter des individus à initier eux-mêmes des attaques, généralement autofinancées[94].

Les données recueillies par la suite dans le cadre d'une série d'études et de rapports gouvernementaux nationaux ou régionaux ont fourni des indications précieuses sur les sources de financement de ces types d'attentats et de complots. Celles-ci englobent des revenus légitimes, des crédits ou des prêts, des prestations versées par l'État, des dons de particuliers, la vente d'effets personnels et les produits d'activités illicites ; si certains éléments attestent de l'utilisation d'actifs virtuels pour se procurer du matériel au cours de la phase de préparation d'un attentat, ces actifs ne semblent pas avoir été utilisés comme *source de* financement[95] (pour plus d'informations, voir l'étude de cas n° 2). Bien que le tableau dressé ci-dessus tende vers un paysage de menaces relativement peu technologique en matière de lutte contre le financement du terrorisme (LFT), la plupart de ces sources de financement – et la manière dont elles sont ensuite utilisées pour acquérir des armes, d'autres composants ou mener des activités de reconnaissance – interfèrent encore généralement avec le système financier ordinaire et nécessitent (dans une certaine mesure) l'utilisation de la technologie pour accéder aux fonds, les distribuer et les dépenser.

Bien entendu, le financement du terrorisme en Europe ne se limite pas à la conduite d'attentats, des fonds étant requis pour soutenir un large éventail d'activités terroristes (en particulier à des fins de radicalisation et de recrutement). Là encore, ces fonds proviennent entre autres de structures commerciales légales, de la collecte de dons – notamment lors d'événements en présentiel – ou des cotisations de membres, et d'activités criminelles. Les acteurs terroristes ont également recours à la vente de marchandises, de vidéos, de publications et de billets de spectacles (par exemple des concerts), y compris sur des plateformes de commerce

94. Reimer S. et Redhead M., « A new normal : countering the financing of self-activating terrorism in Europe », RUSI Europe, mai 2021.
95. *Ibid.*

électronique, pour recueillir des fonds[96]. Cette pratique est particulièrement répandue parmi les groupes et mouvements d'extrême droite.

Cependant, les activités de LFT en Europe – du moins en ce qui concerne les arrestations et les condamnations – se sont principalement intéressées aux flux de fonds en provenance de ce continent et destinés à des groupes terroristes établis dans d'autres parties du monde, notamment en Syrie. Ainsi, en 2020, l'Autriche, l'Allemagne, l'Irlande, les Pays-Bas, l'Espagne, la Suède, la Suisse et le Royaume-Uni ont arrêté, inculpé ou condamné des individus pour des infractions de financement du terrorisme liées au transfert de fonds hors d'Europe, à destination de groupes tels que l'EIIL/Daech et le Parti des travailleurs du Kurdistan (PKK)[97]. En 2022, les États membres de l'Union européenne ont fait état de 14 arrestations pour des infractions liées au financement du terrorisme, toutes en rapport avec le « terrorisme inspiré par l'EIIL/Daech ou Al-Qaida », la majorité des personnes concernées étant accusées d'avoir levé des fonds pour des organisations terroristes situées hors de l'UE[98].

Plusieurs facteurs expliquent cette focalisation sur les fonds transférés d'Europe vers les groupes terroristes. Parmi eux figurent notamment le changement de stratégie organisationnelle et d'attaque opéré par Al-Qaida et l'EIIL/Daech, la résonance que continuent d'avoir les actions menées par ce dernier en Syrie auprès des acteurs terroristes établis en Europe – en particulier en ce qui concerne les femmes et les enfants affiliés à l'EIIL/Daech encore en détention et dont beaucoup sont européens ou entretiennent des liens étroits avec l'Europe – et les conséquences à long terme des mesures de lutte contre le terrorisme et son financement sur la capacité des groupes terroristes à transférer des fonds vers l'Europe[99].

