UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
Programme Office in Doha

OSCE PA
Organization for Security and Co-operation in Europe
PARLIAMENTARY ASSEMBLY

مجلس الشورى
The Shura Council
State of Qatar • دولة قطر

Parliamentary Engagement
in Preventing and Countering Terrorism

الوثيقة الختامية

الحوار البرلماني الرابع بشأن سياسات
مكافحة استخدام الذكاء الاصطناعي
والتقنيات الجديدة لأغراض إرهابية

روما، إيطاليا
5 كانون الأول/ديسمبر 2024

لا تمثل هذه الوثيقة استنتاجات رسمية، ولا تقدم سجلاً شاملاً لجميع القضايا التي نوقشت أثناء الحوار البرلماني بشأن السياسات. ويقصد منها أن تكون بمثابة مجموعة من النقاط ذات الصلة والاستنتاجات والتوصيات التي يمكن الرجوع إليها مستقبلاً. وفي حين يسعى مكتب الأمم المتحدة لمكافحة الإرهاب لضمان دقة المعلومات المقدمة وصلتها، فإنه لا يدعي، ولا يقدم أي ضمانات، صريحة أو ضمنية، بشأن كمال هذه المعلومات أو دقتها أو موثوقيتها. ووجهات النظر والتوصيات المتضمنة مدرجة فقط كمرجع ولا ينبغي تفسيرها على أنها نهائية أو شاملة.

ملخص تنفيذي

قام مكتب برنامج إشراك البرلمانيين في منع الإرهاب ومكافحته التابع لمكتب الأمم المتحدة لمكافحة الإرهاب ووحدة أمن الفضاء الإلكتروني والتقنيات الجديدة التابعة لمكتب مكافحة الإرهاب، بدعم من مجلس الشورى بدولة قطر، وبالتعاون مع الجمعية البرلمانية لمنظمة الأمن والتعاون في أوروبا، بتنظيم الحوار البرلماني الرابع بشأن السياسات بعنوان "مجابهة استخدام الذكاء الاصطناعي والتقنيات الجديدة لأغراض إرهابية." ضمت الفعالية، التي استضافها البرلمان الإيطالي في روما في 5 كانون الأول/ديسمبر 2024، أكثر من 70 مشاركاً حضورياً، و10 مشاركين عبر الإنترنت، منهم ممثلين للجمعيات البرلمانية والبرلمانات الوطنية عبر أفريقيا وآسيا وأوروبا، بالإضافة إلى كبار الخبراء من وكالات الأمم المتحدة ذات الصلة، والمنظمات البحثية الدولية والجهات الأكاديمية.

وقد شارك ممثلون من أربعة عشر جمعية برلمانية، منها الاتحاد البرلماني الأفريقي والاتحاد البرلماني العربي، والبرلمان العربي، و الجمعية المشتركة بين برلمانات البلدان الأعضاء في رابطة أمم جنوب شرق آسيا والجمعية البرلمانية للفرنكوفونية، والبرلمان الأوروبي، والجمعية المشتركة بين برلمانات الدول الأعضاء في رابطة الدول المستقلة، والجمعية البرلمانية للتعاون الاقتصادي في منطقة البحر الأسود، والجمعية البرلمانية لمجلس أوروبا، والجمعية البرلمانية للبحر المتوسط، والجمعية البرلمانية لمنظمة الأمن والتعاون في أوروبا، والجمعية البرلمانية لمنظمة التعاون الإسلامي، والجمعية البرلمانية للدول التركية، والمنتدى البرلماني للجماعة الإنمائية للجنوب الأفريقي. كما شارك أيضاً ممثلون من مجلس الشورى بدولة قطر.

