NUMÉRO 30 - AOÛT 2021

متحالفون

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

LA CIMCT ACCUEILLE LE CHEF DES OPÉRATIONS DU CENTCOM AMÉRICAIN QUI DONNE UNE CONFÉRENCE SUR "LES DRONES"

La CIMCT a accueilli à son siège à Riyad le major-général pilote Alexus Grynkewicz, chef des opérations au commandement central américain, et la délégation l'accompagnant, qui ont été informés des efforts de la Coalition dans la lutte contre le terrorisme.

Au cours de la visite, le général Grynkewich a donné une conférence intitulée "Drones", dans laquelle il a évoqué l'importance de la coopération et de la coordination entre les Etats pour éviter que les drones ne tombent entre les mains d'organisations terroristes **P.6**.

L'Ambassadeur Japonais au Royaume visite la CIMCT

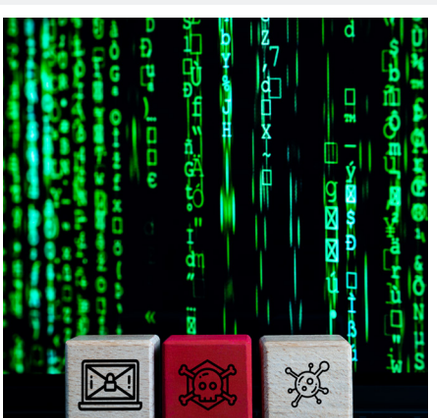
Le secrétaire général désigné de la CIMCT, le major général pilote Mohammed bin Saeed Al-Mughidi, a reçu le mercredi 30 juin 2021 l'ambassadeur du Japon au Royaume, M. Iwai Fumio et la délégation l'accompagnant.

Le diplomate a écouté une explication détaillée des efforts de la Coalition dans ses quatre domaines d'action (idéologique, médiatique, LFT et militaire), et pour coordonner l'action des États membres.

Le général Al-Mughidi a indiqué que la CIMCT offre un système intégré visant à renforcer la coopération entre les États membres dans ses différents domaines, tout en fondant son action sur les valeurs de légitimité, d'indépendance et de compatibilité avec les réglementations, normes et lois internationales.

P. 2 Course effrénée

P. 4 Guerre idéologique



P. 8 Le cyber-terrorisme

COURSE EFFRÉNÉE

RÔLE DES TECHNOLOGIES ÉMERGENTES DANS LA DÉTECTION PRÉCOCE DES CONTENUS EXTRÉMISTES

Confronter les thèses et discours des organisations terroristes sur Internet est l'un des axes de travail de la CIMCT qui a organisé une conférence intitulée (Rôle des technologies émergentes dans la détection précoce du contenu extrémiste et terroriste à travers les réseaux sociaux), présentée par Dr Majdal bin Sultan bin Safran, professeur d'intelligence artificielle à l'Université Roi Saoud, le 5 juillet 2021 au siège de la Coalition Islamique à Riyad.

Le conférencier a indiqué au début que les réseaux sociaux sont devenus un acteur important et influent dans les médias: Facebook compte 7,2 milliards d'utilisateurs, YouTube 2,2 milliards, WhatsApp 2 milliards, Messenger 1,3 milliard et Instagram 1,2 milliard.

Plus de 3,96 milliards d'utilisateurs mensuels sont actifs sur ces plateformes dont l'utilisation continue d'augmenter rapidement. Les autorités concernées devraient donc s'empresser d'activer l'utilisation des technologies émergentes dans la lutte contre le terrorisme à travers ces réseaux.

Terrorisme et réseaux sociaux

La ministre britannique de l'Intérieur Amber Rudd a décrit la lutte contre les contenus extrémistes sur Internet comme une course aux armements entre les extrémistes et les organes d'application de la loi et de l'ordre. Elle a révélé que depuis le début de 2017 jusqu'en novembre de la même année, des éléments extrémistes violents ont créé près de 40 000 nouveaux sites Web et applications sur Internet. Comme toute course aux armements, cela fait appel aux dernières technologies. En 2017, le projet d'intelligence artificielle "IA Conversation" a été créé.

Il s'agit d'un projet de recherche qui vise à découvrir et à supprimer au maximum les contenus extrémistes sur Internet qui ne cessent de croître. Le recours à l'apprentissage automatique pour l'accomplissement de cette tâche a contribué de manière significative à réduire le volume important de ce contenu.

Les géants de la technologie, menés par Microsoft, Google, Facebook, Amazon et Twitter, ont annoncé leur soutien à l'initiative internationale connue sous le nom de (Christchurch Call), qui encourage la lutte contre les contenus extrémistes sur Internet, en vertu de laquelle ces entreprises s'engagent à constamment mettre à jour leurs conditions d'utilisation, diversifier les moyens de signaler les contenus extrémistes et investir dans les technologies de surveillance.

La Direction exécutive de lutte contre le terrorisme des Nations Unies a lancé l'initiative «Technologie de lutte contre le terrorisme », qui surveille activement plus de 500 chaînes extrémistes réparties sur plus de 20 plateformes de contenu et applications de messagerie.

Les organisations terroristes bénéficient de ces réseaux pour réduire leur fardeau financier, renforcer leur identité collective et accélérer l'accès à tous les groupes. Cela leur permet aussi d'atteindre nombre d'objectifs tels que la coordination, le recrutement d'adeptes, la diffusion d'idées, la formation virtuelle de leurs adeptes et l'obtention du soutien financier et moral.

L'intelligence artificielle

Les techniques d'intelligence artificielle (IA) sont devenues les technologies émergentes les plus importantes dans la lutte contre les contenus extrémistes sur Internet. Environ 99 % du contenu d'al-Qaïda et de Daech supprimé de Facebook a été découvert par des systèmes d'intelligence artificielle avant d'être découvert par des humains, selon le témoignage de Zuckerberg lors de la session du Sénat américain.

Parmi les avantages de l'IA qui en ont fait la meilleure arme pour lutter contre le terrorisme dans le monde du Big data, ses capacités à détecter automatiquement les contenus, les tendances et les communautés virtuelles extrémistes et terroristes, et à anticiper et prévenir l'avenir les risques terroristes ou en atténuer l'impact.

L'IA produit des prédictions précises permettant de réduire les mesures inutiles appliquées à une grande partie de la population, les biais humains dans la prise de décision et le nombre de citoyens soumis à la surveillance.