Malgré son incidence moins directe et à court terme sur le paysage européen de la menace, la présence de groupes terroristes dotés de ressources suffisantes et opérant à partir de lieux relativement sûrs en lien direct avec l'Europe reste très préoccupante. De plus, alors que la menace posée par le terrorisme d'extrême droite a considérablement augmenté au cours des cinq dernières années, son modèle de résistance sans chef ne facilite pas la tâche des États membres pour ce qui est de proscrire, désigner ou interdire des groupes terroristes d'extrême droite ; or il s'agit souvent d'un préalable essentiel à toute action efficace de lutte contre le financement du terrorisme à l'échelon national.

Actifs virtuels et méthodes émergentes

Ce sont principalement les actions de ces acteurs terroristes extérieurs, par opposition à ceux qui mènent des activités de collecte de fonds et/ou envoient des fonds à l'étranger depuis l'Europe, qui ont motivé l'utilisation des nouvelles technologies dans le domaine du financement du terrorisme. S'agissant de l'EIIL/Daech et de l'utilisation ou de la réception d'actifs virtuels, malgré son intérêt de plus en plus marqué et sa capacité accrue à en percevoir depuis 2020, d'importantes variations régionales subsistent entre les provinces et les sous-groupes de l'organisation.

Bien que l'EIIL/Daech central s'appuie principalement sur les passeurs de fonds et le réseau hawala, d'autres provinces de l'EIIL/Daech ont adopté une approche plus diversifiée, l'EIPK et le réseau de l'Afrique de l'Est et du Sud se distinguant par leur utilisation croissante (mais encore relativement limitée) des cryptomonnaies. En revanche, peu d'éléments attestent d'un tel recours par la province de l'État islamique en Afrique de l'Ouest (EIAO) ou les groupes de l'EIIL/Daech opérant au Mozambique et en République démocratique du Congo[100]. Ces variations sont elles-mêmes le reflet d'un ensemble de facteurs internes et externes. Les scientifiques mettent en avant l'importance de la situation locale, notamment la présence d'un secteur des cryptomonnaies bien développé dans le pays de destination et le besoin impérieux de contourner les systèmes financiers conventionnels[101].

Certaines données probantes montrent que des individus établis en Europe cherchent à envoyer des fonds à l'EIIL/Daech à l'aide d'actifs virtuels. En février 2024, les autorités espagnoles ont interpellé un homme qui aurait transféré à l'EIIL/Daech près de 200 000 euros en cryptomonnaies[102]. En juin de la même année, les autorités

96. Europol, « European Union terrorism situation and Trend Report 2023 », Office des publications de l'Union européenne, Luxembourg, octobre 2023.
97. Europol, « European Union terrorism situation and Trend Report 2021 », Office des publications de l'Union européenne, Luxembourg, 22 juin 2021.
98. Europol, « European Union tTerrorism sSituation and Trend Report 2023 », op. cit., octobre 2023.
99. Une juridiction a signalé que des groupes terroristes ont également cherché à exploiter des catastrophes naturelles (telles que des tremblements de terre) pour collecter des fonds sous le couvert d'une « aide aux sinistrés ».
100. Davis J., « The financial future of the Islamic State », CTC Sentinel, juillet-août 2024.
101. *Ibid*.
102. « Jordanian national arrested in Spain for sending 200,000 euros in cryptocurrencies to the Islamic State », *TRM*, 1er février 2024.

allemandes ont procédé à l'arrestation d'une personne qui avait notamment viré près de 1 700 dollars des États-Unis en cryptomonnaies à une adresse liée à l'EIPK[103].

Dans une perspective européenne, cette différence de capacité selon les groupes (ou sous-groupes) terroristes à recevoir et à utiliser des actifs virtuels aura ainsi une incidence sur la mesure dans laquelle les acteurs européens pourront envoyer des fonds par ce biais à des groupes terroristes implantés à l'étranger. Diverses raisons peuvent expliquer qu'un individu ou un groupe soit plus enclin à envoyer des fonds à l'EIAO plutôt qu'à l'EIPK par exemple (notamment l'origine nationale ou ethnique, les liens familiaux ou amicaux, ou encore l'impact/la visibilité de leurs opérations terroristes). Il se peut qu'à l'avenir la propension d'une « province » de l'EIIL/Daech à percevoir des fonds au moyen d'une technologie particulière (par exemple les cryptomonnaies), ou sa meilleure compatibilité technologique avec des sources potentielles de financement du terrorisme en Europe puissent également influer sur le choix du destinataire.