شارك في الحلقة النقاشية المخصصة للخبراء ممثلين من مكتب الأمم المتحدة المعني بالمخدرات والجريمة، و المديرية التنفيذية للجنة مكافحة الإرهاب التابعة لمجلس الأمن، ومجلس النواب في البرلمان الإيطالي، ووكالة الأمن السيبراني الإيطالية، وغيرها من المنظمات ومُجمَّعات الفكر الدولية، مثل مركز جنيف للسياسات الأمنية ومختبرات ميثوس ومركز الدراسات العالمية بالجمعية البرلمانية للبحر الأبيض المتوسط واللجنة المخصصة لمكافحة الإرهاب التابعة للجمعية البرلمانية لمنظمة الأمن والتعاون في أوروبا.

تألف الحوار السياسي من ثلاث جلسات رئيسية:

1. التحديات والتهديدات العالمية والإقليمية المرتبطة باستخدام الذكاء الاصطناعي وغيره من التقنيات الجديدة لأغراض إرهابية؛
2. الممارسات الدولية والإقليمية البرلمانية الجيدة في مجال منع ومكافحة استخدام الذكاء الاصطناعي وغيره التقنيات الجديدة لأغراض إرهابية؛
3. الإطار القانوني الدولي لمنع ومكافحة استخدام الذكاء الاصطناعي وغيره من التقنيات الناشئة لأغراض إرهابية.

اختتم الحوار بتوصيات رئيسية بشأن منع ومكافحة استخدام المنظمات الإرهابية والمتطرفة للذكاء الاصطناعي والتقنيات الناشئة، مع التأكيد على الأدوار الحاسمة للبرلمانات الوطنية والجمعيات البرلمانية المتعددة الأطراف في تلك الجهود.

تقارير الجلسات

الجلسة الأولى. التحديات والتهديدات العالمية والإقليمية المرتبطة باستخدام الذكاء الاصطناعي وغيره من التقنيات الجديدة لأغراض إرهابية

قدمّت الجلسة نظرة شاملة على التحديات الحالية والناشئة التي تواجه الأمن العالمي والإقليمي والناجمة عن إساءة استخدام الذكاء الاصطناعي، وغيره من التقنيات الناشئة، لأغراض إرهابية. أكد المشاركون على الأثر التحويلي لهذه التقنيات على الطبيعة المتحولة للإرهاب وعلى تداعياتها الهامة بالنسبة للأمن القومي للدول الأعضاء.

استكشفت المناقشات التهديدات العالمية المرتبطة بالأدوات المدفوعة بالذكاء الاصطناعي، مثل اختلاق ونشر المعلومات المضللة والدعاية الزائفة والتزييف العميق، والتي يتزايد استخدامها في التجنيد والدفع نحو التطرف. كما أثيرت مخاوف بشأن ميكنة

هذه الوثيقة هي ترجمة غير رسمية مقدَّمة للأغراض الإعلامية فقط. وفي حالة وجود أي تعارض أو غموض، فإن النسخة الأصلية باللغة الإنجليزية هي التي تسود.

الهجمات من خلال الطائرات المُسيرة المزودة بالذكاء الاصطناعية والأنظمة الآلية. وقد جرى تحديد أوجه الضعف المرتبطة بالفضاء الإلكتروني، وبخاصة تلك التي تستغل أساليب الاختراق المحسنة بالذكاء الاصطناعي، والتي تستهدف البنية التحتية الحيوية، باعتبارها من القضايا العالمية المُلحة.

على المستوى الإقليمي، أبرز المشاركون أوجه التباين في القدرات التكنولوجية، والتي تؤدي إلى قدرات متفاوتة في مجال الكشف عن تهديدات الذكاء الاصطناعي ومجابهتها. وتؤدي أوجه التباين هذه إلى تفاقم تحديات إدارة المخاطر، مثل خوارزميات وسائل التواصل الاجتماعي التي عادة ما تُضخِّم المظالم المحلية، وتؤجِّج الاستقطاب والتطرف.

كما جرى التأكيد على تداعيات تلك التهديدات على الأمن القومي، حيث أشار المشاركون إلى زيادة المخاطر التي تتعرض لها البنية التحتية، مثل شبكات الطاقة والأنظمة المالية وشبكات الاتصالات. كما أشير إلى مدى تعقيد أساليب التخفي المعتمدة على الذكاء الاصطناعي كأحد التحديات الكبرى في مجال الكشف عن تلك التهديدات والتخفيف من آثارها.

