

مناقب

Bulletin mensuel publié par la Coalition Islamique Militaire pour Combattre le Terrorisme (CIMCT)

MÉMORANDUM DE COOPÉRATION CONJOINTE ENTRE LA CIMCT ET L'UNIVERSITÉ ISLAMIQUE IMAM MOHAMMED BIN SAOUD



Le Major Général Mohammed bin Said Al Mughaidi, Secrétaire Général, désigné, de la CIMCT et le Professeur Ahmed bin Salem Al-Ameri, Président de l'Université Islamique Imam Mohammed bin Saoud, ont signé, à Riyad, le 28 février 2021, un mémorandum de coopération conjointe entre la Coalition et l'Université. Al-Mughaidi a souligné que le but du mémorandum est de renforcer le partenariat entre les deux institutions en incarnation de leur rôle pionnier local, régional et international dans la lutte contre l'extrémisme et le terrorisme, se disant impatient de tirer parti de cette coopération.

Le Prof. Al-Ameri a salué, de son côté, les efforts de la Coalition, émettant l'espoir que ce partenariat contribuera à atteindre les objectifs des deux parties au service des sociétés arabe et islamique. 🌸

LE SECRÉTAIRE GÉNÉRAL REÇOIT LE CHARGÉ D'AFFAIRES DE L'AMBASSADE DE SIERRA LEONE À RIYAD



Le Secrétaire Général désigné de la CIMCT a reçu son excellence l'Ambassadeur Hassan Koroma, chargé d'affaires à l'ambassade de Sierra Leone à Riyad et la délégation l'accompagnant. Les deux parties ont examiné la coopération bilatérale et les visions communes pour lutter contre le terrorisme.

L'Ambassadeur a entendu une explication sur les efforts de la Coalition dans la lutte contre le terrorisme dans les quatre domaines d'action: (Idéologique, médiatique, anti-financement du terrorisme et militaire), en plus du soutien aux États Membres.

L'Ambassadeur Koroma a rencontré par ailleurs les Délégués de Sierra Leone auprès de la Coalition et a pris connaissance de leur action. Son Excellence a salué l'impact de la Coalition dans la lutte contre le terrorisme, à travers les partenariats stratégiques noués entre les États Membres, et le soutien aux États et organisations pour renforcer les capacités, échanger les expériences et promouvoir les efforts visant de paix. 🌸

TERRORISME ENTRE PENSÉE ET CROYANCE



Le Centre de la Coalition Islamique Militaire pour Combattre le Terrorisme (CIMCT) a organisé, à son siège à Riyad, le 01.02.2021, une Conférence intitulée (Le terrorisme entre pensée et croyance), présentée par Dr. Zayed bin Ajeer Al-Harithi, Délégué du Royaume d'Arabie Saoudite à la CIMCT. Al-Harithi a souligné au début que le phénomène du terrorisme s'est largement atténué, mais qu'il restera problématique pendant un certain temps avant que l'humanité ne s'en débarrasse, précisant que l'un des facteurs qui entravent le processus de contrôle du phénomène réside dans l'incapacité à parvenir à des définitions communes aux termes clés de ce fléau, ce qui empêche d'élaborer les programmes préventifs et stratégiques susceptibles de l'éradiquer.

Al-Harithi a souligné les interférences entre les termes de déviation, d'extrémisme, de terrorisme et d'outrance idéologiques ainsi que pour d'autres termes du domaine, affirmant bien que les spécialistes en linguistique, psychologie, sociologie, religion et sécurité aient traité ces termes en détail, depuis des décennies, il n'en reste pas moins vrai que le désaccord subsiste concernant les définitions de certains termes au niveau mondial, comme cela c'est le cas des définitions de l'extrémisme et du terrorisme, chacun avançant sa propre définition, en particulier au sujet de l'acte terroriste, considéré en fonction de son arrière-plan idéologique, de son substrat dogmatique, de son interprétation personnelle et des intérêts qu'il représente.

Le conférencier a estimé que la clarification des différences entre les différents termes de ce lexique devra paver le chemin aux idées qui en découlent, et que l'élaboration minutieuse de cette terminologie ouvre la voie pour développer une stratégie réussie permettant de faire face à ce phénomène qui pose un défi pour le monde entier. Il a ajouté que la meilleure définition qu'il a trouvée sur l'extrémisme précise qu'il s'agit d'un "terme relatif utilisé pour qualifier des idées ou des actions perçues par ceux qui initient cette expression, comme injustifiées idéologiquement, et que les termes extrémisme et terrorisme sont utilisés presque toujours

par autrui, de sorte qu'aucun groupe ne se dit extrémiste, et qu'aucun parti politique ou religieux ne se qualifie d'extrémiste". Ainsi, il apparaît que le concept d'extrémisme est difficile à définir et qu'il s'enchevêtre avec d'autres expressions identiques, telles que l'outrance et la déviation qui sont des concepts intellectuels à l'instar des types de personnalité et d'autres concepts abstraits, tels que l'intelligence, l'introversion, la dépression, qui se répartissent parmi les êtres humains de façon équitable comme l'illustre la figure (1):

Al-Harithi devait indiquer que le sens commun de l'extrémisme intellectuel est le fait de s'écarter des règles intellectuelles, des valeurs, des normes et des styles de comportement courants dans la société et de s'isoler de la communauté, ou d'adopter des valeurs et des normes différentes, dont la défense peut aller jusqu'au recours à la violence individuelle ou collective, visant à provoquer un changement dans la société, et d'imposer par la force ses points de vue aux autres. Cette position réfère au dogmatisme et au fanatisme qui traduit l'incapacité à accepter ou à tolérer des idées contraires à ses propres idées ou à celles de la collectivité.

Mesurer et juger l'extrémisme et le terrorisme

Dr. Al-Harithi a indiqué que la question épineuse ne réside pas dans les actes terroristes et l'extrémisme violent, dont la responsabilité incombe aux autorités sécuritaires et judiciaires, mais concerne plutôt la façon de mesurer et de juger le concept (d'extrémisme intellectuel) et celui de (terrorisme intellectuel), qui sont deux hypothèses dont la définition est largement entachée par les actions et les comportements de leurs adeptes et les événements traumatisants qui en découlent, outre que celui qui adopte l'idéologie extrémiste ne commet pas forcément des actes terroriste. Al-Harithi souligne à ce propos l'importance de faire la différence entre l'extrémisme intellectuel et l'agression physique, de sorte à pouvoir mesurer de façon scientifique et objective l'extrémisme intellectuel et idéologique indépendamment de l'action et du