Bien d'autres technologies nouvelles ou émergentes sont utilisées pour transférer des fonds à des groupes terroristes régionaux ou internationaux, dont les systèmes de paiement mobile, les échanges et portefeuilles en ligne, le financement participatif, les transferts en ligne entre particuliers et la sollicitation de dons sur les plateformes de réseaux sociaux, y compris par le biais de la fonctionnalité « super-*chat* »[104]. Là encore, même si les terroristes ont toujours principalement recours aux méthodes traditionnelles pour déplacer des fonds (y compris les espèces, les systèmes de transfert de fonds et le hawala), chacune de ces nouvelles technologies est susceptible de mettre à rude épreuve les approches actuelles en matière de lutte contre le financement du terrorisme, en raison notamment de leur utilisation possible pour diversifier les risques et/ou en combinaison les unes avec les autres.

103. « German authorities arrest man suspected of sending cryptocurrency to ISKP », *TRM*, 13 juin 2024.
104. Direction exécutive du Comité contre le terrorisme des Nations Unies (DECT), « CTED's tech sessions : highlights on threats and opportunities related to new payment technologies and fundraising methods », 29 octobre 2022.

Réponses antiterroristes au détournement des nouvelles technologies

Enseignements tirés

Afin de mieux comprendre la manière dont les terroristes exploitent les nouvelles technologies et l'impact de ces innovations sur le paysage terroriste en Europe, des entretiens ont été menés avec divers experts nationaux, régionaux et internationaux. Chacun d'entre eux dispose d'une expérience solide et contemporaine de la lutte contre l'utilisation des nouvelles technologies par les terroristes dans différents contextes. Au cours de ces entretiens, ils ont recensé les bonnes pratiques et les enseignements tirés qui pourraient, à l'avenir, s'appliquer plus largement à la lutte contre le détournement des nouvelles technologies, dans un contexte antiterroriste.

- **Lenteur des réponses :** plusieurs des expertes ont opposé la rapidité avec laquelle les acteurs terroristes sont capables de tester et d'adopter une multitude de nouvelles technologies, et le temps que mettent souvent les organisations nationales, régionales et internationales à identifier les risques que leur utilisation pourrait poser, avant même d'envisager la meilleure façon d'y répondre. Tout en reconnaissant que, de par leur nature même, les acteurs terroristes sont généralement plus souples et plus agiles que les acteurs étatiques, les parties prenantes ont jugé excessif le décalage entre les deux réponses.
- **Défis liés au partage de l'information :** étant donné le caractère transnational de la menace terroriste, souvent favorisé par la technologie, les services nationaux ne sont pas en mesure de gérer seuls cette menace, en raison en particulier des différences (souvent importantes) de capacités techniques et de ressources dont ils disposent. Cependant, les experts interrogés ont identifié des obstacles structurels et organisationnels récurrents à l'échange efficace et rapide d'informations entre les pays (et parfois en leur sein).
- **Difficultés d'accès à l'information** : l'utilisation des technologies à des fins terroristes a souvent exacerbé ce problème car les États sont contraints d'entretenir des relations complexes avec différentes entités du secteur privé situées dans plusieurs juridictions. Les parties prenantes ont mis en avant des différences notables en termes de qualité des relations établies entre certaines entreprises du secteur privé (notamment les grandes plateformes de réseaux sociaux ou de communication) et plusieurs pays européens, en particulier les États moins bien dotés en services de renseignement et de police, ou confrontés depuis moins longtemps au problème du terrorisme. Ces difficultés ont eu une incidence directe sur les résultats opérationnels et ont contribué à une dépendance accrue à l'égard des renseignements communiqués par les services étrangers (dans certains contextes nationaux).
- **Progrès technologiques et phénomène du *going dark* (passage dans la clandestinité) :** l'évolution des capacités offertes par un ensemble de nouvelles technologies, dont les drones, la criminalistique numérique et l'IA, ainsi que les nombreux aspects de nos vies disponibles en ligne d'une manière ou d'une autre, offrent aux acteurs gouvernementaux de nouveaux moyens de mieux surveiller et comprendre les activités des acteurs terroristes. Toutefois, ces outils et d'autres nouvelles technologies posent également des défis supplémentaires en matière de surveillance, notamment en raison de l'utilisation généralisée du cryptage. Auparavant, ce procédé entravait principalement la capacité des forces de l'ordre et des services de renseignement à intercepter les communications des terroristes, mais il a aujourd'hui de plus en plus d'impact sur la criminalistique numérique à travers une gamme bien plus étendue de dispositifs (dont les drones, les voitures et les équipements de l'Internet des objets). En d'autres termes, les acteurs gouvernementaux risquent de perdre de vue le détournement d'un éventail bien plus large de nouvelles technologies, de même que toute information connexe sur les éventuelles futures menaces.
- **Incohérence des objectifs stratégiques :** malgré les preuves d'inefficacité accumulées depuis plusieurs décennies, la rhétorique antiterroriste continue de s'attacher à la *prévention* de toute utilisation abusive d'une technologie particulière à des fins terroristes, ce qui a parfois une incidence sur les objectifs stratégiques des activités concernées (par exemple la législation relative au retrait des contenus à caractère terroriste publiés sur les services en ligne). Certaines des personnes interrogées ont estimé que l'incapacité à admettre qu'il est fondamentalement impossible d'assurer une prévention totale fait obstacle à un ajustement des objectifs généraux des réponses à apporter et des activités spécifiques qui les sous-tendent.