وتضمنت النقاط الأساسية من المناقشات ما يلي:

- **الطبيعة المزدوجة للذكاء الاصطناعي**: يمثل الذكاء الاصطناعي فرصاً ومخاطر في آن واحد، مما يستلزم التنظيم المناسب من قِبل الحكومات.
- **النمو التكنولوجي السريع**: عادة ما يفوق النمو المطرد لتلك التقنيات سرعة إصدار التدابير التنظيمية، مما يخلق فجوات في الرقابة.
- **استخدام الذكاء الاصطناعي كسلاح**: تستغل المنظمات الإرهابية الذكاء الاصطناعي لإنتاج ونشر المُسيَّرات المزودة بالأسلحة والتزييف العميق في مناطق النزاعات. كما جرى تحديد بعض المخاطر الناشئة، مثل الإفساد المتعمد لأنظمة الذكاء الاصطناعي (مثل تسميم النماذج اللغوية الكبيرة الحجم).
- **استغلال الدعاية الكاذبة والتجنيد**: يتزايد استغلال المنظمات الإرهابية للذكاء الاصطناعي من أجل تحسين الدعاية الكاذبة وجهود التجنيد، مع حدوث تقدم كبير في استخدام التقنيات الجديدة لأغراض شريرة.

الجلسة الثانية الممارسات الدولية والإقليمية البرلمانية الجيدة في مجال منع ومكافحة استخدام الذكاء الاصطناعي وغيره التقنيات الجديدة لأغراض إرهابية

ركزت الجلسة على استعراض الممارسات البرلمانية الدولية والإقليمية الفعالة في منع ومكافحة استخدام الذكاء الاصطناعي وغيره من التقنيات الناشئة لأغراض إرهابية. كما استهدفت أيضاً تحديد الإجراءات اللازمة لتنفيذ إجراءات فعالة مضادة مع الحفاظ على التقدم التكنولوجي والنمو الاقتصادي. وبالإضافة إلى ذلك، استكشفت الجلسة الطرق التي يمكن للبرلمانيين والجمعيات البرلمانية استخدامها لدعم تلك الجهود على المستويين الوطني والدولي.

شهدت الجلسة عرضاً تقديمياً من الوكالة الوطنية الإيطالية لأمن الفضاء الإلكتروني، والتي تتناول القضايا المرتبطة بالإرهاب كجزء من ولايتها الأعم المتعلقة بأمن الفضاء الإلكتروني. تعمل الوكالة الوطنية لأمن الفضاء الإلكتروني على مجابهة التحديات المرتبطة بالذكاء الاصطناعي في إطار أمن الفضاء الإلكتروني وتولي الأولوية لتجب الأخطاء التي ارتكبت أثناء المراحل المبكرة من تطوير الإنترنت. في الوقت الحالي، تركز الوكالة على أهمية إعطاء الأولوية للأمن في التقنيات الناشئة للتقليل من أوجه الضعف. كما تسعى إلى تحسين التعاون بين الوكالات من أجل ابتكار استجابات فعالة للتحديات السريعة التطور. وإقراراً بالقدرة الهائلة لتلك التقنيات السريعة التطور على التسبب في فوائد وأضرار على حدٍ سواء، تستثمر الوكالة الوطنية لأمن الفضاء الإلكتروني في التنبؤ بتطور تلك التقنيات من أجل تقليل المخاطر الأمنية المحتملة.

كان القرار الذي أصدرته الجمعية البرلمانية لمنظمة الأمن والتعاون في أوروبا بعنوان "الذكاء الاصطناعي والحرب على الإرهاب" (والذي اعتمد في 29 حزيران/يونيو 2024، في بوخارست، رومانيا) موضوعاً رئيسياً للمناقشة أثناء الحوار وكان

هذه الوثيقة هي ترجمة غير رسمية مقدَّمة للأغراض الإعلامية فقط. وفي حالة وجود أي تعارض أو غموض، فإن النسخة الأصلية باللغة الإنجليزية هي التي تسود.