Les capacités prédictives de l'IA ont été confirmées. Les services de sécurité et de renseignement utilisent l'analyse automatisée des données pour évaluer les risques des voyages aériens et révéler les liens entre les organisations terroristes et leurs membres. Certaines entreprises technologiques utilisent ces capacités pour perturber les activités terroristes sur les plateformes de médias sociaux, et le secteur financier les utilisent pour signaler toute activité financière suspecte.

L'IA est également utilisée pour analyser les réseaux sociaux, identifier les suspects et leurs relations en ligne, classer leurs caractéristiques, analyser leur relation de communication et détecter les tendances extrémistes dans les communautés virtuelles. La National Security Agency des États-Unis a utilisé le logiciel SKYNET usant d'un algorithme d'IA, pour analyser les métadonnées de 55 millions d'utilisateurs de téléphones portables nationaux dont environ 15 000 ont été identifiés comme des terroristes potentiels.

Grâce à l'IA, Facebook a réussi à réduire le temps moyen d'identification des vidéos qui violent ses règles de diffusion en direct à seulement 12 secondes, soit à 90 % par rapport à avant.

Le conférencier a passé en revue les techniques de traitement du langage naturel et leur impact sur la lutte contre les contenus extrémistes sur Internet. L'IA nous permet de former les appareils à comprendre notre langage et à découvrir des informations dans de très grands groupes de textes sans intervention humaine en utilisant les différents schémas linguistiques à caractère extrémiste et terroriste.

Défis de l'utilisation de l'intelligence artificielle

Malgré les progrès réalisés, les technologies IA de lutte contre les contenus extrémistes et terrorisme sur Internet se heurtent encore à des problèmes d'analyse des contenus linguistiques, notamment avec la diffusion de langues hybrides comme le franco-provençal et les dialectes familiers, ou le recours aux signaux et images non verbaux, qui entravent l'analyse automatisée de contenus énormes et très développés, impossibles à maîtriser uniquement par les capacités humaines. Nous avons encore un long chemin à parcourir pour atteindre des modèles capables de saisir le sens implicite et précis du langage et d'aller au-delà de la mémorisation de mots et de phrases spécifiques pour pouvoir interpréter les données en contexte, facteur clé pour comprendre les comportements en ligne.

Adam Hadley, directeur exécutif de l'initiative (Tech Against Terrorism) lancée par la Direction exécutive de lutte contre le terrorisme des NU, souligne un sérieux défi auquel est confronté le retrait du contenu extrémiste d'Internet, à savoir que les gouvernements occidentaux n'ont désigné que quelques organisations et groupes comme terroristes. Il estime que le classement des organisations d'extrême droite dans la liste des groupes terroristes aide les petites plateformes de médias sociaux vulnérables à l'exploitation par l'extrême droite, à supprimer les contenus violents sans faire face à des pressions ou des défis.

Claudia Wallner, analyste au sein du groupe de recherche sur le terrorisme et les conflits de l'Institut Royal des services unis pour les études de défense et de sécurité (RUSI), est pessimiste quant au succès de la nouvelle stratégie de l'UE visant à supprimer le contenu terroriste, à cause de l'ambiguïté de définition du contenu extrémiste ou terroriste, l'utilisation par les gouvernements de diverses définitions et les listes de classification nationales qui ne comprennent souvent qu'une petite partie des groupes extrémistes ou terroristes actifs.

Il est difficile de détecter le contenu extrémiste dans ce que l'on appelle (le contenu de la zone grise), publié par les groupes et les individus extrémistes, et qui ne comprend ni par déclaration ni par insinuation, d'incitation à la violence ou à la haine, mais utilise l'humour et l'ironie pour cacher leurs intentions violentes.

Pire, la suppression du contenu extrémiste d'Internet pousse les extrémistes et les terroristes à migrer des grandes plates-formes vers des sites Internet plus sûrs, ce qui rend difficile pour les forces de l'ordre de détecter leurs activités.

Les petits sites de réseaux sociaux sont désormais plus attractifs et utilisés par Al-Qaïda, Daech et les groupes d'extrême droite en raison de leurs ressources limitées leur permettant de supprimer le contenu terroriste.

GUERRE IDÉOLOGIQUE

ARGUMENTS SPÉCIEUX DES GROUPES TERRORISTES ET COMMENT Y REMÉDIER

La défaite des organisations terroristes ne se fait pas en détruisant leur machine de guerre ou en les expulsant des zones qu'elles contrôlent, car aucune organisation terroriste n'a pu vaincre un État ou préserver une terre qu'elle a prise à un État, mais on peut les vaincre en réfutant leurs arguments spécieux et en confondant leur idéologie, dans ce qu'on appelle la guerre idéologique, permettant non seulement d'immuniser les gens contre leurs idées fallacieuses, mais aussi de libérer les jeunes dupés de leur sujétion.

La CIMCT s'est engagée à confronter les idées des organisations terroristes à travers l'un de ses quatre principaux domaines d'action. Dans ce cadre, elle a tenu, le 8 juillet 2021, une conférence intitulée (Arguments spécieux des groupes terroristes et leur rôle dans la manipulation des jeunes), présentée par Dr Ibrahim bin Muhammad Al-Mayman, professeur des dogmes à l'Université Islamique Imam Muhammad bin Saoud, et ancien vice-recteur de l'Université, qui a traité dans son allocution les arguments trompeurs les plus importants des organisations terroristes, leur réfutation et l'approche de traitement religieux des arguments spécieux d'extrémisme et de terrorisme.

Audace du Takfirisme

Au début de la conférence, Dr Al-Mayman a souligné que les arguments spécieux des groupes terroristes sont anciens mais se renouvellent constamment et se déguisent pour se conformer à la réalité de l'époque, comme de se targuer de défendre les droits de l'homme et les droits civils pour atteindre leurs objectifs visant à jeter l'anathème sur les régimes, les dirigeants et les peuples, et se donner le droit de verser le sang, s'accaparer les biens, violer l'honneur et financer les opérations terroristes.

Dr Al-Mayman a passé en revue les faux arguments des groupes terroristes dont le plus important est le Takfir (excommunication, taxer le musulman de mécréant) prétendant que puisque les contredits de l'islam sont confirmés par les oulémas, le Takfir est un droit pour tout musulman en obéissance à Dieu et à son messager (S) à l'encontre de quiconque commet ces contredits, et que tout musulman a le droit de tuer.