- **Approches cloisonnées et spécifiques à la lutte contre le terrorisme :** malgré l'élaboration de réponses solides (et dans l'ensemble efficaces) spécifiques à ce domaine, notamment en ce qui concerne les contenus à caractère terroriste en ligne et le financement du terrorisme, les experts ont estimé que l'on n'accordait pas suffisamment d'attention à l'interconnexion entre ces réponses (et les phénomènes sur lesquels elles portent) et les domaines d'action et contextes plus larges. Bien que la lutte contre le terrorisme ne soit pas toujours l'angle d'approche le plus approprié pour relever les défis (ou du moins pas le seul), elle tend encore à prédominer.
- **Risques en matière de droits humains :** bien que les nouvelles technologies offrent d'importantes possibilités en termes d'amélioration ou de renforcement de toute une panoplie de mesures antiterroristes, ces outils puissants engendrent également des risques majeurs pour les droits humains, en particulier en ce qui concerne les activités légitimes de la société civile et des groupes de défense des droits fondamentaux. Dans certains cas, les violations des droits humains sont le fruit de réactions excessives d'acteurs gouvernementaux, délibérées ou non, mais elles sont également imputables aux actions d'entités du secteur privé faisant suite à une demande des autorités ou découlant d'une application trop zélée et abusive des conditions générales d'utilisation des services.
- **Conflit entre respect de la vie privée et sécurité :** les personnes interrogées ont également fait part de leurs préoccupations quant aux contradictions ou chevauchements fréquents des législations, s'agissant en particulier de l'imposition de conditions de sécurité qui pourraient être contraires à celles liées au respect de la vie privée. Ce conflit est particulièrement problématique pour les entreprises du secteur privé qui cherchent à s'y retrouver dans toutes ces dispositions législatives. Dans le même temps, certains représentants des pouvoirs publics étaient toujours d'avis que l'équilibre entre ces deux principes penchait trop en faveur du respect de la vie privée, ce qui limitait les moyens techniques à leur disposition, notamment en ce qui concerne l'interception et le cryptage.
- **Contexte géopolitique** : plusieurs des interlocuteurs et interlocutrices ont évoqué les défis liés à l'effritement de l'ordre international, caractérisé par la remise en cause du multilatéralisme et l'intensification de la concurrence nationale et régionale ; d'où le fossé grandissant entre les normes relatives aux droits humains, les approches des nouvelles technologies et la gouvernance d'internet elle-même, la technologie étant perçue comme un vecteur de concurrence et non de coopération. Cette situation pose de plus en plus de problèmes à de nombreuses parties prenantes, notamment aux entreprises du secteur des technologies, dont beaucoup ont une dimension transnationale ou internationale. Elles sont ainsi amenées à jongler avec différentes exigences et normes législatives nationales ou régionales, qui sont souvent en conflit les unes avec les autres.