هناك إقرار بأنه يعد أحد أفضل الممارسات الدولية. يضع القرار إطاراً شاملاً للتعامل مع الفرص والمخاطر التي يفرضها الذكاء الاصطناعي في جهود مكافحة الإرهاب. وهو يؤكد على الحاجة لمجابهة التطرف والتطرف العنيف مع التمسك بحقوق الإنسان، والحريات الأساسية، وسيادة القانون. وإقراراً بإمكانيات الذكاء الاصطناعي في مجال تحسين الأمن، يتناول القرار أيضاً مخاطر إساءة استخدامه من قبل المنظمات الإرهابية لتنفيذ أنشطة مثل التخطيط والتجنيد ونشر الدعاية الكاذبة. ويدعو القرار لتقوية الأطر القانونية والآليات الرقابية لتنظيم تطوير الذكاء الاصطناعي واستخدامه، مما يضمن الشفافية، والامتثال الأخلاقي، والمساءلة. ويلقي الضوء على أهمية الشراكات بين القطاعين العام والخاص من أجل فرض الشفافية وتجنب المخاطر، مع تعزيز استخدام أدوات الذكاء الاصطناعي للكشف عن الأنشطة الإرهابية ومجابهتها. ومن أجل تعزيز القدرة المجتمعية على الصمود، يدعو القرار إلى حملات توعية جماهيرية، تستهدف الشباب على وجه التحديد، من أجل تحسين الإلمام بالإعلام ومكافحة الاستقطاب على شبكة الإنترنت. كما يؤكد على أهمية الإلزام بوضع علامات مميزة للمحتوى المولّد عبر الذكاء الاصطناعي لمكافحة المعلومات المضللة. وهناك تأكيد على التعاون الدولي كعنصر حاسم، حيث يشجع القرار الدول على تبادل الممارسات الفضلى والخبرات الفنية من خلال المنتديات المتعددة الأطراف مثل منظمة الأمن والتعاون في أوروبا. ومن خلال استغلال الذكاء الاصطناعي بشكل مسؤول وتعاوني، يقدم القرار نهجاً متوازناً لتعزيز جهود مكافحة الإرهاب العالمية مع حماية حقوق الإنسان.

قدم مركز الدراسات العالمية بالجمعية البرلمانية للبحر الأبيض المتوسط تقريره المعنون: "الاستخدام الشرير للذكاء الاصطناعي والتقنيات الجديدة من قِبل الجماعات الإرهابية والجنائية: الأثر على الأمن والتشريعات والحوكمة". يستكشف التقرير كيفية استغلال الجماعات الإرهابية، والشبكات الإجرامية العابرة للحدود الوطنية وغيرها من الجهات الفاعلة غير التابعة لدولة، للتقنيات الجديدة والناشئة. ويفحص أثر تلك التقنيات على الأمن الوطني والإقليمي، بالإضافة إلى عواقبها بالنسبة لمؤسسات الدولة وعملياتها، بما في ذلك الهجمات السيبرانية، والمعلومات المغلوطة والمضللة، والعنف السياسي والثقافات المدفوعة بالكراهية، والقدرة النظامية على الصمود. بالإضافة إلى ذلك، تُقيّم الوثيقة الوضع الحالي للأطر التنظيمية المتعلقة بالأمن على المستويات الوطنية والقارية، مع تسليط الضوء على المجالات التي تحتاج إلى تحسين. وهي تتماشى مع الاتجاهات الاستراتيجية المستمدة من القرارات والإعلانات والتقارير الصادرة عن الأمم المتحدة والمنظمات المرتبطة بها، بالإضافة إلى المبادرات والتشريعات الهادفة إلى حوكمة الذكاء الاصطناعي لدى الدول الأعضاء في شتى أنحاء العالم. يقدم التقرير مجموعة شاملة من التوصيات الاستراتيجية والفنية والمتعلقة بالسياسات، ويركز كثيرٌ منها على الدور الحاسب للاستجابات البرلمانية. وباعتباره "وثيقة قابلة للتعديل"، من المستهدف أن يخضع للرصد والتحديث باستمرار لكي يعكس التحديات والفرص الناشئة.