La réfutation de cet argument fallacieux se résume ainsi:

- L'un des objectifs de la charia est d'appeler à la tolérance et la miséricorde et d'inviter les gens au bien au lieu de les débouter.
- Le Takfir est un aspect de la science juridique spécialisée dont la compétence revient aux scholastiques et aux juges par voie de nomination pour régler les affaires des gens, et pour éviter tout débordement et tout chaos.
- Nul n'a le droit, par caprice ou soupçon, de taxer quiconque de mécréant, à part celui que Dieu et Son Messager (S) ont explicitement qualifié de mécréant, car la peine capitale est un châtiment spécifique bien déterminé, décidée par l'Etat à travers l'autorité judiciaire, et personne n'a le droit d'enfreindre cette disposition.
- Le musulman a la foi par principe, et il n'est pas permis de le déclarer mécréant par simple doute, illusion ou soupçon.
- Les annulations de la foi mentionnées par les savants sont similaires à la mécréance d'action, et non de principe, et il n'est permis à aucun musulman de proclamer le Takfir en soi, à moins qu'il ne soit un érudit bien établi.
- Le Takfir dans la charia est un cadre étroit, autorisé uniquement selon des conditions très strictes, à la lumière de la violation du caractère sacré de la religion, en guise de parade, et il n'est pas une arme pour mater les gens et semer la zizanie dans la société.

Argument spécieux de gouvernance

Les groupes terroristes promeuvent l'argument mensonger de gouverner par

d'autres lois que celles révélées par Dieu (Al-Hakimiyya), slogan promu antan par les Kharijites, et moyen pour réaliser des objectifs politiques car il permet de discréditer les régimes et les gouverneurs.

La réponse à cette accusation est que cet argument en soi ne fait nullement partie des annulateurs de la foi, comme démontré par les érudits et les chercheurs dans les affaires des sectes qui estiment que ce jugement ne fait pas sortir du giron de l'Islam. Même si la question est considérée comme un point de vue, la base de blasphème dans cette question (de l'avis de nombreux érudits) est le déni et l'altération, et non le simple fait de gouverner par d'autres lois que celles révélées par Dieu.

Il n'est pas de même admis, comme le prétendent les extrémistes et les fanatiques, que les règlements et les lois dans les pays arabes et islamiques s'apparentent à celles que Dieu n'a pas révélées. Il s'agit d'une grave erreur car les systèmes de ces pays tirent leurs dispositions et leurs lois en général des objectifs et des dispositions de la charia, en particulier les lois sur le statut personnel qui se basent toutes sur la jurisprudence islamique.

Loyauté et désaveu

Le troisième argument spécieux des groupes extrémistes est celui de la loyauté et du désaveu, qui est un principe religieux, mais les membres de ces organisations le présentent de manière pervertie, à travers son aspect émotionnel, et l'utilisent pour isoler les jeunes de leurs pays et sociétés, alors que ce principe islamique préserve en fait l'identité religieuse sans impliquer ni exclusion, ni discrimination, car les droits des non-musulmans sont préservés et protégés par la charia.

De ce faux argument découle l'argument spécieux de l'appartenance nationale, prétendant qu'il s'agit d'une affiliation anti-islamique (relevant de la Jahiliya, l'ère avant l'islam) qui contredit la fraternité en Dieu et viole l'unité religieuse, de sorte que cette prétention rompt le lien du jeune avec sa patrie, l'isole de son État et de sa société et le rend vulnérable à la délinquance et au recrutement contre pays. Or, la thèse islamique se basant sur le Coran et la Sunna décrète que la patrie est un besoin humain qui fait partie de la nature de l'homme, sachant que l'Islam ne contredit jamais la nature humaine et renforce cette affiliation pour réaliser le but de la création, qui est la servitude envers Dieu Tout-Puissant.

En témoigne l'amour du Messager d'Allah (S) pour son pays nata l et sa patrie bien qu'il soit envoyé à tous les peuples du monde.

L'illusion d'un prétendu conflit entre appartenance à la patrie et fidélité à la religion est une erreur fatale, car les deux affiliations sont complémentaires et non contradictoires.

Manipulation du Jihad

Les groupes terroristes prétendent par ailleurs que les Etats entravent le Jihad, culte valable jusqu'au jour de la résurrection, ne nécessitant aucune autorisation si des non-musulmans s'attaquent aux musulmans.

Dr Al-Mayman réfute cet argument en affirmant que le Jihad est une prérogative de l'État au pouvoir, dont le recours varie en fonction de la force ou la faiblesse de l'État. Le Jihad est un moyen et non une fin en soi, qui est régi par des pactes, des chartes et la conjoncture internationale, sachant que le respect des pactes est un principe islamique, qui assure la stabilité de l'État , de sorte que le Jihad nécessite l'autorisation du gouverneur, or le rejet de cette autorisation par les groupes terroristes se base sur le Takfir de ceux qui n'appliquent pas selon eux la loi de Dieu.

Le Jihad est une décision juridique régie par des dispositions, qui vise surtout à repousser l'agression contre les terres islamiques et la violation par les infidèles des pactes et ne se base point sur les émotions et l'enthousiasme.

Approche de réfutation

Après avoir examiné et réfuté ces différents arguments spécieux des groupes terroristes, al-Mayman a mis l'accent sur les caractéristiques de ces allégations imprégnées de passion et visant à susciter l'enthousiasme, ce qui est l'apanage des gens égarés dont Allah dit: {Les gens qui ont au cœur une inclination vers l'égarement, mettent l' accent sur les versets à équivoque} agissant de mauvaise foi e {cherchant la dissension en essayant de leur trouver une interprétation} pour en faire une sorte de caprice répréhensible, dont Allah dit: {Vois-tu celui qui prend sa passion pour sa propre divinité? Et Allah l'égare sciemment}.

Pour que la réfutation de ces allégations soit efficace, elle doit se fonder sur le saint Livre et la Sunna, les objectifs fondamentaux de la charia islamique, les règles jurisprudentielles et les avis antérieurs et postérieurs, tout en étant attractif et réaliste et jouir d'une compréhension intégrative qui tient en compte les causes et les aspects du problème, selon une perception globale de l'allégation, de son affiliation et de ses motifs.

DÉFIS FUTURS!

LES DRONES, ARMES À VENIR DES TERRORISTES

Les drones ont donné aux terroristes la possibilité de développer leurs attaques terroristes, ce qui pourrait en faire leur arme de prédilection à l'avenir. Si les terroristes utilisent dans la plupart de leurs attaques, des armes susceptibles de conduire à leur arrestation ou leur mort, ce qui les incite à mener des opérations suicides, le recours aux aéronefs sans pilote pourra leur permettre de lancer de nombreuses attaques efficaces, sans avoir besoin d'opérations suicides ni craindre d'être arrêtés.