Bonnes pratiques

- **Analyse prospective :** certains des spécialistes interrogés ont constaté que la conduite d'exercices d'analyse prospective ou de prospective stratégique avait permis à leurs organisations de réduire le délai entre le détournement des nouvelles technologies par des terroristes et l'identification des risques qui y sont associés. Grâce à cette identification plus rapide, les organisations de divers secteurs d'activité sont ainsi mieux à même de répondre à ces risques.
- **Approches multipartites** : pour faciliter ce type d'échanges, les parties prenantes ont mis en avant l'efficacité des plateformes d'échange multipartites, qui ont déjà permis un meilleur partage de l'information entre les autorités nationales et les entreprises du secteur privé. Bien que ce type d'approche présente des défis importants, liés notamment à la confiance, à la sécurité et aux ressources, il est jugé essentiel pour mieux comprendre les méthodes et les points de vue de chaque secteur et a contribué à créer une boucle de retour d'information constructive entre les différentes entités impliquées. Le recours par le GIFCT à des groupes de travail multipartites pour mener des exercices selon la méthode de « l'équipe rouge » (*red teaming*) sur les menaces émergentes, notamment les armes imprimées en 3D, est un exemple de cette approche dans le contexte de l'identification des menaces et des risques[105]. Sur le plan opérationnel, la plateforme pour la lutte contre les contenus illicites en ligne (PERCI) d'Europol a également permis aux États membres de l'UE de normaliser leurs pratiques de signalement de contenus à caractère terroriste à des entités du secteur privé et de bénéficier d'un retour d'information précieux destiné à améliorer la coopération à l'avenir.

105. Red Team Working Group, « Risks and challenges in online communities for 3D-printed firearms among extremists and terrorists », GIFCT, 20 septembre 2023.