كجزء من مساهمتها في الممارسات البرلمانية الدولية والإقليمية الجيدة، قدمت الجمعية المشتركة بين برلمانات الدول الأعضاء في رابطة الدول المستقلة نظرة عامة على جهودها في هذا المجال. ففي عام 2023، اعتمدت الجمعية توصيات بشأن الإطار التنظيمي للذكاء الاصطناعي، تضمنت معايير أخلاقية للبحوث والتطوير، تهدف إلى إنشاء نظام موحد للمعايير القانونية والأخلاقية التي تعزز تطوير الذكاء الاصطناعي عبر مختلف القطاعات الاقتصادية لدى الدول الأعضاء في رابطة الدول المستقلة مع ضمان حماية حقوق المواطنين والحفاظ على الأمن. وتعكف الجمعية المشتركة بين برلمانات الدول الأعضاء في رابطة الدول المستقلة في الوقت الحالي على صياغة قانون نموذجي يتناول *تقنيات الذكاء الاصطناعي*، من أجل تنظيم الذكاء الاصطناعي عبر دورة حياته بالكامل، يتماشى مع جدولي الأعمال الصادرين عن الجمعية العامة للأمم المتحدة والاتحاد الدولي للاتصالات. ومن بين الخصائص الرئيسية لهذه المبادرة دمج تقييمات الأثر التكنولوجي ضمن العملية التشريعية للتقليل من المخاطر ومنع العواقب السلبية المؤثرة على الإنسانية. وبالإضافة إلى ذلك، تقوم الجمعية المشتركة بين برلمانات الدول الأعضاء في رابطة الدول المستقلة بوضع قانون نموذجي يتناول *مكافحة استخدام الأنظمة الآلية وأنظمة الروبوت لأغراض إرهابية ومتطرفة*، إقراراً بالحاجة لمجابهة التحديات الأمنية التي يفرضها التطور السريع للذكاء الاصطناعي. ومع شيوع استخدام الأنظمة المستقلة والروبوتية كأدوات تستخدم داخل المنزل، تسعى مسودة القانون هذه إلى مجابهة النوايا الإجرامية - سواء من مطوري النظم، المسؤولين عادةً عن تصميم البرامج، أو من المستخدمين الساعين إلى استغلال الأنظمة المصممة لأغراض عامة في أغراض شريرة.

ناقش الخبراء والمشاركون أيضاً قرار البرلمان الأوروبي بشأن الذكاء الاصطناعي في العصر الرقمي (الذي اعتُمد في 3 أيار/مايو 2022)، والذي يعد أحد أكثر القوانين شمولاً التي تدرس وتتناول الأثر التحويلي للذكاء الاصطناعي وتداعياته على الإرهاب والتطرف والأمن. يلقي القرار الضوء على الدور الحاسم الذي يقوم به الذكاء الاصطناعي في مساعدة وكالات إنفاذ القانون في مجابهة الجريمة المنظمة والإرهاب والجريمة الإلكترونية. جرى تحديد القطاعات العالية المخاطر كأولويات لتقييم

هذه الوثيقة هي ترجمة غير رسمية مقدَّمة للأغراض الإعلامية فقط. وفي حالة وجود أي تعارض أو غموض، فإن النسخة الأصلية باللغة الإنجليزية هي التي تسود.