Développement effréné

Entre 1994-2018, il y a eu environ 14 attaques terroristes ou tentatives d'attentats, à différents endroits, à l'aide de drones. En 1994, le groupe japonais "Aum Shinrikyo" a essayé d'utiliser un hélicoptère télécommandé pour pulvériser du gaz sarin, mais la tentative a échoué et l'hélicoptère s'est écrasé. En 2013, les forces de l'ordre ont mis fin à une attaque planifiée d'Al-Qaïda au Pakistan à l'aide de drones. En 2014, Daech a commencé à utiliser des drones commerciaux à grande échelle dans des opérations militaires en Irak et en Syrie. En août 2018, deux drones chargés d'explosifs ont été utilisés lors d'une tentative infructueuse pour l'assassinat du président vénézuélien Maduro.

La diffusion rapide des drones a conduit à l'émergence d'un marché actif, ce qui pousse à développer techniquement ces avions, comme d'améliorer leur portée et leur charge utile, les rendant plus meurtriers et plus difficiles à contrer. Les nouveaux modèles de drones sont désormais capables de soulever 227 kg, se déplacer à des vitesses de plus de 129 km/h, avec **une autonomie de 16 km.**

De nombreux drones modernes sont commandés à travers la large gamme de fréquences radio (RF), ce qui permet de les contrôler avec précision et de transmettre des informations et diffuser des images en direct. L'un des derniers développements dans les technologies de ces avions est la possibilité de lancer plusieurs avions simultanément, ce qui pose un défi pour les capacités de défense. En 2018, un escadron de 13 drones a attaqué deux bases russes en Syrie et tenté de lancer des missiles à une distance de plus de 50 km.

Grand intérêt

Compte tenu de l'importance de cette question, la CIMCT a tenu une conférence intitulée: **(Drones)**, présentée par le **Major-Général Pilote Alexus Grynkewich,** chef des opérations du US CENTCOM au siège de la Coalition à Riyad, le jeudi 29 juillet 2021.

Le conférencier a évoqué les causes du recours aux drones sur les champs de bataille modernes, ce qui incite les groupes terroristes à utiliser cette technologie, les menaces potentielles de ces types d'appareils et les mesures préventives à prendre pour faire face aux drones des terroristes.

Au début de la conférence, le général Grynkewich a salué les efforts déployés par la CIMCT, pour contrer le terrorisme et a dit: « Quand je réfléchis aux domaines de lutte contre le terrorisme entrepris par la CIMCT, je constate qu'ils correspondent aux domaines d'action requis pour faire face à une cette nouvelle menace de drones, à laquelle bientôt de nombreux pays seront confrontés, vu que ces avions se propagent dans le monde entier. »

Le conférencier a passé en revue les types, les tailles et les moyens d'utiliser les drones, devenus une source majeure de menace pour la sécurité nationale de nombreux pays, en raison de leur large diffusion, leur faible coût d'achat, la facilité de les fabriquer et la possibilité de les utiliser dans diverses opérations : détection, reconnaissance, transport de marchandises et autres.

La propagation de l'industrie des drones a conduit à leur utilisation par les extrémistes pour commettre des actes illégaux comme le trafic de drogue et les opérations terroristes. Ces avions servent aussi à des fins de renseignement et de reconnaissance, et dans ce cas, pour obtenir des données permettant aux terroristes d'utiliser leurs armes contre nous.

Menaces complexes

Le général Grynkewich a souligné l'importance de l'élément de surprise dans les drones, ce qui rend leur menace dangereuse et complexe. Il a dit :"Les principaux aspects sur lesquels les terroristes s'activent, c'est de rendre notre tâche de défense plus compliquée et la menace de ces avions hautement complexe, bon marché et multiforme".

Ces drones sont également susceptibles de causer autant de dégâts que les bombardiers conventionnels. Et comme les drones utilisent le système de positionnement mondial (GPS) pour cibler leurs objectifs, leurs tirs sont désormais directs et précis, et causent des dommages de loin plus graves que les tirs chaotiques d'avant effectués par les groupes terroristes.

Cela nous rappelle la Seconde Guerre mondiale lorsque les Japonais menaient des attaques à l'aide d'avions kamikazes, mais les drones obtiennent le même résultat sans avoir besoin de pilote. Ils sont aussi similaires aux missiles de croisière, mais volent à basse altitude et lentement, et leur coût financier est de loin inférieur à celui de ces missiles.

Moyens de prévention

Le général Grynkewich a discuté des moyens de répondre à l'attaque aux drones et a présenté nombre de solutions dont notamment:

- Les terroristes ont besoin de fonds pour acheter des drones. Il faudrait donc les empêcher d'en avoir, ce qui est cohérent avec la lutte contre le financement du terrorisme visant à empêcher les fonds d'atteindre les groupes terroristes. Les Etats doivent également coopérer et surveiller la production industrielle des drones, afin d'éviter qu'ils ne tombent entre les mains de groupes terroristes.
- Le recours aux drones nécessite l'acquisition de connaissances techniques, pour savoir comment faire fonctionner ces avions, comment les programmer et les orienter vers la cible. Les terroristes peuvent recourir à l'auto-éducation sur les sites Web terroristes qui publient des clips de formation en ligne. Les autorités compétentes devraient intervenir pour bloquer ces sites et arrêter les opérations de formation électronique.
- Les groupes terroristes ont recours au stockage de drones après leur achat pour les tester, s'assurer de leur bon fonctionnement, savoir les utiliser avec précision, puis former leurs éléments à leur utilisation, d'où l'importance du suivi des zones de stockage par des systèmes de renseignement et d'information pour détruire ces appareils.
- Les groupes terroristes déplacent leurs plates-formes et leurs drones d'un endroit à un autre, ce qui nécessite des moyens (logistiques) importants, et si nous pouvons connaître les réseaux chargés du transport de ces équipements, et où ils sont déplacés, il sera possible d'arrêter ces technologies dès le début, de les désactiver et de les éliminer avant qu'elles n'atteignent le stade de lancement.