- **Rôle du milieu universitaire et de la société civile dans l'identification des tendances :** bien que les acteurs étatiques ou du secteur privé aient généralement accès à des documents classifiés ou sensibles qui leur offrent un éclairage unique sur les tendances émergentes, les experts ont également souligné le rôle déterminant joué par les institutions universitaires et de la société civile pour compléter ces sources d'information. Ils ont notamment cité les recherches menées par le Global Network on Extremism and Technology (GNET) (Réseau mondial sur l'extrémisme et la technologie)[106], avec le soutien du GIFCT, ainsi que les activités du réseau consultatif du Centre européen de lutte contre le terrorisme d'Europol[107]. Pour les entreprises du secteur privé confrontées au problème du détournement des plateformes ou des technologies par des acteurs terroristes, ces travaux de recherche (et ceux réalisés par divers autres réseaux et instituts de recherche) sont essentiels et amplement mis à profit. Les acteurs de la société civile sont également souvent bien placés pour identifier les nouveaux méfaits, compte tenu de leurs liens avec les communautés les plus touchées par le terrorisme et l'extrémisme violent.
- **Collaboration avec le secteur privé :** les parties prenantes ont estimé que les entreprises du secteur privé avaient également besoin de forums leur permettant de partager les enseignements tirés de l'exploitation de leur technologie par les terroristes et la meilleure façon d'y répondre. Les bonnes pratiques établies dans le cadre de la lutte contre l'utilisation d'internet à des fins terroristes et du financement du terrorisme pourraient servir de modèle à suivre dans d'autres contextes technologiques ; toutefois, il a été reconnu qu'il fallait redoubler d'efforts pour associer un éventail plus diversifié d'entreprises. Il convient notamment de soutenir davantage les petites entreprises, qui disposent généralement de moins de ressources pour s'attaquer directement à l'exploitation des technologies par les terroristes, répondre aux demandes des services répressifs et appréhender les dispositions législatives ou réglementaires, qui relèvent souvent de plusieurs juridictions. Outre le partage d'informations et de bonnes pratiques, cette collaboration pourrait également être mise en place sous la forme d'un mentorat entre pairs, d'une formation ou d'un soutien.
- **Clarté des objectifs stratégiques :** les objectifs stratégiques (et leur formulation) s'avèrent plus efficaces lorsqu'ils sont axés sur des résultats atteignables – à savoir l'objectif de rendre aussi difficile que possible le détournement d'une technologie donnée par les terroristes – plutôt que sur des arguments rhétoriques convaincants. Les approches fondées sur ce type d'objectif stratégique visent généralement à faire obstacle à l'utilisation d'une technologie donnée par les terroristes et à limiter la portée et l'impact des activités connexes. Selon les parties prenantes, elles pourraient encore avoir un effet positif sur le paysage terroriste.
- **Approches neutres sur le plan technologique :** les interlocuteurs et interlocutrices ont comparé l'efficacité des approches technologiquement neutres, qui mettent l'accent sur les résultats escomptés, à celle des initiatives qui cherchent à définir les mesures à prendre pour les atteindre. Avec cette dernière approche, en particulier lorsqu'elle est axée sur les activités technologiques, la législation pourrait devenir obsolète ou dépassée à mesure que les menaces et les réponses évoluent en corrélation avec les nouvelles technologies. Dans les faits, lorsque le choix s'est porté sur une approche technologiquement neutre, les entreprises du secteur privé ont été en mesure de mettre à profit leur expertise pour accroître l'impact.
- **Meilleure utilisation des outils et approches existants** : certaines personnes interrogées ont salué les réponses à l'exploitation des nouvelles technologies par les terroristes, qui incluent l'utilisation d'outils et de législations développés dans différents contextes de lutte contre le terrorisme. Par exemple, les personnes qui fournissent des drones ou d'autres nouvelles technologies à des acteurs terroristes pourraient faire l'objet de sanctions en vertu des obligations découlant des Résolutions 1267 (1999) et 1373 (2001) du Conseil de sécurité des Nations Unies.
- **Approches plus larges s'intégrant mieux dans les réponses non liées à la lutte contre le terrorisme ou se rattachant à ces réponses** : les parties prenantes ont estimé que les actions antiterroristes les plus efficaces, en particulier dans le domaine des technologies, étaient celles qui s'inscrivaient le mieux dans un environnement politique plus large. En règle générale, elles ont également reconnu que certains aspects du problème de l'utilisation des nouvelles technologies à des fins terroristes étaient mieux abordés en dehors du cadre de la lutte contre le terrorisme.

106. Pour plus d'informations, voir le site internet du GNET.
107. Pour des informations sur la conférence annuelle 2024 du réseau consultatif, voir le site internet d'Europol.

Conclusion

Sur la base des conclusions du rapport – en particulier des informations recueillies lors des entretiens – sont présentées ci-après un ensemble limité de recommandations à l'intention des États membres du Conseil de l'Europe, d'autres organes gouvernementaux, d'institutions intergouvernementales, d'acteurs du secteur privé et de la société civile.