المخاطر من أجل التخفيف من التهديدات المحتملة للأمن والحقوق الأساسية. وتمثل إساءة استخدام الذكاء الاصطناعي في الحروب المختلطة والتدخل الأجنبي أحد المخاوف الرئيسية، حيث يؤكد القرار على مخاطر مثل حملات المعلومات المضللة وزعزعة الاستقرار الاقتصادي والتلاعب بالانتخابات الذي يمكن أن يعطي الأفضلية للجماعات المتطرفة أو يقوض المؤسسات الديمقراطية. كما يحذر أيضاً من انتشار التزييف العميق وسرقات الهوية التي يتيحها الذكاء الاصطناعي، مما يقوض الثقة في المحتوى الرقمي ويفاقم من الاستقطاب الاجتماعي والسياسي. ويؤكد القرار مجدداً على دعوة البرلمان الأوروبي لإنفاذ حظر دولي على الأسلحة الفتاكة الذاتية التشغيل، ويؤكد على ضرورة الرقابة الإنسانية المجدية في تطبيقات الذكاء الاصطناعي العسكرية لضمان الامتثال للمبادئ القانونية والأخلاقية. ومن اجل مجابهة هذه التحديات، يؤكد القرار على الحاجة لأطر تنظيمية قوية ومرنة وتصلح للمستقبل، لحماية الحقوق الأساسية وحقوق الإنسان.

كما أشار المشاركون إلى قرار الاتحاد البرلماني الدولي بعنوان "أثر الذكاء الاصطناعي على الديمقراطية وحقوق الإنسان وسيادة القانون،" والذي اعتمد في 17 تشرين الأول/أكتوبر 2024، مع تسليط الضوء على صلتة بسياق مكافحة الإرهاب. يؤكد القرار على أهمية قيام البرلمانات بدور نشط في تشكيل حوكمة الذكاء الاصطناعي لضمان ألا تؤدي التطورات التقنية إلى تقويض القيم الديمقراطية أو حقوق الإنسان أو سيادة القانون. وعلى الرغم من أن القرار لا يتناول الإرهاب بشكل مباشر، إلا أنه يثير عدداً من المخاوف الحاسمة، مثل إمكانية استخدام الذكاء الاصطناعي لتيسير نشر المعلومات المضللة والمكذوبة والتطرف - وجميعها من العوامل التي يمكن أن تزعزع استقرار المجتمعات وتؤجج الأيدولوجيات العنيفة. كما يؤكد القرار أيضاً على خطر تضخيم الذكاء الاصطناعي للتحيز والتمييز، ويشمل ذلك العنف القائم على النوع الاجتماعي والتطرف عبر الإنترنت، كما يدعو إلى أطر قانونية قوية لضمان الشفافية والمساءلة في تطوير الذكاء الاصطناعي ونشره. بالإضافة إلى ذلك، يدعو القرار إلى نهج يركز على الإنسان إزاء حوكمة الذكاء الاصطناعي، ويحث على اتخاذ تدابير لمنع إساءة استخدام الذكاء الاصطناعي للمراقبة والتلاعب بالبيانات وإنشاء محتوى ضار، مثل التزييف العميق المولّد بالذكاء الاصطناعي. ويؤكد على الحاجة لتعاون دولي شامل من أجل ضمان استخدام تقنيات الذكاء الاصطناعي بشكل مسؤول ومنصف، بحيث تحمي حقوق الأفراد وتعزز الثقة المجتمعية. بالإضافة إلى ذلك، يدعو القرار البرلمانات إلى أن تعطي الأولوية للتثقيف وبناء القدرات في مجال الذكاء الاصطناعي، مما يضمن استعدادها لمجابهة التحديات التي تفرضها التقنيات الناشئة، بما في ذلك أثرها المحتمل على الأمن القومي وجهود مكافحة الإرهاب.