Questions et débats

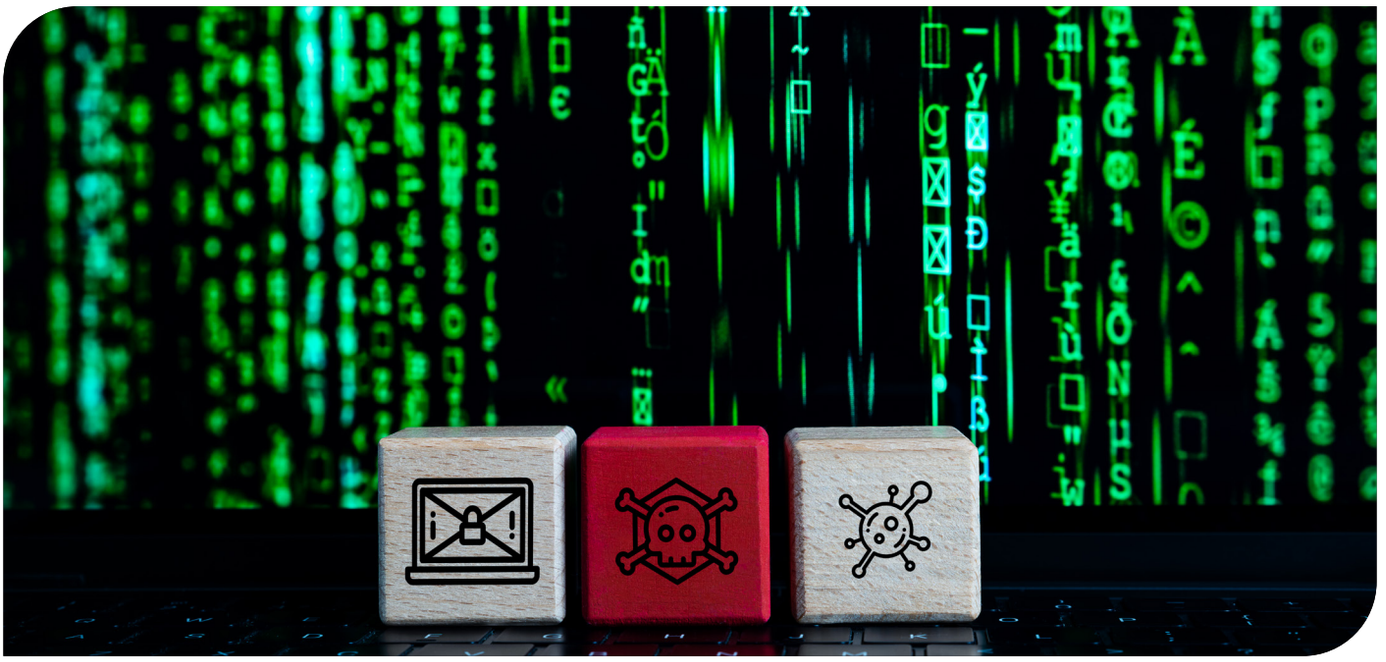
Dans les interventions à la fin de la conférence, le délégué de Bahreïn, le colonel pilote Ali Muhammad Mahmoud, a déclaré que le monde a été témoin lors de la cérémonie d'ouverture des Jeux Olympiques dans la capitale japonaise Tokyo (en 2021), de la participation d'environ 1824 drones, et si l'on imaginait que chacun de ces avions transportait à son bord 40 kilogrammes de matière explosive, serions-nous prêts à envisager une telle hypothèse ?

Le conférencier a répondu que non disant: « Je ne pense pas que nous soyons prêts à cela ! Nous avons vu de plus petits essaims d'attaques de drones de la part de groupes comme Daech, ou le mouvement armé Houthi qui a lancé des attaques avec un essaim de drones, comptant entre dix et vingt avions. En cas d'attaque d'essaim de drones, il sera peut être trop tard pour faire face à une telle offensive, et la meilleure défense appropriée sera la mobilisation de plusieurs capacités dont les techniques de détection précoce pour éliminer le plus grand nombre possible de cet essaim. L'élément clé pour contrer un essaim de drones est de commencer par empêcher aux terroristes l'accès à ces drones.

Le délégué du Royaume hachémite de Jordanie, le général de brigade Raed Al Marashda, a demandé au conférencier si l'intérêt accru pour les drones et le développement de leurs technologies réduiraient l'importance de l'armée de l'air conventionnelle. Alexus a répondu qu'à l'avenir, il y aurait beaucoup de drones dans toutes les forces aériennes, pour diverses raisons, notamment parce qu'ils sont moins coûteux en termes de fabrication et d'exploitation, mais si on exclut les drones du contexte du terrorisme et que l'on focalise sur les conflits entre États, ou les conflits au sens large, alors certains de ces avions ne sont pas adaptés à ce type de conflit.

Les capacités de puissance aérienne conventionnelle pourraient ajouter plus de technologies aux drones, comme la capacité de survie accrue. Il y aura également beaucoup de types de drones, mais les forces aériennes conventionnelles resteront actives et useront des technologies disponibles dans les drones, a-t-il conclu.

LE CYBER-TERRORISME
CHOIX DE PRÉDILECTION POUR LES TERRORISTES



M. Mahmoud Al Hamdan

La structure décentralisée d'Internet permet l'anonymat de l'usager, caractéristique vitale pour les activités illégales réussies qui rend de nombreuses cibles attractifs sur Internet très vulnérables au crime, et transforme le réseau en une plate-forme tenace pour promouvoir les objectifs de l'extrémisme violent. Par conséquent, cette exploitation insidieuse d'Internet pour promouvoir l'extrémisme violent et les nombreux avantages qu'il offre aux extrémistes sont devenus un défi urgent pour les gouvernements, car les terroristes cherchent à saper la légitimité des États et à briser le monopole traditionnel de la violence liée à leur autorité.

Entre récompenses et risques

Il ne fait aucun doute que le cyber-terrorisme est une menace nationale de premier plan pour les gouvernements, du fait de la dépendance du monde envers les systèmes informatiques. Les cibles principales de ce terrorisme sont les gouvernements et leurs institutions, les banques et les services publics, tels que : l'eau, l'électricité, le pétrole, le gaz et les infrastructures de communication, pouvant causer de graves dommages économiques, politiques et matériels.

Les groupes cyber-terroristes sont devenus plus performants et peuvent profiter de n'importe quel ordinateur connecté à Internet pour lancer des attaques contre les grandes institutions et les internautes.

Le cyber-terrorisme est désormais une option parce qu'il est moins cher que le terrorisme traditionnel, le terroriste ayant besoin uniquement d'un ordinateur personnel et d'une connexion Internet, et nullement d'armes à feu ou d'explosifs. La confection et la transmission d'un virus informatique par une communication téléphonique traditionnelle ou sans fil est une méthode terroriste électronique courante qui cause des dommages aussi graves que ceux causés par les armes et les explosifs.

Armes de cyber-terrorisme

Il existe toujours une ambiguïté concernant la définition d'une cyber-arme et si le terme était approprié pour désigner les logiciels utilisés à des fins malveillantes. Deux éléments importants ont été mis en évidence pour distinguer une arme d'un outil, qui est l'intention du contrevenant, élément essentiel du préjudice causé, ou de la menace de nuire à une victime, faisant partie intégrante de la définition de l'arme cybernétique.

Ainsi, si un marteau est utilisé pour causer des dommages corporels ou matériels, la définition du marteau changera pour le reconsidérer en tant qu'arme nocive. Cette logique s'applique également aux logiciels malveillants, et une cyber-arme doit être considérée comme telle, ce qui signifie que la perception de l'objectif de l'arme causant des dommages réels doit toujours être présente.

L'étendue des dommages causés par une cyber-arme s'appuie sur la dépendance de la population vis-à-vis du réseau ciblé par cette arme. Ainsi, les effets des cyber-armes ciblant les infrastructures critiques du pays, comme le réseau électrique, sont plus sévères. Compte tenu de la nature de ces armes, il existe un risque constant que des organisations terroristes en fassent l'acquisition. Ainsi, un groupe connu sous le nom de Shadow Broker a piraté l'Agence Américaine de Sécurité Nationale (NSA) et prétendu avoir volé des cyber-armes nationales dans le but de les vendre aux enchères, ce qui montre que ces armes cybernétiques peuvent devenir plus vulnérables à l'achat et à la vente illégaux que les armes conventionnelles.

Attaque de zéro et de bots

Les logiciels malveillants (Malware) est un terme générique pour tout type de logiciel conçu pour endommager ou exploiter un appareil, un service ou un réseau programmable. Ils sont couramment utilisés par les cybercriminels pour extraire des données

à utiliser à des fins financières. Ces données peuvent aller des données financières, aux dossiers de soins de santé, messages électroniques ou mots de passe personnels. Les informations qui peuvent être piratées sont infinies.

Les «Failles de la Journée Zéro» (Zero day exploits) indiquent une nouvelle vulnérabilité jusqu'alors inconnue et l'un des meilleurs moyens d'accéder aux systèmes et de les endommager. Cette vulnérabilité peut être exploitée par des pirates informatiques pour accéder à des informations restreintes et de créer et utiliser des logiciels malveillants et espions.

Les attaques par déni de service, vol de données, envoi de spams et autorisation à l'attaquant d'accéder à l'appareil peuvent également être exécutés par un botnet. Les bots ou robots sont des appareils connectés à Internet, exécutant une ou plusieurs missions que l'attaquant contrôle à l'aide d'un logiciel de commande et de contrôle.

Virus et bombes

Les virus sont les types de logiciels malveillants les plus connus et les plus anciens, qui s'attachent aux ordinateurs ou aux fichiers, se reproduisent pour se propager à d'autres fichiers ou ordinateurs, et ont la capacité de détruire ou d'effacer les données. L'ordinateur ne peut pas être infecté à moins que le logiciel malveillant ne soit exécuté. Le virus peut rester en sommeil jusqu'à ce que le fichier infecté ou la pièce jointe soient ouverts. Les virus nécessitent le concours de l'internaute pour infecter d'autres fichiers et systèmes, en exécutant le programme infecté dans une liste de diffusion.

Les terroristes utilisent souvent des bombes logiques pour se venger de la victime à travers le cyber-sabotage. Les bombes logiques peuvent également être utilisées de façon moins nocives, telles que pour les essais gratuits des programmes qui désactivent le logiciel après une date ou une durée prédéterminée. Les terroristes savent l'importance des bombes logiques car l'infrastructure de la plupart des pays du monde dépend des réseaux informatiques et qu'une série d'attentats à la bombe logique peut arrêter et désactiver de nombreux systèmes bancaires et de transport dans le monde.

Ciblage des infrastructures

Les infrastructures essentielles soutiennent les services de base dont la société a besoin, tels que les transports, l'énergie, la santé, etc., et de graves perturbations de ces services peuvent priver une grande partie de la population de nourriture, d'électricité et de carburant, ainsi que d'autres nécessités. Le recours des services aux chaînes logistiques électroniques amplifie les effets négatifs de toute cyberattaque à laquelle ils sont exposés, car ils représentent l'épine dorsale de l'économie du pays: sécurité, santé, énergie, eau, transport, navigation, communications, services bancaires et financiers.

Les infrastructures critiques sont de plus en plus vulnérables au cyber-terrorisme. L'inclusion de systèmes de contrôle industriels dans les infrastructures de communication publiques et la propagation de l'intelligence artificielle affectent la cyber-sécurité des infrastructures nationales, en raison de la forte augmentation de nouveaux systèmes électro-physiques pouvant être exposés aux nouvelles attaques, telles que de provoquer des accidents aux voitures autonomes.

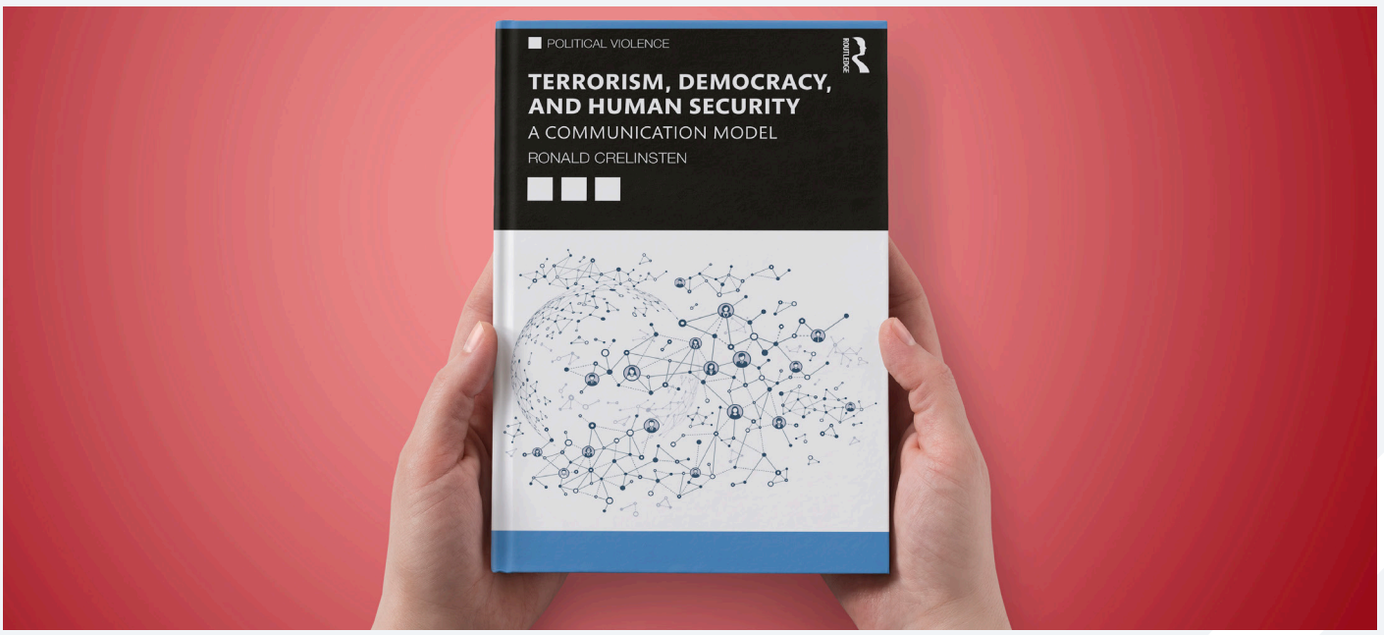
Le développement rapide et l'interdépendance des technologies sont également une source de préoccupation, en grande partie en raison de l'émergence de l'Internet des objets qui a créé de nombreux nouveaux vecteurs d'attaque que les cybercriminels et les terroristes peuvent exploiter.

Le 8 avril 2020, l'Agence pour la cyber-sécurité et la sécurité des infrastructures et le Centre National de Cyber-sécurité au Royaume-Uni ont émis un avertissement concernant les incidents de sécurité qui ont ciblé l'infrastructure vitale des agences de soins de santé et pharmaceutiques, telles que les entreprises, instituts de recherche médicale et universités, à la suite de l'émergence du (Covid-19). Aux États-Unis, la santé n'était pas le secteur d'infrastructure le plus critique ciblé par les cyber-attaquants. En mars 2019, les attaquants ont profité d'une faille dans le pare-feu pour créer des angles morts pour les opérateurs de réseaux électriques pendant environ 10 heures.

En février 2021, des pirates ont infiltré une station d'eau d'une petite ville de Floride pour élever le niveau d'hydroxyde de sodium à 11.100 parties par million, ce qui est un niveau élevé et dangereux, heureusement, l'attaque a été détectée avant qu'elle ne se produise. Le même mois, le Département de Sécurité Intérieure a révélé une attaque de ransomware ciblant l'infrastructure critique d'une installation de compression de gaz naturel. L'assaillant a utilisé l'hameçonnage, attaque conçue pour amener les gens à fournir des informations sensibles telles que des mots de passe, pour accéder aux réseaux de l'établissement, ce qui a entraîné la fermeture de l'établissement pour deux jours.

Une tactique similaire d'hameçonnage a été utilisée dans d'autres attaques à l'échelle nationale ciblant le personnel ayant un accès privilégié aux contrôles critiques dans de nombreuses centrales nucléaires dont la Société d'exploitation nucléaire de Wolf Creek au Kansas.

DILEMME DU TERRORISME DANS LES DÉMOCRATIES LIBÉRALES



Si vous souhaitez comprendre les dilemmes des démocraties libérales face au terrorisme, ce livre vous offre l'analyse la plus approfondie et la plus complète. Son auteur a passé quatre décennies dans la recherche spécialisée dans le domaine de la lutte contre le terrorisme, fournissant de nouvelles perspectives sur l'un des problèmes les plus complexes et les plus persistants de l'agenda mondial.

Dans son livre "Terrorisme, Démocratie et Sécurité Humaine: Modèle de Communication", l'auteur, Dr Ronald Crelinsten, affirme que le terrorisme doit être compris de manière multiforme et amène le lecteur à comprendre l'interrelation entre le terrorisme et l'économie, vie sociale, culturelle et politique, la relation entre terrorisme et contre-terrorisme, et l'impact de cette relation dans le contexte plus large de la communication, du contrôle, du pouvoir et de la gouvernance démocratique, aux niveaux national et international.

Crelinsten cherche à présenter une théorie du terrorisme et du contre-terrorisme, non seulement en tant que sorte de menace pour la vie démocratique et la liberté individuelle, mais aussi comme une forme de communication violente ou de persuasion coercitive visant à contraindre les victimes directes à se conformer ou à répondre aux demandes, intimider un public plus large, ou exciter et impressionner (pour attirer l'attention).

L'auteur considère que le terrorisme et la lutte contre ce phénomène sont un type de communication qui interagit et se développe au fil du temps entre le gouvernant (l'État) et les gouvernés (le peuple, dont les terroristes). Par conséquent, il présente un cadre innovant qui définit le contexte dans lequel le terrorisme et l'antiterrorisme interagissent, évoluent à travers des modèles qui passent de la vision locale à la vision globale, dans un contexte plus large de la vie sociale, culturelle, politique et économique, en pleine conscience des conditions et des faits à plusieurs niveaux, devenus un mélange de positions et de points de vue.

L'auteur, ancien professeur de criminologie à l'Université d'Ottawa et chercheur associé à l'Université Victoria au Canada, présente la relation entre le terrorisme et l'antiterrorisme dans un large éventail de domaines : politique, militaire, social, économique, et environnemental. Il passe du niveau micro au niveau macro. Son livre examine le concept de sécurité humaine qu'il relie aux droits et besoins de l'homme, dont en premier rang d'être à l'abri de la peur et de la misère. Il aborde le défi de définir des valeurs et des normes mondiales dans la lutte contre le terrorisme, sur fond de militarisation ayant suivi les attentats du 11 septembre 2001.