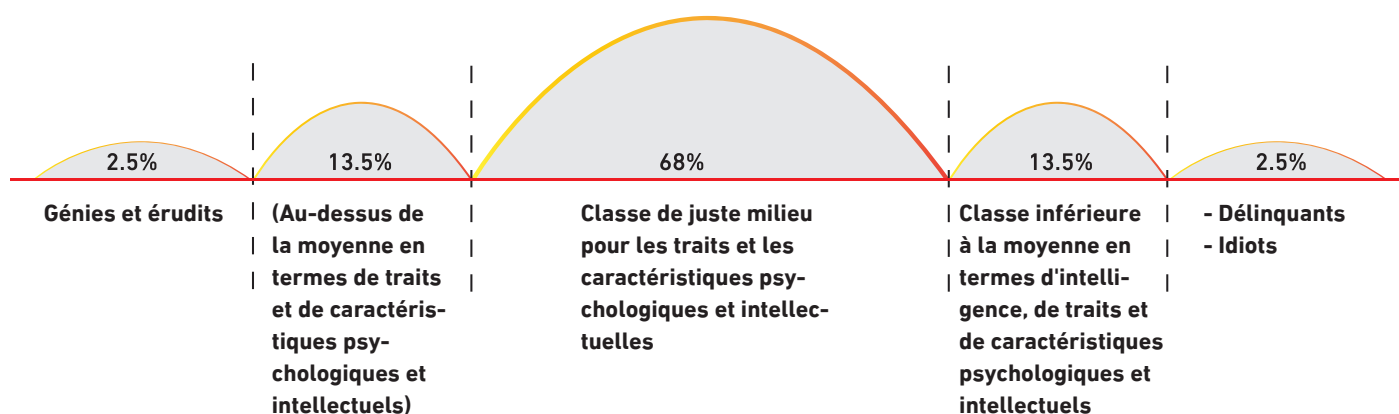


figure (1) Conceptions interdépendantes et analogues au concept d'extrémisme

comportement terroristes, ce qui permet de disposer d'un cadre de référence utile aux États, aux organisations et aux experts de ces questions, comme c'est le cas avec les maladies mentales, les traits de personnalité et les caractéristiques sociales. Les centres de recherche et les universités ont produit de nombreuses normes pour de nombreux domaines, mais le besoin d'avoir des paramètres pouvant mesurer les termes d'extrémisme et de terrorisme intellectuels et idéologiques est toujours de mise et demeure de la plus haute importance.

Al-Harhi a souligné que le magazine "American Psychologist" a réservé en 2017 un numéro spécial intitulé (The Psychology of Terror), pour traiter de cette problématique et expliquer comment les individus deviennent extrémistes, comment prédire qui parmi ces extrémistes deviendra terroriste et comment se produit le passage de la non-violence au stade de l'extrémisme violent puis au terrorisme. Les Chercheurs Clark McCauley et Sophia Moskalkenko ont proposé dans ce numéro intitulé (Comprendre l'extrémisme politique: le modèle pyramidal) un modèle hiérarchique pour faire la distinction entre l'extrémisme idéologique et l'extrémisme en action. Puis McCauley a développé le modèle dans son étude publiée dans le Journal du Terrorisme et de Violence Politique (mai 2020) et a souligné l'importance de distinguer ces deux types d'extrémisme, affirmant qu'il est préjudiciable de faire le contraire, car cela risque de justifier les punitions collectives d'individus ou de groupes simplement pour leur appartenance à une idéologie ou une croyance spécifique.

Al-Harhi a estimé qu'il est impérieux d'instituer des mesures objectives mondiales de l'extrémisme et du terrorisme intellectuels et idéologiques, loin des interprétations et des jugements subjectifs liés aux différents contextes et cadres politiques et religieux.

Pensée, croyance et terrorisme

Dans sa Conférence, Dr. Al-Harhi a analysé les termes pensée, croyance et terrorisme, précisant que la pensée est le résultat d'un processus de réflexion régulier et que toute irrégularité et incohérence intellectuelle s'oppose au concept même de pensée qui se caractérise par l'ordre, la cohérence, la logique et l'argumentation. Quant à la croyance et au dogme, c'est ce à quoi le cœur croit de façon ferme et sincère, que cette croyance soit religieuse ou non. De même, la croyance diffère de la pensée en ce qu'elle est stable et enracinée tandis que la pensée est flexible et relativement stable, de sorte que le penseur peut facilement modifier ses pensées, mais presque jamais ses croyances.

Al-Harhi a conclu à cet égard qu'il est important de faire la différence entre pensée et croyance, notamment pour élaborer des plans, des programmes et des stratégies visant à affronter et combattre le terrorisme, et pour prévenir ses effets destructeurs pour les individus et les sociétés.

Motifs complexes

Al-Harhi a indiqué que les motivations du comportement terroriste sont si complexes que ceux qui commettent l'acte terroriste eux-mêmes ne s'en rendent souvent pas vraiment compte. Il a cité ce que John Horgan, l'une des références mondiales les plus importantes en matière d'études sur le terrorisme, a conclu après avoir interrogé des dizaines d'anciens terroristes sur les motivations de leurs actes terroristes. La réponse choquante était souvent: "Je ne sais pas vraiment", c'est-à-dire que beaucoup de ceux qui ont rejoint les combats en Syrie et en Irak n'ont aucune idée du conflit sectaire dans lequel ils se sont impliqués.

Conclusions

En conclusion de sa Conférence, Dr. Al-Harhi a présenté nombre de déductions importantes, notamment:

- ▶ Le terrorisme est un phénomène complexe et enchevêtré et ne peut être étudié ou analysé en vue de le prévenir ou le combattre, selon une seule approche et partant d'une tendance unique.
- ▶ Il y a confusion et amalgame dans l'étude du phénomène entre les concepts de base tels que l'extrémisme, l'extrémisme intellectuel, la déviation idéologique, le terrorisme intellectuel et le terrorisme physique.
- ▶ La révision de la terminologie de base du phénomène du terrorisme et l'élaboration de mesures scientifiques et objectives des concepts d'extrémisme et de terrorisme intellectuel doivent précéder la planification de programmes de lutte contre l'extrémisme et le terrorisme, car cela évite de s'impliquer dans les détails du phénomène sans l'avoir défini et cerné au préalable; de même que la distinction entre pensée et croyance est une priorité dans cette perspective.
- ▶ Bénéficier de toutes les spécialités et expériences internationales pour établir une approche globale et mondiale du phénomène, loin de toute unilatéralité et de toute forme de fanatisme pour une tendance quelconque ou un contexte local ou régional spécifique. 🌍

Les Technologies de l'Information et des Télécommunications Propagent et Combattent à la fois l'Extrémisme et le Terrorisme!



Grâce à l'apport des Technologies de l'Information et des Télécommunications (TIT), la capacité des terroristes à planifier, exécuter, financer et recruter a doublé. Si les terroristes du siècle dernier étaient vivants, ils enverraient les terroristes du XXIème Siècle. En un seul clic, ces derniers peuvent diffuser leur propagande et leurs idées toxiques à des millions de personnes, transférer des fonds et acheter des armes. En contrepartie, les TIT ont donné aux États, aux gouvernements et aux peuples de meilleures capacités de Lutte Contre l'Extrémisme et le Terrorisme (LCET). Ce double tranchant des TIT entre adeptes et ennemis du terrorisme a fait l'objet du Séminaire, organisé par la CIMCT à son siège, à Riyad, le 03.02.2021, sous l'intitulé: (Rôle des TIT dans la propagation de l'extrémisme et du terrorisme et dans la LCET). Le Séminaire était modéré par le Général de brigade Dr. Mustafa Ibrahim Sweissi, Délégué de la Libye à la Coalition et présenté par le Général de brigade Rashid Al Dhaheri, Délégué des ÉAU et le Général de brigade Tawfiq Al Batayneh, Délégué du Royaume Hachémite de Jordanie.

L'événement a focalisé sur deux thèmes: La relation entre les TIT et les organisations terroristes et les méthodes de LCET grâce aux TIT.

La convergence entre le terrorisme et le monde informatique repose sur la menace de paralyser les ordinateurs et les réseaux informatiques et de détruire les informations stockées pour terroriser les gouvernements et les peuples et atteindre des objectifs politiques et sociaux. Le concept d'extrémisme sur Internet se définit comme étant (l'utilisation d'Internet et de tous les services électroniques qui lui sont associés pour créer des sites Web et diffuser et recevoir les services facilitant la transmission de contenus intellectuels qui nourrissent l'extrémisme intellectuel et incitent à la violence).

Les organisations terroristes ont recours au Web pour les avantages qu'il leur offre en termes de vitesse, d'impact et d'efficacité, en plus du faible coût, de la facilité d'utilisation, du manque de contrôle et des difficultés à y traquer le crime. Internet -les médias sociaux en tête- sont devenus le moyen favori pour les organisations terroristes pour diffuser leur propagande, organiser leurs opérations et recruter de nouveaux éléments.

Ces organisations se sont concentrées sur les médias sociaux qui jouissent de nombreux aspects attractifs dont notamment :

- ◆ Présentation artistique innovante
- ◆ Services passant outre le blocage des sites
- ◆ Mises à jour permanentes du contenu
- ◆ Coordination entre les sites
- ◆ Abondance des contenus audio-visuels
- ◆ Offres d'alternatives d'accompagnement

Millions de messages, sites Web et tweets

Le Séminaire a révélé que les organisations terroristes ont créé 270000 sites Web extrémistes et 16 réseaux médiatiques en plusieurs langues et publié sur YouTube 9 millions de clips en anglais, plus de 47 mille en français, plus de 20 mille en russe et plus de 12 mille en arabe. 70% des partisans de groupes extrémistes publient 2612 tweets par heure (93% en textes), et certains comptes sont mis à jour toutes les 5 minutes.

Le Colloque devait débattre ensuite l'utilisation de Twitter par Daech pour mener sa bataille idéologique, promouvoir son prétendu État Islamique (Daech), soutenir les loups solitaires,

recruter des partisans, améliorer l'image des kamikazes morts. L'organisation utilise aussi la plate-forme pour détecter les sympathisants sur la base de leurs commentaires, et leur envoyer des messages privés pour les persuader de se joindre à elle, commettre un acte terroriste ou fournir de l'assistance à des actes terroristes dans leurs pays.

Faire face au terrorisme sur le Web

Le second thème de la Conférence traitait de la lutte contre le Cyber-terrorisme et des moyens les plus importants de lutter contre ce type de terrorisme en bloquant les sites Web, en légiférant des lois et des sanctions, en créant des départements de lutte contre le «terrorisme électronique» relevant des systèmes sécurité, et en développant les capacités gouvernementales pour faire face aux Cyber-menaces.

Le Colloque a évoqué le rôle de l'ONU dans la LCET via Internet, en publiant une série de décisions à travers son Assemblée Générale face à l'utilisation non pacifique des TIT, selon trois niveaux: L'alerte et la sensibilisation, la prise de décisions et l'élaboration de stratégies de lutte contre les activités terroristes. L'ONU a lancé la Stratégie mondiale antiterroriste en 2006, qui appelait à coordonner les efforts aux niveaux international et régional pour lutter contre le terrorisme dans tous ses formes et manifestations sur Internet. Le Conseil de Sécurité a publié les Résolutions n° 1373 en 2001 et n° 1566 en 2004, obligeant les États Membres à prendre des mesures législatives et non législatives pour lutter contre le terrorisme et mettre en œuvre les conventions et protocoles internationaux, relatifs au terrorisme, ainsi que les résolutions 1624 de 2005 et 1963 de 2010, appelant les États Membres à travailler ensemble pour empêcher les terroristes d'exploiter le TIT.

Coopération Internationale de LCET dans le Cyber-espace

Sur le plan international, en plus de l'ONU, les efforts des États-Unis, ont représenté un développement qualitatif pour faire face à la menace du terrorisme et de l'extrémisme via Internet, en diversifiant les moyens et les méthodes législatifs, techniques, militaires ou sécuritaires.

Dans le même contexte, le Groupe européen a pris des mesures visant à protéger le réseau Web contre les infiltrations terroristes, en promulguant une législation qui fournit des capacités préventives contre la survenance de tels actes et permet de poursuivre leurs auteurs.

La capitale saoudienne Riyad a accueilli la Conférence internationale sur la lutte contre le terrorisme en 2005, qui a recommandé les niveaux les plus élevés de coopération et de coordination entre les pays dans la lutte contre le terrorisme, et la création d'un organe international conjoint, en coordination avec les Nations Unies, pour échanger les informations et les expériences entre les pays, et pour développer les méthodes, les formations, les législations, les technologies et les capacités nationales de lutte contre le terrorisme.

Efforts arabes

Le Séminaire a examiné les efforts de LCET sur le Web au niveau du monde arabe, dont le projet de stratégie arabe de LCET, la Convention Arabe contre le terrorisme en 1998, l'Accord arabe sur la lutte contre les crimes de TIT, les recommandations de la 18ème

Conférence arabe du Conseil des Ministres Arabes de l'Intérieur en 2015, appelant à réduire la propagation du discours extrémiste et sectaire et à lutter contre le terrorisme.

Au niveau national, le Colloque a passé en revue les efforts de LCET dans le secteur du TIT du Royaume d'Arabie Saoudite et des ÉAU. L'Arabie Saoudite a élaboré une stratégie pour faire face aux déviations idéologiques de la société saoudienne en 2007 et des plans performants pour vérifier les soupçons de terrorisme sur Internet et sur les médias sociaux. Elle également publié la loi de Cyber-criminalité en 2007 et lancé le Centre Etidal en 2017.

Les ÉAU ont créé les Centres Hedaya (2012) et Sawab (2015), développé l'Initiative Internationale, incriminant le terrorisme électronique, en 2017, et publié nombre de lois dont:

- ◆ Loi sur la "coopération judiciaire internationale en matière pénale" (2006).
- ◆ Loi sur la lutte contre les crimes terroristes (2014).
- ◆ Loi de lutte contre le blanchiment d'argent et le financement du terrorisme.
- ◆ Loi fédérale n° (5) de 2012, contre les délits liés aux technologies de l'information, et ses amendements en 2016 et 2018.

Conclusions et Recommandations

Le Symposium a conclu que le terrorisme électronique est lié au progrès scientifique et qu'il est donc difficile d'instituer des méthodes infaillibles pour protéger le système d'information contre les infiltrations, la plupart des pays et des institutions continuant à adopter des mesures électroniques pour faire face à toute intrusion terroriste. Il a formulé des recommandations, dont:

- ◆ Diffuser la culture préventive et éduquer la société sur les dangers du terrorisme en général et du cyber-terrorisme en particulier.
- ◆ Promulguer des lois pour combler les lacunes liées au crime du terrorisme électronique à la lumière du développement technologique rapide.
- ◆ Créer un système juridique international sous l'égide du monde islamique, chargé de coordonner les efforts de lutte contre le terrorisme électronique, en tenant compte des lois et des législations en vigueur aux Nations Unies.
- ◆ Être fin prêt à repousser les attaques électroniques et élaborer de scénarios de risques potentiels et de méthodes de lutte.
- ◆ Sécuriser les réseaux d'information, les systèmes de communication et les sources d'énergie, physiquement (durabilité des bâtiments, mesures de sécurité, gardes) et techniquement (formation, programmes de protection).
- ◆ Soutenir la recherche scientifique liée à la sécurité des TIT, créer des programmes de protection nationaux et essayer de se passer des logiciels de cryptage importés.
- ◆ Former le personnel de sécurité aux techniques du terrorisme électronique et aux méthodes de surveillance et d'enquête.
- ◆ Soutenir les États Membres islamiques aux capacités matérielles et techniques limitées de lutte contre le terrorisme virtuel. 🌟

Lutte contre le blanchiment d'argent et le financement du terrorisme

Cours de formation



Le Centre de la CIMCT à Riyad a organisé, en coopération avec l'Académie Financière, deux cours de formation sous l'intitulé «Lutte contre le blanchiment d'argent et financement du terrorisme», auxquels ont participé deux groupes de stagiaires, fin janvier et mi-février 2021, animés par le formateur Hassan Khalaf Al-Faouri, secondé par Hatem Al-Qahtani. Les stages visaient à apprendre aux stagiaires les opérations de lutte contre le blanchiment d'argent (BA), les crimes financiers, les indicateurs de blanchiment d'argent, le financement du terrorisme (FT) et les moyens de détecter ces crimes.

Crime de blanchiment d'argent

Le formateur a indiqué que le blanchiment d'argent vise à dissimuler la véritable source des fonds acquis par des moyens illégaux pour les rendre légitimes et les injecter dans le cycle économique et pouvoir les transférer à travers les frontières internationales et les canaux des institutions financières légales. La relation entre le BA et la corruption est très étroite, car les régimes à défaut de transparence et de surveillance ont des niveaux élevés de BA et de corruption, selon le Rapport Mondial sur la Corruption de l'Organisation Internationale de Transparence.

Le formateur a révélé que les opérations de blanchiment d'argent constituent désormais une menace mondiale, la part de l'argent blanchi étant estimée entre 2% à 5% du PIB mondial, soit entre 800 milliards et 2 trillions de dollars par an, portant notamment sur ce qui suit:

- ▶ Commerce de drogue.
- ▶ Contrebande et commerce d'armes.
- ▶ Contrebande de marchandises.
- ▶ Prostitution.
- ▶ Pots-de-vin et corruption administrative.
- ▶ Vols ou détournements de fonds publics ou privés.
- ▶ Contrefaçon.

- ▶ Fraude et escroquerie.
- ▶ Évasion fiscale.
- ▶ Traite d'êtres humains.
- ▶ Extorsion et kidnapping contre rançons.

Éléments du crime et effets

Le formateur a présenté les deux éléments du crime de BA: Le premier est matériel et comprend la localisation du crime (fonds, produits et revenus), et le comportement (possession, acquisition, utilisation, transfert et dissimulation). Le second est d'ordre moral et comprend «l'intention criminelle».

Quant aux étapes des opérations de BA, elles comportent d'abord l'étape de dépôt ou de substitution, destinée à introduire des fonds résultant d'activités illégales dans le système financier bancaire. Puis l'étape du camouflage ou de la couverture, à travers le transfert de ces fonds pour dissimuler leur origine illicite (transferts bancaires, achats et ventes d'investissements et de contrats d'assurance). Puis intervient la phase de fusion réintroduisant ces fonds dans le système financier, en achetant des actifs, des actions, des biens immobiliers ou des matières premières de valeur, ou en les investissant dans des projets. Le processus de BA peut ne pas passer par les étapes précédentes (dépôt, camouflage, fusion) et se dérouler en une ou deux étapes, selon les circonstances et le type d'opérations de blanchiment.

Le formateur a analysé les effets négatifs des opérations de BA qui affaiblissent la capacité de l'État à mettre en œuvre ses politiques économiques, perturbent la croissance économique et le marché des changes, minent la confiance dans les banques, affectent les bourses et les marchés financiers et augmentent les niveaux d'inflation. Au niveau politique, il est responsable de la propagation de la corruption politique et administrative, des abus de pouvoir, d'atteinte à la réputation de l'État, et du renforcement du pouvoir des blanchisseurs d'argent dans l'État et leur impact sur les législations et les lois. Sur le plan social, les opérations de

blanchiment d'argent aggravent le problème du chômage, de la corruption au travail et de l'achat de soutiens.

Initiatives internationales

Ensuite, Al-Faouri a discuté des initiatives internationales dans le domaine de la lutte contre le BA, avec en tête le Groupe d'Action Financière (GAFI), créé en 1989 par le Groupe des sept pays industrialisés, et qui comprend désormais 37 pays membres et deux organisations régionales: La Commission Européenne, et le CCG, le GAFI, a émis 40 recommandations qui constituent les normes minimales pour lutter contre le BA et le FT, et qui ont été adoptées par plus de 180 pays. En juin 2019, le Royaume d'Arabie Saoudite est devenu le premier pays arabe à rejoindre le GAFI.

Le Comité de Bâle a publié en 1988 un document de principes sur la prévention de l'utilisation du système bancaire aux fins des délits de blanchiment d'argent.

Financement du terrorisme

Le financement du terrorisme (FT) désigne les opérations de collecte de fonds destinés à être utilisés en tout ou en partie dans la mise en œuvre d'actions visant à causer la mort ou des blessures graves à une personne, terroriser la population, ou contraindre un gouvernement ou une organisation internationale à faire ou s'abstenir de toute action.

Le formateur estime que le FT est un type de blanchiment d'argent, mais il en diffère par le fait que l'argent initial peut être légitime et régulier. Les montants de FT sont généralement modestes et ne suscitent pas de suspicion. Les activités terroristes sont souvent menées à des fins politiques ou idéologiques. Les fonds peuvent être transférés à travers le système bancaire via les transferts ou en contrebande à travers les frontières.

Modèles de blanchiment d'argent et de financement du terrorisme

Le formateur a énuméré certains modèles liés au BA et au FT dont notamment:

- ◆ **Transfert:** Services de transfert alternatifs, (tels que les hawala, obligations), moyens informels de transfert basés sur des réseaux de confiance pour transférer de l'argent, et fonctionnant souvent en parallèle avec le secteur bancaire traditionnel. Ces services ne sont pas réguliers, et les blanchisseurs d'argent et les financiers terroristes les utilisent pour transférer de l'argent sans être poursuivis et pour dissimuler l'identité de ceux qui contrôlent cet argent.
- ◆ **Agencement:** Diverses opérations (dépôts, retraits et transferts), impliquant souvent de nombreuses personnes et de multiples transactions de faible valeur, sur divers comptes pour éviter d'éveiller les soupçons des institutions financières.
- ◆ **Change de devises:** Cette méthode facilite la contrebande d'argent entre les pays et profite du relâchement des institutions de change pour réduire le risque de démasquer ces transactions (dont l'achat de chèques de voyage pour transférer de l'argent entre pays).
- ◆ **Contrebande de monnaie:** Déplacer secrètement à travers les frontières les fonds pour éviter les procédures de divulgation des trésoreries.
- ◆ **Cartes de crédit et chèques:** Pour accéder à l'argent déposé sur des comptes bancaires, souvent dans un autre pays.
- ◆ **Achats d'actifs:** Investir l'argent sale dans l'achat de biens

coûteux (immobiliers, voitures, actions), échangeables aisément et nécessitant moins de contraintes susceptibles de démasquer leurs origines.

- ◆ Virements télégraphiques: Transferts électroniques entre banques, souvent vers un autre pays.
- ◆ Blanchiment commercial, dont la falsification de factures et le financement de biens pour déjouer la transparence financière.
- ◆ Investir sur les marchés financiers, en achetant des obligations négociables.
- ◆ Investissement dans les entreprises, étape majeure de blanchiment combinant le produit illicite à des fonds commerciaux légitimes pour dissimuler la source de ces fonds.
- ◆ Utilisation d'institutions fictives, pour dissimuler l'identité des personnes qui contrôlent les fonds.
- ◆ Recours aux intermédiaires, pour cacher l'identité des propriétaires de l'argent illicite.
- ◆ Recours aux prestataires de services professionnels, tels que les avocats, comptables et courtiers.

Indicateurs de suspicion

Pour aider les stagiaires à identifier les opérations de BA et de FT, le formateur a fourni des indicateurs de suspicion dont:

- ◆ Indicateurs relatifs aux clients: Comme de fournir de fausses données, difficiles à vérifier ou suspectes, ou que le montant de l'opération ne soit pas proportionné à la nature du travail.
- ◆ Indicateurs liés à la nature du mouvement de compte: Comme d'effectuer des virements fréquents, importants et récurrents, suivis de retraits ou de virements, ou que la valeur ou le type de transactions soient disproportionnés à la nature du compte, ou d'avoir une activité soudaine sur un compte inactif.
- ◆ Indicateurs liés aux transactions financières: Comme l'achat ou la vente de titres dans des circonstances ou situations anormales, ou le remboursement de prêts à des clients contre des actifs de source inconnue.
- ◆ Indicateurs liés au comportement du suspect: Comme de ne pas traiter directement avec les employés de la banque et préférer traiter avec les guichets automatiques, ou d'avoir plusieurs comptes bancaires, ou bien d'annuler la transaction en cas de demande par la banque d'informations importantes.

Quant aux indicateurs de suspicion liés au FT, notons ce qui suit:

- ◆ Transfert depuis ou vers des pays zones de troubles politiques ou sécuritaires.
- ◆ Valeur des transactions non proportionnelle aux informations, activités, revenu, mode de vie et comportement du suspect.
- ◆ Traiter avec des personnes ou des entités sans lien visible avec le suspect.
- ◆ Interagir avec plusieurs personnes de nationalités différentes.
- ◆ Détenir une grande somme d'argent en liquide à travers les frontières.
- ◆ Transfert à nombre de personnes dans différents pays sans raison apparente.
- ◆ Inscription du nom du suspect ou du bénéficiaire sur les listes des Nations Unies. 🌐

SÉCURITÉ DES SMARTPHONES AU SIÈGE DE LA CIMCT



Le Centre de la CIMCT à Riyad a organisé une conférence intitulée: «Sécurité des Smartphones», présentée par Dr. Ihab bin Abdulaziz Al-Rasan, Professeur assistant des Technologies d'Internet et des Systèmes Distribués, le mardi 23 février 2021. Le Conférencier a souligné au début l'importance de la sécurité des téléphones mobiles, en particulier les Smartphones, considérés actuellement comme des ordinateurs portables qui permettent aux usagers d'accéder aisément à Internet, télécharger des applications et des jeux et stocker leurs informations personnelles. Les internautes doivent protéger leurs téléphones tout comme ils protègent leurs ordinateurs personnels ou portables. Une grande partie de nos données sur ces appareils est vulnérable au piratage et à l'espionnage, et comme ils sont portables, ils sont également vulnérables à la perte et au vol.

Cyber-attaques

Selon les statistiques de Kaspersky, le nombre de cyberattaques dans la région du Moyen-Orient, Turquie et Afrique (META) a atteint 1,5 million d'attaques par jour et 575 millions d'attaques en un an. L'Arabie Saoudite a connu une augmentation significative de ces attaques, avec 387% d'attaques de rançons, 11% d'infections de logiciels malveillants, 43% d'attaques de chevaux de Troie et 4% d'attaques de logiciels malveillants.

Une étude analytique menée par Kaspersky a révélé que les attaques violentes de Phishing au deuxième trimestre de 2019 ont atteint plus de (973.000) attaques au Royaume d'Arabie Saoudite, (617.347) aux Émirats Arabes Unis, (492.532) en Égypte, (193.379) au Sultanat d'Oman, (128.356) au Qatar, (106.245) au Koweït et (67.581) au Bahreïn.

On sait que le Phishing est l'un des types les plus anciens d'attaques numériques connu sous le nom d'ingénierie sociale, et le plus flexible, utilisé de maintes façons et à des fins multiples pour piéger les internautes.

Avec la généralisation des téléphones mobiles et intelligents et des appareils en général, l'intérêt des Cyber-criminels ou des pirates informatiques s'est accru pour subtiliser les informations sensibles des internautes, planter des logiciels malveillants et de Phishing, entre autres. Cent millions d'attaques ciblant les appareils intelligents ont été détectées dans le monde, et les statis-

tiques de piratage électronique montrent que pour l'année 2019, plus de 24.000 applications malveillantes pour Smartphone ont été bannies chaque jour des Appstores. En outre, l'étude de test de sécurité Viracode a révélé qu'environ 59% des entreprises ont constaté une augmentation des logiciels malveillants ciblant les téléphones mobiles non sécurisés.

Entre le root et le jailbreak

L'utilisation des outils «root» sur les appareils Android et de «jailbreak» sur les appareils Apple sont les types d'attaque les plus courantes contre les Smartphones. Le «rootage» accorde les pouvoirs de super utilisateur sur le système Android, et en obtenant ces pouvoirs, l'utilisateur pourra assumer de nombreuses fonctionnalités, telles que d'installer divers thèmes, améliorer les performances du système et augmenter la durée de vie de la batterie, mais en utilisant les outils de «root», les applications installées peuvent facilement accéder aux données de l'utilisateur et installer certains programmes malveillants.

Quant au processus de «jailbreak» pour le système «IOS» des téléphones Apple, il surmonte les difficultés de placer des logiciels espions dans les appareils iPhone et iPad, de sorte que le pirate informatique doit «rompre la protection» de l'appareil avant de pouvoir installer des applications qui ne sont pas approuvés par l'entreprise.

L'utilisateur doit s'assurer que son appareil n'est pas en "jailbreak", le mettre à jour l'appareil et utiliser des logiciels tels que SnapStats, qui l'informe si son appareil iPhone est soumis au "jailbreak"!

Quant au réseau privé virtuel VPN, il fournit un tunnel crypté sur Internet, connectant l'appareil de l'utilisateur au serveur de l'un de ses réseaux, dit (tunnel). Contrairement à d'autres trafics de navigation cryptés, tels que le protocole «https», le VPN dissimule tous les services, protocoles et contenus. Étant donné que le trafic de navigation passe par un serveur VPN, il n'a besoin que d'accéder au serveur intermédiaire pour analyser l'activité des utilisateurs, aussi, est-il important de choisir soigneusement son service VPN et d'utiliser de nombreux VPN, car la répartition du trafic de données limite les dégâts causés par un appareil piraté.



Ingénierie sociale

Quant à l'ingénierie sociale, il s'agit de tentatives d'acquérir des informations sur un système ou un réseau spécifique par le biais de méthodes sociales, telles que de causer avec les employés des sociétés, ou à travers un e-mail, ou une commande piège, permettant, au pirate, au cas où la victime ouvre le lien pour achever les procédures, d'accéder aux données de l'appareil dont les informations bancaires. Pour se protéger contre l'ingénierie sociale, le Conférencier a présenté nombre de mesures dont l'établissement de politiques de sécurité strictes et la formation des employés.

Ciblage des personnalités de premier plan

Les comptes Twitter de personnalités éminentes ont fait l'objet de piratage électronique dans le cadre d'une escroquerie liée au Bitcoin, notamment: Elon Musk, Jeff Bezos, Bill Gates, Barack Obama, Joe Biden et Kanye West. "Tout le monde me demande de rendre la pareille, envoyez-moi 1000 dollars, et je vous enverrai 2000 dollars", disait Bill Gates dans son tweet. Twitter a déclaré qu'une attaque "coordonnée" ciblait ses employés par l'intermédiaire de parties en possession de "détails sur la saisie des systèmes et outils internes" de l'entreprise, et a utilisé ces détails pour contrôler de nombreux comptes accrédités de célébrités, afin d'envoyer des tweets en leurs noms. De même, le service Cloud a été piraté et des photos de célébrités volées. Toutes ces opérations ont eu lieu à cause d'un virus sur l'ordinateur des clients, ou de leur téléchargement d'une application factice sur leurs appareils Android.

Piratage de comptes bancaires

Certaines fraudes ont été détectées par nombre de clients du service Al-Mubasher de l'une des banques. Soyez donc attentifs aux messages contextuels qui vous demandent de saisir le numéro de votre téléphone portable, le type de votre mobile, votre numéro de carte de crédit ou un quelconque mot de passe, car les applications bancaires ne vous demandent pas de saisir de telles informations lors de votre utilisation du service individuel Al Mubasher.

Méfiez-vous d'une application appelée «Al Rajhi mToken» ou «mToken» ou «Alrajhicerificate», car il s'agit d'une application factice qui transfère les messages qui vous sont envoyés par la banque, y compris votre mot de passe temporaire, pour entrer dans le service personnel d'Al Mubasher.

Manipulation sécurisée

Les médias sociaux peuvent être offensants et nuisibles lorsqu'ils servent à répandre des mensonges, des illusions et des rumeurs, cultiver la haine, s'attaquer aux autres, porter atteinte à l'honneur et à la dignité de certaines personnes, violer la vie privée des gens, republier des clips offensants, usurper les identités, et toutes formes d'utilisation abusive de ces moyens.

Comment savez-vous que votre téléphone est piraté?

Dr. Al-Rasan a précisé que les méthodes de piratage passent souvent par des applications non sécurisées, car le logiciel malveillant fonctionne en cachette sans que l'utilisateur ne s'en rende compte, ou le remarque dans la liste des applications en cours d'exécution. Ces logiciels peuvent utiliser les Smartphones comme outils à des fins publicitaires et consommer une grande partie de la charge de l'appareil pour accomplir leurs tâches. Vous pouvez savoir que votre Smartphone est piraté selon nombre d'indicateurs:

- ▶ Utilisation lente du téléphone.
- ▶ Lenteur soudaine du téléphone.
- ▶ Applications fermées fonctionnant en arrière-plan.
- ▶ Le dossier de l'expéditeur contient des messages qu'il n'a pas envoyés.
- ▶ Modification inopinée de l'interface de votre téléphone.

Protégez votre Smartphone

À la fin de la Conférence, Dr. Al-Rasan a donné des conseils pour protéger les Smartphones:

- ▶ Placer des mots de passe pour accéder au téléphone.
- ▶ S'assurer des autorisations des applications, lors de leur téléchargement.
- ▶ Activer la fonction de validation à deux facteurs.
- ▶ Lire les instructions et la politique de confidentialité avant de télécharger l'application et lui permettre d'accéder à vos données personnelles.
- ▶ Utiliser des fonctionnalités biométriques, telles que les empreintes digitales et la reconnaissance faciale.
- ▶ Éviter de télécharger des logiciels anonymes.
- ▶ Mettre à jour le système d'exploitation, les logiciels installés et les logiciels de sécurité.
- ▶ Conserver une copie de sauvegarde de vos données pour les protéger du risque de perte, vol ou cryptage des logiciels de rançons.
- ▶ Installer un logiciel antivirus.
- ▶ Activer la fonction d'effacement des données à distance en cas de vol ou de perte de l'appareil.
- ▶ Revoir les applications installées sur votre téléphone pour s'assurer qu'aucun logiciel suspect n'est installé à votre insu.
- ▶ Ne pas partager pas les mots de passe ou le code PIN de votre téléphone portable avec qui que ce soit, même les gens dignes de confiance.
- ▶ En accédant à l'Internet, sur un réseau sans fil, s'assurer que le réseau est crypté et que vous faites confiance à sa source, qu'elle soit interne ou externe. 🌐

MAGAZINE ALTAHALOUF DANS DE NOUVEAUX ATOURS

6ème Numéro: Richesse du contenu et plaisir de la forme



Le 6ème Numéro du Magazine "Altahalouf" est paru début février 2021, en trois langues: Arabe, anglais et français. Il se distingue par son nouveau look et son identité visuelle et fournit au lecteur de solides connaissances combinant la force du contenu et la qualité du design, renforçant le progrès continu du périodique, que ce soit au niveau de la diversité de ses thèmes, la profondeur de ses approches, la bonne sélection de ses sujets, son identité visuelle authentique ou le raffinement de sa présentation. Ce niveau enregistré est dû à l'effort incessant déployé par les responsables de la Coalition, dirigés par le Superviseur Général du Magazine, Son Excellence le Major Général Mohammed bin Saïd Al-Mughaidi, le Secrétaire Général, désigné, de la CIMCT.

Ce clin d'œil nous permettra de faire le tour rapide des différents Chapitres, thèmes et nouveautés de cette nouvelle parution innovante.

Diversité des sujets et des auteurs

Le 6ème Numéro du Magazine se caractérise par la diversité de ses Chapitres, thèmes et matériaux, ainsi que par la diversité de ses écrivains et de leurs pays, le nombre d'auteurs atteignant 18 écrivains de 14 pays et de différents continents, tous hautement qualifiés et expérimentés dans le domaine de leur spécialité, outre les articles conçus et préparés par le comité de rédaction du magazine.

Thèmes du numéro

Les thèmes du numéro se répartissent sur les Chapitres fixes comme suit:

Avis: Il contient cinq articles: Comment la pensée se forme et se radicalise, écrit par Prof. Zayed Al-Harithi, Delegue du Royaume d'Arabie Saoudite à la CIMCT dans le domaine intellectuel; Sauver la femme victime des griffes de l'extrémisme et du terrorisme par Bedai Sherif Mokhtar Palari, Chercheur sur les questions d'extrémisme à l'Université de Diffa au Niger; Le pouvoir des idées, la diplomatie publique et le terrorisme par Dr. Al-Sadiq Al-Faqih, Professeur de Sciences Politiques à l'Université de Khartoum; Des motifs sociaux à l'échappatoire religieuse, causes de la radicalisation des jeunes au Niger, par Dr. Umaru Makama Bawa, Professeur d'Anthropologie Politique et Chercheur sur l'Islam Contemporain et les Conflits entre Sociétés; Pour une éducation réconciliée et préventive dans le Sahel, par M. Khouma Seydou, Inspecteur et Chercheur en Sciences de l'Éducation.

Initiatives internationales: Confronter l'extrémisme violent avec les multimédias créatifs, par Dr. Dzeneta Karabegovic Chercheuse Bosnienne en Relations Internationales et en Sociologie Politique Internationale et Comparée.

Indicateurs: Terrorisme selon l'Indice Mondial (GTI 2020): Menaces qui se dissipent et défis renouvelés.

Analyses: Il comprend 2 articles: Impact de l'extrémisme violent au Mali et dans le Delta Central, par l'écrivaine Yida Seydou Diall, Chercheuse sur les questions d'extrémisme violent au Sahel Central; Changer les visions pour gérer les conflits, modèle du peuple des Mapuche d'Argentine, par Dr. Mariano Jorge Gancedo, Professeur d'Anthropologie et Chercheur sur les conflits.

Dossier du numéro: Il contient 5 articles: Le terrorisme comme acte de communication, les terroristes ciblent le public par la peur et la terreur avant de cibler leurs victimes par le meurtre, et Médias terroristes et terrorisme médiatique par Ashour bin Ibrahim Al-Juhani, Rédacteur en Chef du Magazine; Sémiologie de la violence, signification des signes, symboles et images dans les médias terroristes par Dr. Ammar Ali Hassan, Romancier et Chercheur en Sociologie Politique; Terminologie du terrorisme dans le domaine médiatique, entre arbitraire et nécessité d'un dictionnaire unifié par l'écrivain Omanais A. Mohammed bin Saeed Al-Futaisi, Chercheur Universitaire en Politiques Criminelles contre le Terrorisme; Médias et lutte contre le terrorisme, responsabilité et impact par Prof. Howayda Mostafa, Doyenne de la Faculté des Médias de l'Université du Caire.

Expériences: Expérience Camerounaise de lutte contre le terrorisme, de la confrontation et de l'endiguement à l'intégration et à la réhabilitation, par Prof. Ousmanou Adama, Chercheur spécialisé dans les identités ethniques et religieuses de la région du bassin du Tchad.

Critiques: Sources de l'équilibre dans les thèses intellectuelles du Chercheur, par Porf. Mohammed Al-Subaihi, Délégué du Royaume d'Arabie Saoudite à la CIMCT dans le domaine médiatique.

Études: Les tweets de la CIMCT sur Twitter, étude et analyse, par le colonel Abdullah Muhammad Shadi, représentant de la République du Yémen à la CIMCT.

Enjeux: Migration internationale et terrorisme mondial, par Dr. Idris Al-Kanbouri, Chercheur et écrivain, Directeur du Centre du Futur pour la Recherche et le Savoir à Rabat.

Sous les projecteurs: Organisation des Gardes de la religion, par Dr. Mohammed Aref Al-Adhamat, Chercheur sur les questions de terrorisme et ancien Directeur du Centre Jordanien pour l'extrémisme.

Islam authentique: Commandements de l'Islam, religion de justice, de tolérance et de modération, par Salim Alwan Al-Husseini, Secrétaire Général de Dar Al-Fatwa, Conseil Suprême Islamique d'Australie.

Actualités: Coup d'envoi du programme intellectuel et médiatique de la CIMCT avec deux Conférences: Facteurs d'adhésion des

jeunes aux organisations d'extrémisme violent, présenté par Dr. Mansour Al-Qarni, Directeur du Département Idéologique; Formulation de l'anti-discours violent, présenté par Dr. Mohammed Al-Subaihi, Délégué médiatique Saoudien à la Coalition.

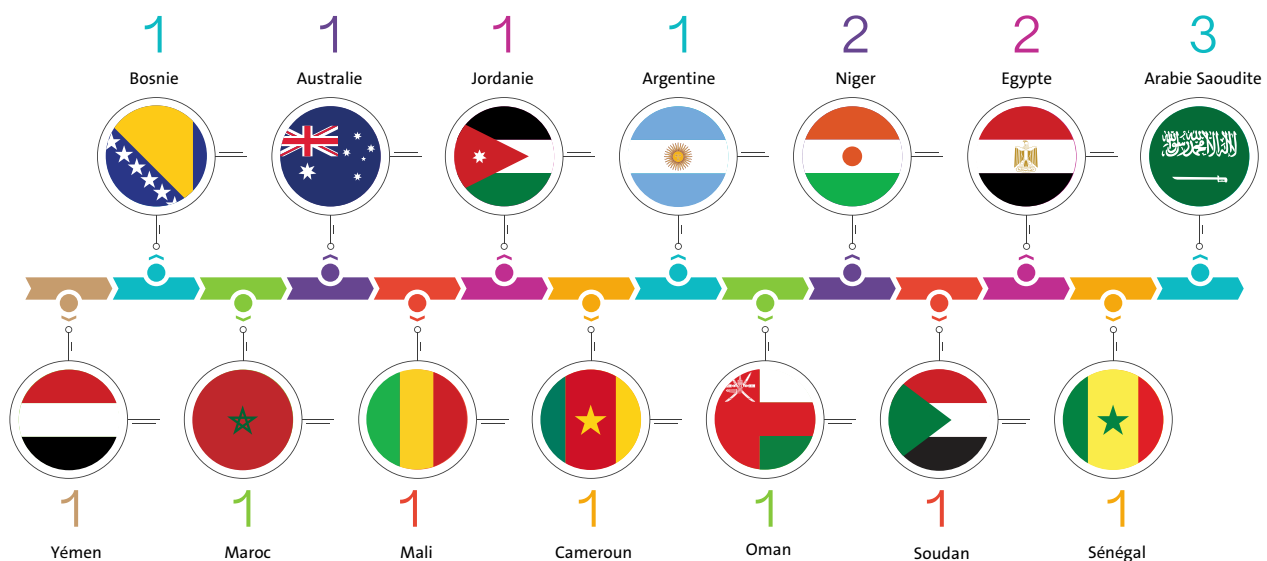
Fenêtres: Il contient 5 articles: Washington retire le Soudan de la liste du terrorisme et classe "Saraya Al-Mukhtar" organisation terroriste; un Rapport international met en garde contre les répercussions du Coronavirus sur les efforts de lutte contre le **terrorisme**: L'Europe soutient les mesures de lutte contre le terrorisme; Le Pakistan arrête le chef d'un groupe extrémiste pour financement du terrorisme; Craintes d'infiltration de l'extrême droite dans l'armée en Allemagne et aux États-Unis.

Éditorial: Pour un pacte d'honneur, suivi médiatique du terrorisme, rédigé par le Rédacteur en Chef.

Il est important de se référer à ce niveau d'évoquer la méthodologie suivie pour sélectionner les articles du Magazine, soumis à un cycle éditorial rigoureux, selon l'approche en vigueur dans les grandes revues scientifiques. Les documents ne publiés qu'après avoir été évalués, révisés et corrigés, puis vérifiés et approuvés, en termes de validité et de qualité des idées, du contenu et de la richesse du matériel, de l'exactitude des significations et la précision des idées, en plus de la qualité de la langue et du style et la rigueur de la formulation.

Réalisation artistique et design

L'affinement ne se limite pas au seul contenu mais porte également sur le design et la réalisation, en commençant par la couverture extérieure, tout en passant par le design intérieur pour finir avec les images et les formes. Un nouveau modèle de conception a été adopté en 2021, pour nombre de chapitres, dont: Avis, Points de vue et Éditorial. Les photos et les images soigneusement choisies expriment le contenu des articles et de nombreuses images ont été rééditées pour correspondre aux idées et aux thèmes des articles, conférant à la revue une élégance particulière et un raffinement concerté. L'harmonie des couleurs, loin des stéréotypes traditionnels, place ce sixième numéro de "Altahalouf", dans un univers spacieux du plaisir visuel, susceptible de convier le lecteur au plaisir de lire, ce qui est notre objectif ultime. 🌸



Diversité géographique des auteurs participant au 6ème numéro du magazine Altahalouf

CÉLÉBRATION DE LA FÊTE NATIONALE DE LA RÉPUBLIQUE DE GAMBIE



Les Délégués de la République de Gambie ont célébré au Centre de la CIMCT à Riyad, le 18 février 2021, la journée nationale de Gambie qui coïncide avec l'anniversaire de son indépendance, obtenue en 1965. La cérémonie a été suivie par le Secrétaire Général, désigné, de la CIMCT, le Major Général Mohammed bin Saïd Al-Mughaidi, le Commandant Militaire de la Coalition, le Général, à la retraite, Raheel Sharif, les Délégués des États Membres et le personnel de la Coalition. 🌸

LE CENTRE DE LA CIMCT CÉLÈBRE LA JOURNÉE NATIONALE DE L'ÉTAT DE KOWEÏT



Le Délégué de l'État du Koweït au sein de la CIMCT a célébré, le 25 février 2021, la 60ème journée nationale du Koweït en présence du Secrétaire Général, désigné, de la Coalition le Major Général Mohammed bin Saïd Al-Mughaidi, du Commandant Militaire de la Coalition, le Général, retraité, Raheel Sharif, des Délégués des États Membres et du personnel de la Coalition. 🌸

LE SECRÉTAIRE GÉNÉRAL REÇOIT LA DÉLÉGATION DE LA FACULTÉ DE COMMANDEMENT ET D'ÉTAT-MAJOR



Le Secrétaire Général, désigné, de la CIMCT, le Major Général Mohammed bin Saïd Al-Mughaidi a reçu le 21 février 2021 une délégation de la Faculté de Commandement et d'État-Major des forces armées, dirigée par le Major Général Mohammed bin Jadooa Al-Ruwaili, Commandant de la Faculté et Directeur de l'Université de la Défense Nationale.

La délégation a été informée des efforts de la Coalition dans le domaine de la lutte contre le terrorisme, ainsi que sur ses initiatives, activités et coordination des efforts États Membres dans les quatre domaines de lutte: Idéologique, médiatique, militaire et la lutte contre le financement du terrorisme. 🌸