ذُكِرَت أثناء الحوار "الاتفاقية الإطارية بشأن الذكاء الاصطناعي وحقوق الإنسان، والديمقراطية وسيادة القانون" الصادرة عن مجلس أوروبا، بجانب صكوك دولية أخرى. وعلى الرغم من أنها لا تتناول القضايا المتعلقة بالإرهاب بشكل مباشر، إلا أنها أو معاهدة دولية ملزمة قانوناً على الإطلاق بشأن الذكاء الاصطناعي تحتوي على تركيز محدد حقوق الإنسان والديمقراطية وسيادة القانون. وتهدف الاتفاقية إلى ضمان اتساق الأنشطة بشكل كامل على مدار دورة حياة أنظمة الذكاء الاصطناعي مع حقوق الإنسان والديمقراطية وسيادة القانون، مع تعزيز التقدم التكنولوجي والابتكار. بالإضافة إلى ذلك، فإنها تسعى إلى سد أي فجوات قانونية قد تنشأ نتيجة التطورات التكنولوجية السريعة.

الجلسة الثالثة الإطار القانوني الدولي لمنع ومكافحة استخدام الذكاء الاصطناعي وغيره من التقنيات الناشئة لأغراض إرهابية

استناداً إلى الجلسات السابقة التي تناولت التحديات والتهديدات والممارسات القائمة، ركزت الجلسة الثالثة بصفة أساسية على عمل الجهات ذات الصلة في الأمم المتحدة، والتوصيات الصادرة عنها، والمنظمات الدولية والإقليمية كذلك، في منع ومكافحة استخدام الذكاء الاصطناعي والتقنيات الجديدة لأغراض إرهابية. استكشفت الجلسة أيضاً الدعم الذي تقدمه تلك المنظمات للدول الأعضاء، بما في ذلك ما يقدم للهيئات التشريعية، في تنفيذ قرارات وتوصيات مجلس الأمن التابع للأمم المتحدة المتعلقة بالذكاء الاصطناعي والتقنيات الجديدة.

قدمت وحدة الأمن الفضائي والتقنيات الجديدة التابعة لمكتب الأمم المتحدة لمكافحة الإرهاب / مركز الأمم المتحدة لمكافحة الإرهاب عرضاً تقديمياً لجهودها في تعزيز قدرات سلطات إنفاذ القانون والعدالة الجنائية في بلدان شريكة مختارة من أجل مكافحة استغلال التقنيات الجديدة والناشئة لأغراض إرهابية. كما ألقت الوحدة الضوء على عملها في دعم الدول الأعضاء في استغلال تلك التقنيات في الحرب على الإرهاب. وبالإضافة إلى ذلك، استعرضت الوحدة سلسلة من إصداراتها في موضوع أمن الفضاء الإلكتروني والتقنيات الجديدة، والتي تتضمن:

هذه الوثيقة هي ترجمة غير رسمية مقدَّمة للأغراض الإعلامية فقط. وفي حالة وجود أي تعارض أو غموض، فإن النسخة الأصلية باللغة الإنجليزية هي التي تسود.

- إجراء تقييم تهديدات الإرهاب: استخدام التقنيات الجديدة لأغراض إرهابية؛
- تصميم استجابات سياسات مكافحة الإرهاب الوطنية من أجل مكافحة استخدام التقنيات الجديدة لأغراض إرهابية؛
- إطار قدرات إنفاذ القانون بالنسبة للتقنيات الجديدة في مجال مكافحة الإرهاب؛
- مكافحة الإرهاب على شبكة الإنترنت بالذكاء الاصطناعي: نظرة عامة على وكالات إنفاذ القانون ومكافحة الإرهاب في جنوب وجنوب شرق آسيا؛
- الخوارزميات والإرهاب: الاستخدام الشرير للذكاء الاصطناعي لأغراض إرهابية.