Le livre explore les problèmes conceptuels entourant l'étude du terrorisme, tels que les causes profondes du terrorisme, le terrorisme d'État, la question de savoir si le terrorisme est intrinsèquement un phénomène illégal ou criminel, et d'autres formes de contact violent non politique ayant le terrorisme pour point d'intersection. Il traite des divers défis auxquels est confronté le système de gouvernance démocratique réussi dans l'environnement de sécurité complexe du XXIe siècle et examine les moyens de fonctionnement de la gouvernance démocratique au sein de systèmes adaptatifs complexes d'acteurs étatiques et non étatiques visant à contrôler ou prévenir l'extrémisme violent et le terrorisme.

L'ouvrage analyse les relations internationales, bilatérales, multilatérales et intergouvernementales qui encadrent le terrorisme et l'antiterrorisme, et constate que les interactions d'État à État sont beaucoup plus complexes que les relations bilatérales (horizontales) entre deux États, et incluent différents niveaux de bureaucratie qui peuvent interagir avec des niveaux de gouvernement similaires dans d'autres pays, en particulier dans des entités telles que les organisations internationales ou régionales.

Il analyse également les relations sociétales civiles, transnationales et internationales, les manières dont les acteurs non étatiques de différents États interagissent en dehors de leurs propres frontières et leur impact sur le terrorisme international. Certaines de ces interactions incluent des sujets tels que : les flux migratoires, les médias sociaux, le crime organisé transnational, le trafic de drogue, la piraterie, la cybercriminalité, les combattants étrangers et d'autres sujets pertinents.

PRÉVENIR, DÉTECTER ET RÉAGIR CONTRE L'EXTRÉMISME VIOLENT

Le Centre de formation professionnelle de l'Université de Leiden et le Centre international de lutte contre le terrorisme à La Haye (ICCT) organisent un programme de formation virtuelle sur Internet, du 16 au 18 août 2021, dans le domaine de la détection, prévention et lutte contre l'extrémisme violent (EV).

Le programme traite des dilemmes les plus importants découlant de l'extrémisme et du terrorisme, et des dernières tendances dans le domaine de la prévention de l'EV, tout en présentant différentes perspectives sur l'extrémisme et le contre-extrémisme, ainsi que sur la réhabilitation sociale. Il analyse les opportunités et les défis des approches antiterroristes, et les différentes fonctions et visions des acteurs actifs dans ce domaine. Le programme comprend des conférences, sessions de travail et tables rondes, pour échanger les idées, les visions et les expériences avec les praticiens, les chercheurs et les spécialistes.

Le programme sera animé par Bart Schurmann, professeur agrégé à l'Institut de Sécurité et des Affaires Mondiales, Université de Leiden, et Taher Abbas, professeur agrégé au même institut. Il permet aux participants de découvrir les dernières tendances de la recherche dans le domaine antiterrorisme et d'explorer les différentes fonctions et contraintes des parties prenantes et des approches en vigueur.

Le programme devra offrir aux participants:

- Aperçu sur les derniers dilemmes et tendances dans le domaine de l'extrémisme et de la prévention de l'EV.
- Perception des opportunités et des défis dans les différentes méthodes de détection, de lutte et de prévention de l'EV.
- Une bonne compréhension des différentes organisations et parties prenantes travaillant dans le domaine de la prévention de l'extrémisme et de l'EV, et leurs différentes fonctions.
- Apprendre comment concevoir des interventions politiques visant à détecter, prévenir et réagir rapidement à l'EV, tout en respectant les valeurs éthiques et les lois internationales.
- Une connaissance claire et approfondie de la contribution de chaque membre de la société à la prévention et à la lutte contre l'extrémisme et l'EV.

Ce programme intéressera les: praticiens antiterrorisme, décideurs internationaux, régionaux et nationaux antiterrorisme, diplomates, journalistes, universitaires, chercheurs et professionnels désireux d'élargir leur compréhension des défis de prévention de l'EV.

CONFÉRENCE DE STOCKHOLM SUR LA SÉCURITÉ SIXIÈME SESSION EN NOVEMBRE PROCHAIN

Les développements modernes actuels dans le cyber et le cyberespace ont ouvert de nouveaux champs de bataille potentiels dans un avenir proche, et les développements rapides dans le domaine de la technologie ajoutent plus d'incertitude et un besoin accru de comprendre et de gérer la nouvelle conjoncture, en particulier à la lumière du niveau accru de méfiance entre les grandes puissances.

Ainsi, l'Institut international de recherche sur la paix de Stockholm (SIPRI) organise la 6ème Conférence de Stockholm sur la sécurité internationale du 8 au 11 novembre 2021, sur le thème : (Champs de bataille de l'avenir: Tendances des conflits et de la guerre au XXIe siècle). La rencontre vise à explorer les moyens de prévenir les dangers de l'extrémisme et du terrorisme et d'atténuer les destructions et les coûts humains élevés qui en résultent.

La conférence examine dans quelle mesure les types de guerre traditionnels s'adaptent aux nouveaux moyens disponibles ou offrent aux acteurs non traditionnels de nouvelles opportunités de remplir des fonctions plus pertinentes.

La conférence offre une plate-forme pour des discussions approfondies entre les principaux experts, praticiens et décideurs politiques, de différentes spécialisations et orientations pour mieux comprendre les enjeux de la sécurité internationale et la responsabilité des gouvernements, des organisations multilatérales, des acteurs, des chercheurs et de la société civile à faire face aux enjeux des champs de bataille de demain.

UNE DÉLÉGATION DU CCG EN VISITE À LA CIMCT

Une délégation du Secrétariat général du Conseil de Coopération des États Arabes du Golfe (CCG) a visité le siège de la CIMCT à Riyad, le jeudi 8 juillet 2021. Elle a été reçue par le major général Mohammed bin Saeed Al-Mughidi, secrétaire général désigné de la CIMCT, qui a expliqué à la délégation les efforts de la Coalition dans la lutte contre le terrorisme, et discuté avec elle des moyens de coopération conjointe entre la CIMCT et le CCG.

Le général Al-Mughidi a précisé que la Coalition suit une approche intégrée dans la lutte contre le terrorisme dans les domaines idéologique, médiatique, militaire et LFT pour atteindre au mieux ses objectifs.

LA CIMCT CÉLÈBRE LA FÊTE NATIONALE DES COMORES ET DES MALDIVES

Les délégués de la République des Comores et de la République des Maldives à la CIMCT à Riyad ont célébré respectivement les 6 et 27 juillet, les jours d'indépendance de leurs pays, en présence du Secrétaire général de la Coalition, des délégués des États membres et du personnel de la Coalition, qui leur ont souhaité, ainsi qu'à leurs peuples, sécurité et prospérité.