- Les acteurs de la lutte contre le terrorisme et de la protection et de la conservation de la vie privée devraient **s'efforcer de discerner et d'évaluer plus rapidement les risques liés aux nouvelles technologies.** Le raccourcissement du délai entre l'expérimentation terroriste et son identification peut permettre aux acteurs de la lutte contre le terrorisme de mieux contextualiser les risques potentiels qu'une technologie peut poser – et qui, dans certains cas, peuvent être moins importants qu'on ne le pensait – et d'améliorer la rapidité avec laquelle des réactions (le cas échéant) peuvent être élaborées. Cet objectif peut être atteint grâce à une fonction permanente d'analyse prospective ou à des exercices de prévision stratégique ad hoc tels que les attaques informatiques fictives (*red teaming*). Une collaboration accrue avec (et entre) les parties prenantes de différents secteurs peut également contribuer à ce processus d'identification et de réponse.
- Cette façon de procéder devrait être complétée par des actions visant à **améliorer le partage des informations relatives à l'exploitation des nouvelles technologies par les terroristes**. Bien que le partage d'informations soit un défi permanent et de longue date de la lutte contre le terrorisme – compte tenu des sensibilités liées aux capacités et aux activités opérationnelles – le partage de données anonymes ou désagrégées liées à l'utilisation abusive et à l'exploitation des nouvelles technologies par les terroristes (par exemple les tendances liées à l'utilisation abusive de l'IA) peut aboutir à une meilleure compréhension collective des risques qu'elles peuvent poser. Dans la mesure du possible, le partage devrait avoir lieu non seulement au sein des autorités nationales et entre elles, ainsi qu'avec les partenaires régionaux et internationaux, mais aussi entre les gouvernements, le secteur privé, la société civile et le monde universitaire, ce qui permettrait de remédier aux différences de capacités, de relations et d'accès à l'information, ainsi qu'à la nature transnationale du paysage terroriste actuel.
- Chacune de ces recommandations souligne l'importance d'**élaborer des approches multipartites de l'exploitation des nouvelles technologies par les acteurs terroristes**. Outre le partage d'informations, ces approches devraient inclure un dialogue constructif, la création de forums pour le partage des enseignements tirés et des bonnes pratiques, des possibilités de mentorat et d'aide au renforcement des capacités (y compris la fourniture d'outils et de techniques spécifiques), et la création de boucles de retour d'information pour aider à façonner et à reprendre les réactions.
- Ces approches devraient également chercher à impliquer des partenaires moins traditionnels, y compris des entités ayant une expérience de la réaction aux menaces liées aux nouvelles technologies dans d'autres contextes, contribuant ainsi à **développer une approche plus globale et moins cloisonnée de l'exploitation des nouvelles technologies**. En tirant les leçons de l'expérience d'un plus grand nombre d'organisations, les acteurs de la lutte contre le terrorisme peuvent intégrer de nouvelles approches ou de nouveaux partenaires dans leurs réactions.
- Il est nécessaire d'**intensifier les actions menées pour gérer et atténuer les risques importants en matière de droits humains** qui sont souvent associés aux outils et aux approches utilisés pour lutter contre l'utilisation des nouvelles technologies par les terroristes. Nombre des recommandations susmentionnées devraient y contribuer – en particulier la participation accrue de la société civile – mais elles devraient être complétées par de solides mécanismes de transparence et de contrôle (pour les organisations des secteurs public et privé) et par un retour d'information régulier de la part des organisations de défense des droits humains.

- Les acteurs de la lutte contre le terrorisme devraient également s'efforcer de **formuler plus clairement leurs objectifs, notamment en envisageant des approches neutres sur le plan technologique**. En s'attachant à créer des barrières à l'entrée pour l'utilisation par les terroristes d'une technologie donnée – ou en limitant la portée et l'effet de leurs activités connexes –, les acteurs de la lutte contre le terrorisme ont plus de chances d'avoir un effet positif sur le paysage terroriste. En déterminant ainsi les objectifs visés, ils peuvent contribuer à concevoir des approches technologiquement neutres, permettant au secteur privé et aux autres parties prenantes de rester axés sur le résultat souhaité, étant donné en particulier l'évolution rapide du paysage technologique.

Depuis plus de 40 ans, le Conseil de l'Europe s'efforce d'élaborer et de renforcer les normes juridiques essentielles pour prévenir et réprimer les actes de terrorisme. Grâce à une approche globale, l'Organisation aide les États membres à lutter plus efficacement contre le terrorisme en renforçant et en améliorant leur législation nationale, facilitant ainsi la coopération internationale. Dans le plein respect des droits humains et de l'État de droit, le Conseil de l'Europe œuvre sans relâche à traduire les terroristes en justice et à renforcer la coopération internationale.

PREMS 082225

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits humains du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits humains, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE