NUMÉRO 35 - JANVIER 2022

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

Coup d'envoi du plan annuel des activités de la coalition pour l'année 2022

Le SG désigné de la CIMCT, le Major-Général pilote, Mohamad Al-Mughidi a lancé le 29/12/2021 le programme annuel des activités de la CIMCT pour l'année 2022, en présence des délégués des États membres et du personnel de la Coalition.

Le général Al-Mughidi a salué les réalisations de l'année écoulée et le grand soutien que la Coalition reçoit de l'État du siège et remercié les Délégués pour leur participation effective au succès du plan 2021, émettant l'espoir de toujours répondre aux aspirations des Etats membres et de leurs dirigeants.

Le directeur du département idéologique, Dr Mansour Al-Qarni, a passé en revue les composantes du plan 2022 devant être mis en œuvre, en coordination avec les Délégués des États membres, et en harmonie avec le plan stratégique de la Coalition et la politique des États membres en matière de lutte contre l'extrémisme violent et le terrorisme.

Le Secrétaire général reçoit l'Ambassadeur de la République du Cameroun

Le SG désigné de la CIMCT, le Major-Général pilote, Mohamad Al-Mughidi a reçu au siège de la Coalition à Riyad, le 8/12/2021, l'ambassadeur de la République du Cameroun auprès du Royaume, Aya Tijani et la délégation l'accompagnant. L'ambassadeur a écouté une explication détaillée des efforts de la Coalition dans la lutte contre le terrorisme et son rôle pour coordonner la coopération entre les États membres. Dans la salle de situation, l'ambassadeur a été informé des dernières informations et statistiques relatives aux actes terroristes.

De son côté, le Général Al-Moghidi a invité la République du Cameroun à rejoindre la Coalition en tant qu'État membre, vu l'importance de sa position politique, économique et militaire au Centre-Ouest africain, et sa riche expérience antiterrorisme, saluant ses efforts de lutte contre Boko Haram et les groupes terroristes similaires.

Le directeur de l'IBU salue la CIMCT dans ses efforts de lutte contre le terrorisme

Le directeur général de l'Union Islamique de Radiodiffusion (IBU), Dr Amr Mamdouh Al-Laithi, au cours de son entretien avec le SG au siège de la Coalition à Riyad le 14/12/2021, a salué les efforts de lutte contre le terrorisme de la CIMCT ainsi que le rôle pionnier de l'Arabie Saoudite en soutenant la Coalition.

PERSONNALITÉ TERRORISTE ET PSYCHOLOGIE DE L'EXTRÉMISME

La psychanalyse de la personnalité terroriste est devenue une tendance importante dans les politiques antiterroriste au niveau mondial. Le traitement sécuritaire et judiciaire ne suffisent pas pour éradiquer le terrorisme, puisque les terroristes restent un danger même après leur arrestation et leur libération. De nombreux pays s'efforcent de développer différentes méthodes scientifiques liées à l'analyse de la personnalité terroriste afin d'en comprendre les aspects intellectuels et psychologiques.

Dans ce contexte, la CIMCT a organisé, le 9 décembre 2021, un colloque intitulé (Analyse réaliste des traits de personnalité et de leur relation avec la psychologie de l'extrémisme), présenté par Dr. Turki bin Muhammad Al-Atian, professeur de psychologie à UIMS et Dr. Hamid bin Khalil Al-Shayji, professeur de sociologie à l'Université King Saud, et modéré par Dr. Abdullah bin Saeed Al-Dawh, du Département Intellectuel de la CIMCT, en présence du SG, des Délégués des États membres et du personnel de la CIMCT.

Traits de personnalité

Dr. Al-Atian a commencé par l'analyse de la personnalité du terroriste et les types de troubles mentaux communs aux terroristes (schizophrénie, folie périodique et paranoïa), en soulignant que le troisième type est le plus répandu car il entraîne des troubles, notamment:

- Des illusions idéologiques dans l'imagination et capacité de tisser de nombreuses pensées et événements illogiques et irréalistes.
- Une tendance à se quereller et à exagérer les griefs, le fanatisme religieux fondamentaliste et à blâmer les autres vu son manque d'efficacité personnelle et à gérer sa vie.
- Une jalousie très pathologique envers les autres, absence de confiance et attente du mal de leur part, en cherchant constamment de signes et preuves pour étayer ses idées fanatiques.
- Têtu et agressif, qui a tendance à se disputer et à se quereller, critique les autres et soulève des problèmes à leur égard.
- Il apparaît souvent aux autres comme ambitieux, énergique et peu disposé à faire des compromis.

Façons de penser

Dr. Al-Atyan a discuté des méthodes de pensée du terroriste et de la manière dont elles se manifestent dans son comportement, notamment:

- Peur excessive, et sentiment d'échec et de frustration, qui le conduit à un comportement incontrôlé qui évacue ses désirs et prouve son existence.
- Colère intense et persistante, qui s'exprime par un comportement agressif envers les autres.
- Sentiment de perte d'identité et d'infériorité, et sentiment de culpabilité, qui le poussent à haïr la vie et à en désespérer, ce qui le pousse à se venger en tuant, détruisant, sabotant, intimidant et semant la terreur.
- Vantardise et sentiment de fierté pour ses capacités perverses. C'est pourquoi, il peut prendre le surnom d'un grand compagnon, ou changer son apparence et ses vêtements d'une manière particulière.
- Une méthode de pensée irrationnelle et illogique.
- Sa façon de penser dépend de l'enthousiasme et de l'empressement, déformant les faits et critiquer toute la société, et exagérant les erreurs, ce qui l'affecte d'un défaut dans ses relations avec les autres, et le rend incapable de s'adapter,

et d'exercer ses fonctions dans la vie. Il est toujours en conflit avec les valeurs de la société.

- Ignorance de la vérité de lui-même, ce qu'il porte d'opinions et d'idées étant tout à fait naturel, et il ne sent pas qu'il a un défaut dans ses pensées, ses sentiments et son comportement, et que ses problèmes sont, au contraire, causés par les autres.
- Sa façon de percevoir et de penser l'amène à ressentir de l'échec et de la frustration, il a donc tendance à la solitude et à l'isolement, et son désir de vengeance augmente.

Réhabilitation des terroristes

Dans la seconde partie du colloque, Dr. Al-Shayji a abordé la question de la réinsertion des extrémistes violents dans la société, et les obstacles au travail social avec les prisonniers de l'extrémisme violent. Les personnes libérées sont confrontées à de nombreux problèmes liés au prisonnier lui-même et à la société. Le plus important de ces problèmes est la question de stigmatisation sociale qui peut empêcher la personne de reprendre une vie sociale normale.

Al-Shayji a analysé les tendances sociales récentes dans le travail avec ceux qui ont été impliqués dans des actes d'extrémisme idéologique, de violence et de terrorisme, après leur libération. Il a présenté sa théorie des (cinq caractères) pour les qualifier et aider à s'intégrer dans la société. La première lettre symbolise le type de personnes rencontrées dans leur environnement social (l'amoureux, le blêmeur, le sceptique, le glorifié et l'observateur).

1) L'amoureux:

Il s'agit de sa famille proche qui l'aime, mais exercera un contrôle très étroit sur lui, de peur de le perdre à nouveau, et il reviendra sur le chemin précédent, le pont de confiance entre lui et eux étant ébranlé à cause de son comportement inacceptable car grande majorité de ceux qui ont rejoint des organisations terroristes, ou qui se sont rendus dans des zones de conflit, l'ont fait à l'insu de leurs familles. Les membres de la famille les traitent donc différemment peuvent ainsi étouffer leurs mouvements et leur communication avec les autres, ce qui peut entraîner une réaction imprudente ou non calculée de la part des enfants. La confiance ébranlée a besoin de plus du temps pour être reconstruite, d'où l'importance d'éclairer les deux côtés pour comprendre la situation en connaissance de cause avec sagesse, afin de ne pas conduire à des situations tendues et des réactions indisciplinées, affectant les liens de la relation familiale.

2) Le blâmeur

Il s'agit de la famille nombreuse de la personne libérée : les grands-parents, les oncles, les tantes et les personnes âgées de la famille, et certains d'entre eux peuvent le blâmer et le réprimander pour ses actes : pourquoi nous as-tu fait honte avec ton acte honteux ? Le problème réside dans la réaction, qui peut être négative, téméraire ou non calculée, comme le clash, ou la coupure de la communication, qui entrave le processus d'intégration et d'adaptation à nouveau avec la société.

3) Le sceptique

Il s'agit des personnes de l'environnement social entourant la personne libérée : un ancien ami, voisin, collègue de travail ou d'étude, et chaque fois qu'il voyait l'ancien terroriste ou le rencontrait, il évite de lui parler. Ces attitudes négatives envers le terroriste repenti, peuvent entraver son adaptation et sa bonne intégration dans la société.

4) Le glorifié :

Il s'agit des personnes qui appartiennent aux cinq catégories les plus dangereuses, car ils veulent recruter à nouveau l'ancien terroriste ou l'utiliser pour en recruter d'autres, en glorifiant ses actes terroristes antérieurs, et en lui promettant compensation et vengeance pour ceux qui l'ont blessé ou stigmatisé. De cette façon, certains terroristes repentis peuvent à nouveau être entraînés dans l'extrémisme et le terrorisme.

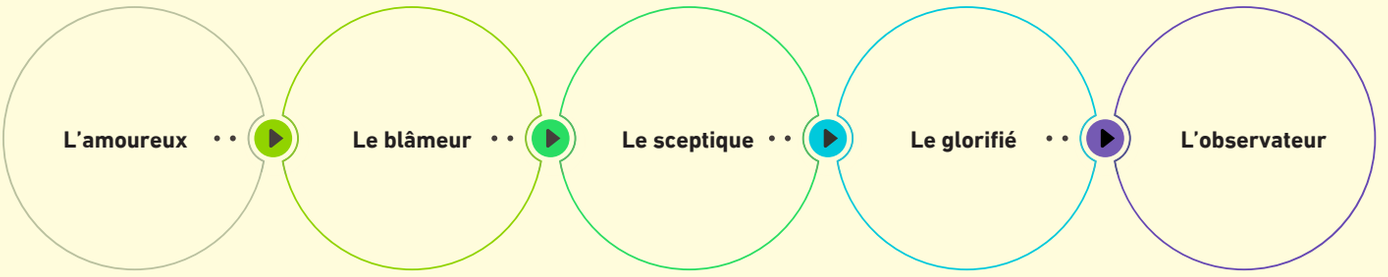
5) L'observateur

Les autorités de sécurité surveillent le terroriste après sa libération afin de s'assurer qu'il s'éloignera des comportements déviants et des idées corrompues, et pour l'aider à s'adapter et à s'intégrer dans la société, le protéger de retomber dans des actes déviants et l'empêcher de communiquer avec des groupes déviants. Certains ex-terroristes repentis compliquent les choses et refusent le suivi et la surveillance, ce qui peut les pousser à des réactions non calculées, et à des comportements qui les mènent au jugement.

Débats et discussions

À la fin du colloque, il y a eu un débat sur certains aspects de la personnalité du terroriste. Pour Dr Al-Atyan, l'aspect le plus important de la personnalité du loup solitaire, c'est l'aspect idéologique et dogmatique. Cette personnalité mène l'acte terroriste sans lien organisationnel, mais avec un motif idéologique et dogmatique qui rend difficile de le contrôler.

Dr. Al-Harthy, Délégué du Royaume au domaine intellectuel, a souligné l'importance de distinguer entre la psychologie de l'extrémisme et celle du terrorisme : tous les extrémistes ne sont pas des terroristes, et tous les terroristes ne sont pas psychotiques ou anormaux. Certains d'entre eux ont été trompés. Il y a une multiplicité des apports au terrorisme, qui ne se limitent pas au côté idéologique, car le côté émotionnel, par exemple, n'est pas moins important. Vu sa longue expérience dans la formation de terroristes, Dr. Al-Atyan a conclu qu'il n'y a pas un seul terroriste normal.



la théorie des cinq caractères

TERRORISME ET DÉFIS DE SÉCURITÉ INTÉRIEURE

Le terrorisme est l'un des phénomènes criminels les plus dangereux que les sociétés aient connu en raison de la menace qu'il fait peser sur les peuples et les États. Il est devenu un prétexte aux interventions internationales, pouvant mener au démantèlement et à la déstabilisation des États, d'où l'importance des forces armées pour assurer l'unité et la stabilité de l'État, affronter le terrorisme et protéger la sécurité nationale devenue un concept multiforme comprenant plusieurs facteurs dont les plus importants sont la stabilité politique, l'état de droit et l'homogénéité du front politique et sécuritaire de l'État.

La CIMCT a organisé le 13/12/2021 une conférence intitulée : (Le terrorisme et les défis de la sécurité intérieure), présentée par le brigadier général Tariq Ahmed Koko Al-Taher, délégué de la République du Soudan à la Coalition. Monsieur Koko a traité de la notion de terrorisme, de ses causes, de la politique des Nations Unies en matière de lutte contre le terrorisme, du plan d'action pour la mise en œuvre de cette politique, du rôle des forces armées dans les opérations de sécurité intérieure et de la vision future du terrorisme à la lumière de la réalité existante.

Politique des Nations Unies

Au début de la conférence, le brigadier général Koko a présenté le concept de terrorisme, les divergences entre chercheurs, spécialistes et politiques dans la définition du terrorisme, et comment les médias présentent les membres d'organisations terroristes selon leurs points de vue politiques, ou la position de leurs pays et gouvernements, pouvant être ainsi terroristes, saboteurs, dissidents, criminels, soldats de libération, militants, ou révolutionnaires.

Il a également évoqué les causes du phénomène du terrorisme sous ses divers aspects, tels que les facteurs économiques, politiques, sociaux ou religieux interdépendants et analysé les sources de menace externes et internes dans les pays propices à l'apparition du terrorisme.

Ensuite, le conférencier a traité de la politique des Nations Unies en matière de lutte contre le terrorisme, et comment l'ONU aide les pays du monde à lui faire face conformément aux normes internationales unifiées. Cette politique onusienne comporte quatre bases:

- Traiter les conditions propices à la propagation du terrorisme.
- Mesures de prévention et de lutte contre le terrorisme.
- Mesures visant à renforcer la capacité des États à prévenir et combattre le terrorisme, et à renforcer le rôle des Nations Unies à cet égard.
- Mesures visant à garantir le respect des droits de l'homme et de l'État de droit en tant que bases fondamentales de la lutte contre le terrorisme.

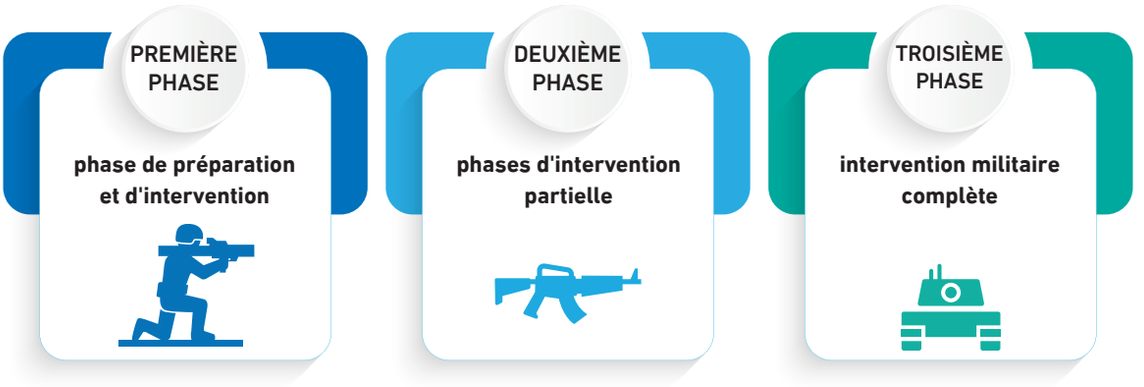
La politique comprend d'importants principes, dont notamment :

- Les actes terroristes portent atteinte aux droits de l'homme, aux libertés fondamentales et à la démocratie, et déstabilisent les gouvernements légitimes.
- Le terrorisme ne peut être associé à aucune religion, nationalité, civilisation ou groupe ethnique.
- Le développement, la paix, la sécurité et les droits de l'homme sont des questions interdépendantes.
- Nécessité de s'attaquer aux conditions aidant à la propagation du terrorisme et de prendre des mesures urgentes pour prévenir et combattre le terrorisme, tout en reconnaissant qu'aucune circonstance ne peut justifier la commission d'actes terroristes.
- Rejet sans équivoque du terrorisme sous toutes ses formes et manifestations, quels qu'en soient les auteurs et où qu'il soit commis.
- La coopération internationale et les mesures prises par les États pour prévenir et combattre le terrorisme doivent être conformes aux conventions internationales pertinentes.

Le Plan d'action joint à la Politique antiterroriste des Nations Unies est consacré à la prévention de l'extrémisme violent et aborde l'impact de l'extrémisme violent sur la paix et la sécurité, le développement durable, les droits de l'homme, l'état de droit et l'action humanitaire. Il analyse le contexte de l'extrémisme violent et ses moteurs représentés dans les conditions propices à l'extrémisme violent et les méthodes de propagation de l'idéologie radicale, et fournit un programme d'action et des recommandations utiles pour la prévention de l'extrémisme violent aux niveaux national, régional et mondial.

Fonction des forces armées

Le conférencier a analysé le rôle des forces armées et dans les opérations de sécurité intérieure et indiqué que la tâche principale



PHASES DU RECOURS AUX FROCES ARMES DANS LES OPÉRATIONS DE SÉCURITÉ INTÉRIEURE

des forces armées est de défendre l'État, préserver l'intégrité de ses territoires, ses eaux et son espace aérien, le protéger de toute agression extérieure et maintenir sa sécurité et sa stabilité.

Les forces armées font partie intégrante du système de sécurité nationale pour défendre le pays contre toute menace extérieure, mais dans certaines circonstances, elles interviennent pour soutenir les autorités civiles dans le rétablissement de la sécurité intérieure, l'application de la loi, et pour pour faire face aux manifestations associées à la violence et aux émeutes ou la rébellion et la désobéissance civile accompagnées d'actes terroristes. L'armée confronte donc les troubles publics et le chaos et soutient aussi la société civile dans l'action de secours en cas de catastrophe.

Le conférencier a divisé les étapes du recours aux forces armées dans les opérations de sécurité intérieure en trois étapes. Primo : la préparation et d'intervention ; secundo : l'intervention partielle, si la police s'avère incapable de faire face à la situation de menace; tertio : l'intervention militaire totale, en cas de risque d'effondrement de l'ordre public, et que les forces de police perdent complètement le contrôle de la situation sécuritaire.

Les autorités ordonnant l'intervention des forces armées diffèrent selon chaque étape : en cas d'intervention complète, la charge incombe à l'autorité politique supérieure du pays, et en cas d'intervention partielle, c'est la responsabilité du Centre d'opérations interarmées des forces armées après approbation de l'Autorité militaire suprême. À toutes les étapes de l'intervention, les forces armées respectent les règles d'emploi de la force létale dans les environnements civils.

Le brigadier général Koko a conclu sa conférence en présentant une vision future du terrorisme, dans laquelle il a appelé à soutenir les capacités des agences concernées par la lutte contre le terrorisme, à encourager l'échange d'informations relatives aux organisations terroristes et à leurs activités, et à accroître l'efficacité des institutions sociales dans la lutte contre le terrorisme.

La CIMCT et la réponse internationale

Au cours des discussions qui ont suivi la conférence, le général retraité Raheel Sharif, commandant militaire de la CIMCT a souligné l'importance des aspects historiques, géographiques et de développement dans la lutte contre le terrorisme, la nécessité de rétablir la normalité suite aux opérations antiterroristes, et l'importance de la réponse internationale à la lutte contre le terrorisme, estimant que la CIMCT constitue avec ses diverses initiatives, une réponse modèle à cette menace.

Brigadier Général Raed Saleem Al-Marashda, délégué de Jordanie, a appelé à distinguer les opérations de sécurité intérieure et les opérations de lutte contre le terrorisme, affirmant que les manifestations et les sit-in ne sont pas du terrorisme, mais s'ils ne sont pas traités, peuvent ouvrir la porte au terrorisme. Les causes du terrorisme sont complexes et se chevauchent, les causes internes peuvent se dégrader avec le soutien externe, et ce qui importe, c'est la sécurité et la stabilité internes, ajoutant que les forces armées ne doivent pas être utilisées pour la sécurité intérieure sauf en cas de nécessité impérieuse et pour une courte durée, la présence de l'armée dans les rues donnant une impression négative du pays à l'étranger.

Le lieutenant-colonel Hamid Karim Beg, délégué du Pakistan, a souligné de son côté l'importance de la formation intégrée des unités antiterroristes, et de ne pas se limiter aux seuls aspects militaires mais les former aussi aux aspects psychologiques et sociaux.

STRATÉGIES COMPARATIVES ANTITERRORISTES

Le terrorisme est une menace pour la paix et la sécurité mondiales car il dévaste les États et les peuples. Les efforts internationaux pour le contrer suivent diverses stratégies: nationales, régionales et internationales. La CIMCT a tenu une conférence intitulée: (Stratégies comparatives antiterroristes), présentée par Dr. Farhat Al-Harshani, conseiller de la CIMCT, le 15 décembre 2021.

Concepts

Dr. Farhat Al-Harshani a abordé les concepts de stratégie et de terrorisme. La stratégie étant l'un des concepts les plus anciens et les plus connus, s'est introduit dans d'autres domaines (militaire, politique et social), avant d'embrasser toutes les activités humaines. Il y a donc la stratégie spécialisée, qui constitue le plan d'étude des objectifs d'une activité spécifique à partir des sous-activités de l'État (l'éducation, la sécurité et l'économie), et la stratégie globale qui est basée sur la réalisation d'objectifs politiques, que ce soit au temps de paix ou de guerre.

Le terrorisme peut être défini selon ses objectifs, ou selon son contenu et ses moyens: l'usage de la terreur et de la violence, quel qu'en soit le but. La communauté internationale n'a pas encore adopté une définition unique et globale du terrorisme. Il est défini différemment dans plusieurs accords partiels, comme celle de Genève pour la répression du terrorisme de 1937, et plusieurs textes de l'Assemblée générale des Nations Unies, ou le Conseil de sécurité internationale entre 1994 et 2004, la Convention antiterroriste arabe de 1998 et la Convention de l'Organisation de l'Unité Africaine de 1999.

Dans tous ces textes, le terrorisme est défini selon le critère du contenu, et non sur celui des objectifs. La Convention arabe définit le terrorisme comme: « Tout acte de violence ou de menace, quels qu'en soient les motifs ou les finalités, se produit pour mener un acte criminel, collectif ou individuel, visant à semer la terreur parmi les personnes, ou à les intimider en leur portant atteinte ou en mettant leur vie, leur liberté ou leur sécurité, ou en causant des dommages à l'environnement ou à une installation ou à un bien public ou privé, ou de l'occuper ou de s'en emparer, ou de mettre en danger une ressource nationale ».

Le conférencier a indiqué la différence entre le terrorisme, l'extrémisme, la violence politique, le crime organisé et la résistance armée.

Il est donc difficile de définir le terrorisme, tant qu'il n'y a pas d'unanimité mondiale là-dessus.

Stratégies de lutte

Dès la propagation du terrorisme, la communauté internationale adopte diverses stratégies de lutte aux niveaux national, régional et mondial. La Stratégie antiterroriste mondiale des Nations Unies, approuvée par l'organisation internationale en 2006, est suivie d'un plan d'action basé sur quatre fondements pour répondre aux conditions propices à la propagation du terrorisme, le prévenir et le combattre, et renforcer les efforts des Nations Unies à cet égard et garantir le respect des droits de l'homme et de l'État de droit comme base de lutte antiterroriste.

Cette stratégie subit un examen chaque deux ans par l'Assemblée générale. Conçue pour s'adapter aux priorités des États Membres dans la lutte antiterroriste, elle constitue un outil complet pour soutenir les efforts de lutte antiterroriste aux niveaux national, régional et international, et comprend des mesures concrètes pour prévenir et combattre le terrorisme.

La Commission européenne a également adopté la Stratégie antiterroriste 2020 de l'Union européenne, pour la lutte antiterroriste, le crime organisé, la détection et la prévention des menaces mixtes et l'augmentation de la résilience des infrastructures critiques. Il s'agit de renforcer la sécurité numérique et la cybersécurité, soutenir la recherche et l'innovation, protéger l'Europe du terrorisme et du crime organisé et renforcer le travail des institutions gouvernementales et non gouvernementales afin de contrer les attaques et les cyberattaques, les campagnes de désinformation, les fake news et l'industrie de haine.

Le Conseil des ministres arabes de l'Intérieur a adopté la stratégie arabe antiterroriste en 1997 dans le but de renforcer et coordonner les efforts antiterroristes en

préservant la sécurité, la sûreté et la stabilité du monde arabe, sur les fondements de la légitimité et de l'État de droit. Elle vise à renforcer et développer la coopération entre les pays arabes et les pays des organisations internationales en matière de lutte antiterroriste. La stratégie a exhorté les pays arabes à établir un comité national composé de représentants des agences compétentes, et créer une unité spécialisée pour collecter des informations sur les actes terroristes, pour garantir son application dans chaque pays.

Stratégies nationales

Dr. Farhat Al-Harshani a abordé une analyse comparative de certaines stratégies nationales, comme celle de l'Arabie saoudite qui a adopté une stratégie globale, multidimensionnelle et intégrée de lutte antiterroriste, fondée sur la prévention, le traitement et le soin.

- La stratégie de prévention vise à renforcer les efforts qui sensibilisent la société aux dangers des pensées extrémistes, déviantes et erronées, encouragent la réflexion modérée, corrigent les idées fausses et luttent contre les idées extrémistes.
- La stratégie de traitement consiste en un ensemble de mesures comprenant des programmes de rééducation et d'éveil, des conseils et des orientations.
- Dans la stratégie de soin, il y a une interaction avec les libérés et leurs familles, en leur apportant un soutien financier et moral, en leur organisant des programmes de réinsertion, en les aidant à se réadapter aux exigences de la société saoudienne et en leur trouvant un emploi pour s'intégrer dans la société.

La stratégie antiterroriste marocaine repose sur une approche intégrée et cohérente, fondée sur la promotion des valeurs de modération, de tolérance, de droits humains et de consolidation de l'Etat de droit, tout en adoptant des mesures de lutte contre la pauvreté et l'exclusion, en réalisant l'égalité sociale, et en soutenant et intégrant les détenus extrémistes et les ex-détenus.

La stratégie antiterroriste tunisienne est fondée sur la stratégie globale de lutte antiterroriste pour isoler le phénomène du terrorisme de ses affluents qui le nourrissent, et développer des moyens de lutte non pas seulement au niveau sécuritaire et militaire, mais aussi avec la participation de toutes les autorités et institutions concernées.

La stratégie antiterroriste des États-Unis d'Amérique, publiée le 4 octobre 2018, qui avait pour objectif ultime de « vaincre les terroristes qui menacent la sécurité des États-Unis, de prévenir de futures attaques et de protéger les intérêts nationaux », comprenait six domaines principaux:

1. Poursuite de terroristes.
2. Isoler les terroristes de leurs sources de soutien.
3. Moderniser les autorités et outils antiterroristes aux États-Unis.
4. Protéger les infrastructures américaines et renforcer la résilience.
5. Lutte contre l'extrémisme terroriste et le recrutement.
6. Renforcer les capacités antiterroristes des partenaires internationaux des États-Unis.

Stratégie de la Coalition

La stratégie de la CIMCT suit un plan vertical selon les domaines intellectuel, médiatique, de la lutte contre le financement du terrorisme, et militaire, qui croisent les stratégies internationales régionales, nationales, et chacun d'eux (à l'exception du domaine militaire) comporte nécessairement un aspect préventif, protecteur et dissuasif. Il y a une parfaite adéquation entre la stratégie de la CIMCT et les différentes stratégies. La CIMCT analyse donc les éléments importants de tout acte terroriste, quelle que soit la nature de ses moyens, à savoir: la pensée, l'argent, les médias, l'aspect militaire.

Conclusions

Suite à l'analyse et la comparaison de différentes stratégies, le conférencier a évoqué les conclusions suivantes:

- L'objectif de toutes les stratégies est similaire en dépit de la différence de leur formulation: déclarer la guerre au terrorisme depuis ses racines. Toutes les stratégies sont d'accord sur la nécessité de combattre l'extrémisme comme voie menant au terrorisme et à la formation de la personnalité fanatique et violente.
- La coopération internationale dans ce domaine est importante, car le terrorisme transcende les frontières des États, et s'active dans des zones frontalières, lieu propice d'instabilité, de guerres ou de rébellions. Il y a donc un lien entre le crime terroriste et le crime organisé transnational.
- Ces stratégies ont prêté attention au cyberterrorisme, où le terroriste suit avec intérêt les dernières technologies et sources d'information pour attirer des recrues et organiser des opérations terroristes.
- L'objectif des stratégies nationales dans divers pays du monde est la lutte antiterroriste, mais elles divergent en raison des différentes capacités et circonstances de chaque pays.

ENQUÊTE FINANCIÈRE SUR LES DÉLITS DE BLANCHIMENT DE CAPITAUX ET DE FINANCEMENT DU TERRORISME

Les crimes de blanchiment d'argent et de financement du terrorisme (BC/FT) portent atteinte à la sécurité et à la paix du monde. Le terrorisme survit grâce à un énorme financement, les fonds blanchis atteignant entre 950 Milliards de Dollars et 1.5 Trillion de dollars, selon le FMI. L'impact de ces crimes augmente à la lumière de la révolution des télécommunications et du développement vertigineux des technologies de l'information, facilitant le mouvement de l'argent à travers les frontières nationales par le biais de systèmes financiers multiples, ultra-rapides et extrêmement complexes.

À cet égard, la CIMCT a organisé, le 22 décembre 2021, à son siège à Riyad, une conférence intitulée : « Procédures d'enquête financière parallèles dans les crimes de BC/FT)» présentée par Ahmed bin Muhammad Al-Muqhim, procureur chargé des crimes économiques et membre fondateur de l'Unité de BC du ministère public du Royaume d'Arabie saoudite..

Risques économiques et sociaux

Au début de la conférence, Al-Muqhim a souligné que les crimes de BC/FT constituent un grave danger pour les potentialités économiques et sociales de tout pays, en particulier les pays aux faibles normes prises dans la lutte contre ces crimes.

Sur le plan économique, ces délits portent atteinte à la réputation du système financier, privent l'État d'importantes ressources financières pouvant être allouées à l'emploi et au développement, augmentent les taux d'inflation et affectent les règles de la concurrence loyale et honnête.

Sur le plan social, les avoirs de ce trafic renforcent le crime, permettent de financer le terrorisme et causent le déclin des valeurs éducatives et culturelles.

Similitudes et différences

Comparant les crimes de BC et FT, le conférencier a indiqué que ces deux types de crimes se basent sur la fourberie et le camouflage, et nécessitent une coopération stratégique internationale, en raison de leur nature transfrontalière, un traitement de suivi et des procédures d'enquête financière. Ils diffèrent toutefois à plusieurs égards:

- Source des fonds : les délits de BC sont de sources illégales et criminelles (trafic de drogue, d'antiquités, de marchandises interdites, d'êtres humains...etc.), tandis que le FT s'effectue avec des fonds légitimes et illégitimes.
- Montant des fonds : Les délits de BC impliquent des sommes énormes, non comparables au montant des délits de FT.
- Objectif : L'objectif des délits du BC est le profit financier, tandis que celui du FT est politique ou idéologique.
- Circulation des fonds : les fonds des délits de BC transitent par les institutions financières de manière circulaire, débutant par le blanchisseur et aboutissant à lui. Quant aux fonds de FT, ils ne suivent pas forcément la trajectoire des institutions financières, et empruntent une trajectoire linéaire qui débute par le financier et aboutit à l'organisation terroriste.
- Champ de détection : Dans les délits de BC, la détection porte sur les relations entre les personnes impliquées dans le délit, alors que pour les délits de FT, l'intérêt porte sur l'argent et son mouvement.

Le conférencier a passé en revue les méthodes les plus courantes pour dissimuler les fonds provenant de crimes, telles que les transactions électroniques, le commerce de marchandises n'ayant aucune norme de valeur ou de contrôle sur les prix à l'instar des antiquités et des tableaux d'art, l'établissement de sociétés fictives et la déclaration de possession de fonds à la douane pour avoir une attestation permettant de déposer des fonds illicites dans nombre de comptes, effectuer plusieurs transferts et établir de gros contrats et imports fictifs afin de pouvoir s'adonner à la contrebande de fonds.

Rôle de l'enquête parallèle

Al-Muqhim a évoqué l'enquête financière parallèle (EFP) et son impact sur la lutte contre le crime de BC/FT, précisant qu'elle vise à recueillir les preuves financières matérielles en dévoilant les transactions financières suspectes et en révélant les mouvements financiers, afin de déterminer et de bloquer les produits et moyens du délit initial et du délit de BC. Dans l'une de ses recommandations, le GAFI indique que les gouvernements devraient mener une

enquête proactive parallèle concernant tous les cas de BC/FT et les crimes associés, ce qui signifie que le tribunal ouvre une enquête financière parallèle à l'enquête pénale, pour traquer les produits financiers du crime et fournir des preuves liant ces produits financiers au crime initial.

Le succès des enquêtes financières parallèles dans la récupération des produits du crime est considéré comme un critère important pour déterminer la conformité de l'État aux exigences de lutte contre les délits de BC, et un facteur clé dans l'évaluation internationale.

L'EFP est proactive d'essence, car elle identifie les produits du crime faisant l'objet d'une enquête, empêche les profits illégaux d'investir l'économie, supprime les instruments du crime futur et renforce le principe clé selon lequel personne ne doit profiter du crime.

L'importance de l'EFP découle de son rôle dans la détermination et la documentation des mouvements d'argent, car elle identifie les motifs et les liens entre les personnes, dévoile les participants à l'acte criminel et la structure des organisations criminelles, identifie le degré de risque de chaque accusé, surveille les produits du crime faisant l'objet d'une enquête, aide à découvrir de nouveaux crimes et précise l'emplacement des suspects, des témoins, des victimes, ainsi que les moyens et les méthodes utilisés dans le crime.

Méthodes d'enquête et sources d'information

Le conférencier a présenté les méthodes les plus importantes utilisées dans l'EFP, et les sources d'informations qui s'y rapportent,

et souligné que les méthodes sont nombreuses, dont certaines suivent des procédures secrètes et cachées, et d'autres procédures ouvertes et publiques. Parmi les procédures les plus importantes du premier type, figurent ce qui suit :

- Recherche et enquête sur le terrain, par déplacement, inspection et surveillance effective.
- Opérations d'infiltration, dans lesquelles l'officier de police judiciaire se déguise en trafiquant pour connaître les dimensions du crime et les parties impliquées. Ces agents suivent généralement une formation approfondie pour maîtriser les compétences furtives.
- Livraison surveillée : on laisse le suspect surveillé poursuivre son activité (livraison de drogue par exemple), pour dévoiler le réseau criminel et arrêter ses membres en flagrant délit.
- Surveiller les communications des accusés, sur autorisation du ministère public, pour connaître leurs relations internes et externes.
- Écrire aux autorités compétentes pour établir les avoirs de l'accusé.

Quant aux méthodes d'enquête usant de procédures publiques, il s'agit notamment : d'assigner à l'accusé de prouver la provenance de son argent, en apportant des justificatifs en papier, permettant à l'officier de police judiciaire de discuter avec lui et de le confronter.

Il existe également de nombreuses sources d'information en EFP, dont notamment:

- Le casier judiciaire qui détermine les antécédents de l'accusé.
- Les appareils électroniques appartenant aux prévenus, sources d'importantes information, la police judiciaire devant y recueillir les informations contenues dans ces sources avant qu'elles ne soient volontairement endommagées ou sabotées.
- Les informations financières provenant des institutions financières : banques et bureaux de change.
- Les informations de sécurité détenues par les services de sécurité.
- Les informations réglementaires détenues par les autorités officielles : organismes industriels et commerciaux, douanes, passeports, etc. Elles comprennent des informations susceptibles de divulguer d'importants aspects des activités des personnes accusées de BC/FT.

Débat

A la fin de la conférence, le brigadier général Nawaf Al-Jitaili, délégué du Koweït s'est interrogé sur les indices du BC/FT. Le conférencier a indiqué qu'il existe nombre d'indices dont le fait d'avoir un mouvement financier non proportionnel aux revenus du suspect. Le brigadier général Rashid Al Dhaheri, délégué émirati, a demandé comment faire face à l'exploitation des célébrités des médias sociaux dans les opérations de BC.

Le conférencier a répondu que les personnes impliquées dans les crimes de BC/FT sont toujours promptes à concevoir de nouvelles méthodes pour commettre leurs crimes, comme en ciblant les célébrités des médias sociaux, faute de normes ou de contrôles pour leurs revenus, d'où l'importance pour eux de documenter leurs bénéfices et de réglementer le contenu publicitaire sur leurs pages, le Royaume d'Arabie Saoudite ayant déjà pris des mesures importantes à cet égard.

INTRUSIONS ÉLECTRONIQUES ET MÉTHODES DE PRÉVENTION

EXEMPLES PRATIQUES D'ÉCRAN DE PIRATE

Les intrusions électroniques sont l'un des problèmes les plus graves qui affligent les internautes à travers le monde, gouvernements, institutions ou particuliers, soient-ils. Ces piratages sont devenus un moyen d'extorsion, de vol d'argent et de nombreux autres crimes. A cause à ces activités de sabotage, les services peuvent être interrompus, les biens détruits et les données effacées. On s'attend même à ce que les guerres se déroulent dans un avenir proche sur le cyberespace, étant le moins cher, le plus simple, le plus rapide et le plus efficace. Afin de mieux comprendre ces risques et les moyens de les prévenir, la CIMCT a organisé le mercredi 27 octobre 2021, à son siège à Riyad, une conférence intitulée (**Comment se produisent les intrusions ? Exemples pratiques de l'écran d'un hacker)**, présentée par **Dr Basil Al-Sadhan**, professeur agrégé de sécurité des réseaux au Collège d'ingénierie de l'Université Roi Saud à Riyad et **l'ingénieur Abdullah Al-Qahtani**, membre de l'Association saoudienne de sécurité de l'information, Département de Cybersécurité, en présence du Secrétaire Général en charge de la CIMCT, des délégués

La cybersécurité

Avec l'intensification des infiltrations électroniques, il est devenu impérieux de faire face à ces opérations de sabotage grâce à la cybersécurité. Certains même s'étonnent que l'on dépense des milliards de dollars en armes conventionnelles, alors qu'un seul individu accroupi devant son ordinateur peut désactiver un porte-avions de plusieurs millions de dollars, saboter l'infrastructure des gouvernements numériques ou pirater les données des ministères de la sécurité et désactiver leurs appareils !

La conférence a porté sur les types d'intrusions informatiques, leurs moyens et les meilleures pratiques de protection, et explicité le concept de cybersécurité, portant sur la protection des réseaux, des systèmes informatiques et de leurs composants, des services qu'ils fournissent et des données qu'ils contiennent, de toute infiltration ou perturbation. Les cyberattaques visent généralement à accéder à des informations sensibles pour altérer, endommager ou extorquer les usagers et obtenir l'argent. Le concept de cybersécurité comprend la sécurité de l'information, la sécurité électronique et la sécurité numérique.

La cybersécurité vise à atteindre les objectifs suivants:

- **Confidentialité:** empêcher l'accès à l'information à part aux personnes autorisées.
- **Sécurité:** validité des informations lorsqu'elles sont saisies, conservées ou transmises, et leur protection contre toute attaque de sabotage ou vol.
- **Disponibilité:** capacité du détenteur de l'information à y accéder en cas de besoin à tout moment et de récupérer les données en cas de violation ou de sinistre.

La cybersécurité est donc un véritable enjeu pour les institutions en raison de l'évolution rapide des technologies à protéger et des menaces qui en découlent et de nombreuses solutions de sécurité développées pour répondre à ces défis.

Les cyberattaques

Les cyberattaques désignent les activités malveillantes menées par des individus ou des institutions pour désactiver, affaiblir ou détruire les systèmes d'information d'organisations ou d'individus, l'assaillant recherchant généralement un avantage ou un bénéfice en investissant le réseau de la victime.

Parmi les **principales catégories d'assaillants**, on dénote:

Script boys: personnes inexpérimentées utilisant des outils prêts à l'emploi pour infiltrer les sites Web et se faire admirer.

Hacktivistes: ressemblent aux script boys, mais ils sont politiquement motivés.

Cybercriminels: ciblent les entreprises commerciales, les services bancaires et les cartes de crédit pour faire du chantage et gagner de l'argent.

Individus financés par les gouvernements: le pire danger car ils

usent des meilleurs talents pour mener des attaques avancées de manière furtive, et parfois même concevoir des attaques personnalisées, ce qui rend la protection de la cible très difficile.

Exemples de cyberattaques

La conférence a traité des modèles les plus importants de cyberattaques comme suit:

Rançongiciel

Ce malware empêche l'usager d'accéder à ses systèmes et fichiers personnels. Le logiciel prétend être utile pour convaincre la victime de le télécharger, puis cible le système d'exploitation et crypte toutes les données stockées pour forcer la victime à payer une rançon pour le décryptage, généralement en Bitcoin.

Le rançongiciel investit le PC de la victime, à travers les publicités malveillantes, les courriers indésirables et l'installation d'applications à risque et constitue une menace majeure pour les institutions de toutes sortes. Selon la société de cybersécurité Sophos, ce cyber-virus a envahi plus de 150 pays dans le monde, notamment: Allemagne, Autriche, Suisse , États-Unis, Royaume-Uni et Canada., atteignant plus de 200.000 victimes.

Chevaux de Troie

La dénomination métaphorique réfère à la duperie, ce programme prétendant être inoffensif pour convaincre la victime de le télécharger sur son appareil, mais le véritable objectif du pirate informatique est d'espionner le contenu de l'appareil, voler certaines données, les effacer ou les détruire complètement. Les pirates envoient à des particuliers et des entreprises, à travers des e-mail ou des documents malveillants, ce virus qui fonctionne comme un ver numérique infectant applications et systèmes logiciels.

Ingénierie sociale

C'est le processus de manipulation psychologique des gens, à travers la ruse pour les tromper et les inciter à révéler des informations confidentielles ou personnelles. L'ingénierie sociale repose sur l'élément humain ayant un certain niveau d'expertise pour effectuer cette tâche, sans recourir aux appareils, ou sans avoir de connaissances approfondies en technologies modernes. Elle fonctionne souvent par téléphone ou par e-mail, le fraudeur se faisant passer pour une personne importante, pour poser des questions personnelles sans éveiller les soupçons de la victime.

Désactivation des services distribués

Appelées attaques par déni de service, ce stratagème vise à rendre les ressources du réseau indisponibles pour leurs utilisateurs légitimes, usant d'un seul appareil ou d'une armée d'appareils. Il cible les ressources de l'appareil telles que: le processeur, la mémoire, le line de capacité du réseau ou les économies d'énergie (batterie) pour empêche la fourniture de services. Ces attaques ressemblent à celui qui appelle constamment une ligne téléphonique pour l'occuper et empêcher les autres d'appeler. Elles sont capables de désactiver le service pendant une longue période.

Messages de piégeage

Le piégeage ou l'hameçonnage est un type de crime sur Internet de plus en plus répandu. Le cyber-pirate envoie des communications frauduleuses qui semblent provenir d'une source fiable, souvent par courrier électronique, permettant de voler les données sensibles, telles que: les données de la carte de crédit, les informations de connexion ou l'installation de logiciels malveillants sur l'appareil de la victime. Le pirate trompe le destinataire du message qui lui donne directement l'information ou l'obtient grâce à un quelconque subterfuge.

Méthodes de protection

La conférence a enfin clarifié les moyens de prévenir ces attaques malveillantes en suivant plusieurs méthodes, dont notamment:

- Mises à jour constantes des différents systèmes d'exploitation et programmes.
- Sauvegarder toujours les données importantes.
- Utiliser des programmes puissants pour lutter contre les virus électroniques.
- Mettre à jour en permanence les programmes anti-virus.
- Désactiver les services inutilisés sur les ordinateurs.
- Etre prudent en installant des logiciels inconnus.
- Établir des politiques exigeant l'utilisation de mots de passe forts.
- En cas d'attaque, ne jamais se conformer aux exigences des pirates, arrêter toutes les opérations dans l'appareil ou sur le réseau et restaurer la copie de sauvegarde.

Quant aux moyens de protection contre l'ingénierie sociale, le conférencier a souligné les points importants:

- Nécessité de changer constamment les mots de passe et ne les partager avec personne.
- Ne pas utiliser de (nom d'utilisateur) et de (mot de passe) pour plusieurs comptes.
- Éviter d'utiliser des wifi non sécurisés.
- Verrouiller l'accès au système d'exploitation des ordinateurs.
- S'assurer des interlocuteurs par téléphone, e-mail ou via les réseaux sociaux.
- Ne pas ouvrir de pièces jointes d'e-mails provenant de personnes anonymes.

Quant aux moyens de protection contre le piégeage des messages, le conférencier a préconisé notamment:

- Eviter d'ouvrir les e-mails inconnus et les supprimer directement.
- Activer la fonction de filtrage des messages pour effacer les messages indésirables.
- Ne pas ouvrir des liens anonymes pouvant conduire au piratage de l'appareil et au vol de données.
- Se méfier des messages demandant des informations personnelles.
- Éviter d'ouvrir des fichiers avec des extensions dans le tableau.
- Éviter d'accéder à des sites Web suspects.
- S'assurer que les programmes et applications sont téléchargés à partir de leurs sources officielles.

En conclusion, le conférencier a résumé les moyens d'atteindre les meilleures pratiques en matière de cybersécurité, à savoir:

- Fournir les dernières technologies.
- S'appuyer sur des personnes qualifiées pour traiter (avec compétence) ces intrusions.
- Élaborer des plans intégrés pour lutter contre ces pratiques de sabotage.

La CIMCT célèbre les fêtes nationales des EAU, Bahreïn et Libye

Délégué des Émirats Arabes Unis

Délégué du Royaume de Bahreïn

Délégué de l'Etat libyen

La CIMCT a célébré les fêtes nationales de trois de ses États membres en décembre 2021, à son siège à Riyad, en présence du SG, des délégués des États membres et du personnel de la Coalition.

Le 2 décembre, les délégués des Émirats Arabes Unis ont célébré la 50è fêtes nationale commémorant la fondation des Émirats en 1971, par cheikh Zayed bin Sultan Al Nahyan. Le 16 décembre, les délégués du Royaume de Bahreïn ont célébré la 50è fête nationale de leur pays, qui commémore l'indépendance et l'accession au pouvoir de Cheikh Isa bin Salman en 1971. Le 26 décembre, le délégué de l'Etat libyen a célébré le 70è anniversaire de l'indépendance de son pays, commémorant les sacrifices des Libyens depuis des décennies jusqu'à l'accession à l'indépendance en 1951.

À cette occasion, la CIMCT a félicité les dirigeants et les peuples de ces pays, souhaitant à tous progrès, sécurité et prospérité.

Le Secrétaire Général reçoit l'attaché militaire de la République Arabe d'Égypte

Le SG désigné de la CIMCT, le Major-Général pilote, Mohamad Al-Moghidi a salué les efforts de la République Arabe d'Égypte dans la lutte contre le terrorisme, et ce en recevant l'attaché militaire égyptien auprès du Royaume d'Arabie Saoudite, le Brigadier Général Mohamad Naji Mohamad Youssef, au siège de la Coalition à Riyad, le jeudi 30/12/2021. L'attaché militaire a souligné l'importance de coopérer avec la CIMCT dans la lutte contre l'extrémisme violent et le terrorisme, saluant les efforts déployés par la Coalition dans ce domaine.

Une délégation du Collège de co mandement et d'état-major de Riyad visite la Coalition

La CIMCT a reçu le 5/12/2021 à son siège une délégation du Collège de commandement et d'état-major de Riyad. La délégation a été informée des efforts antiterrorisme de la CIMCT, dans les quatre domaines: idéologique, médiatique, financier et militaire.

Inauguration du stage de formation de la langue arabe aux non arabophones

Le SG désigné de la CIMCT, le Major-Général pilote, Mohamad Al-Mughidi a donné le 12/12/2021 le coup d'envoi du stage de formation « Enseignement de la langue arabe aux non arabophones », au siège de la Coalition, en présence des délégués des États membres. Le général Al-Mughidi a indiqué que des professeurs de l'Université islamique Imam Muhammad bin Saud se chargeront du programme de formation, notant que le programme vise à promouvoir les compétences cognitives des délégués des États membres.