شاركت وحدة إجراءات مكافحة الإرهاب التابعة لمنظمة الأمن والتعاون في أوروبا رؤيتها وخبراتها في مجال منع ومكافحة استخدام الذكاء الاصطناعي والتقنيات الجديدة لأغراض إرهابية. وقد أكدت الوحدة أن جهودها تتماشى مع القرار الذي اتخذته منظمة الأمن والتعاون في أوروبا مؤخراً بشأن الذكاء الاصطناعي والحرب على الإرهاب. وأبرزت أهمية إشراك نطاق واسع من الجهات الفاعلة غير الحكومية - ومنها المجتمع المدني والنساء والشباب والأعمال التجارية والصناعية والإعلام - في منع التطرف العنيف والتشدد المؤديين إلى الإرهاب. كما أكد العرض التقديمي على الحاجة الملحة لدعم تلك الجهات الفاعلة في استغلال الذكاء الاصطناعي لمجابهة التحديات التي تواجه منع التطرف العنيف والتشدد المؤديين إلى الإرهاب، وحماية الحقوق الأساسية في الخصوصية وحقوق الإنسان.

قدم فرع مكافحة الإرهاب التابع لمكتب الأمم المتحدة المعني بالمخدرات والجريمة عمله في مجال تعزيز الاستخدام المسؤول والأخلاقي للذكاء الاصطناعي والتقنيات المتقدمة من أجل منع ومكافحة إساءة استخدام الإرهابيين لفضاء الإنترنت. وقد أكد العرض التقديمي على أن التطرف العنيف والجماعات المتطرفة تستغل بشكل متزايد النطاق الرقمي لأنشطة مثل الدعاية الكاذبة والتحريض والتجنيد والتنسيق العملياتي. وأشار فرع مكافحة الإرهاب التابع لمكتب الأمم المتحدة المعني بالمخدرات والجريمة إلى أبحاث تشير إلى أن تلك الجماعات تقوم بتجربة أدوات الذكاء الاصطناعي التوليدي لتحسين استراتيجياتها في مجال الدعاية الكاذبة. ويشمل هذا استكشاف قدرات مثل توليد المواد الإعلامية، والترجمة الآلية إلى لغات متعددة، وإنشاء الدعاية الكاذبة التخليقية، وإعادة الاستخدام بتصرف، والرسائل المخصصة، ومن خلال تخطي أنظمة ضمان الاعتدال لتعظيم مدى وصولها. بالإضافة إلى ذلك، شدد مكتب الأمم المتحدة المعني بالمخدرات والجريمة على أهمية اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، التي اعتمد مؤخراً والتي يقوم مكتب الأمم المتحدة المعني بالمخدرات والجريمة بدور الأمانة العامة لها. توفر هذه الاتفاقية الرائدة للبلدان تدابير أساسية لمنع ومكافحة الجريمة السيبرانية مع تعزيز التعاون الدولي المحسَّن في تبادل الأدلة الإلكترونية للقضايا الإلكترونية الخطيرة.

قدمت لجنة مكافحة الإرهاب التابعة لمجلس الأمن والمديرية التنفيذية للجنة مكافحة الإرهاب عرضاً تقديمياً يبرز دعم المديرية التنفيذية للجنة مكافحة الإرهاب للدول الأعضاء في التعرف على النُهج المبتكرة والتشاركية لمجابهة إساءة استخدام الإرهابيين لتكنولوجيا المعلومات والاتصالات. وقد أكد العرض التقديمي على تطوير الحلول التقنية التي تستغل إمكانيات تكنولوجيا الاتصالات والمعلومات للأغراض الإيجابية مع احترام حقوق الإنسان والحريات الأساسية والالتزامات القانونية الدولية. كما شاركت المديرية التنفيذية للجنة مكافحة الإرهاب رؤى بشأن تعزيز وتيسير المساعدة الفنية ورعاية الشراكات بين القطاعين العام والخاص من أجل مواجهة استغلال الجماعات الإرهابية للتقنيات الرقمية. بالإضافة إلى ذلك، تساعد المديرية التنفيذية للجنة مكافحة الإرهاب الدول الأعضاء في مواجهة السرديات الإرهابية سواء على شبكة الإنترنت أو خارجها، مما يؤكد على أهمية تحقيق التوازن بين جهود مكافحة خطاب الكراهية وحماية حرية التعبير. وأكد العرض التقديمي على حاجة الدول للتعاون في تطوير حلول مستدامة لتلك التحديات، مع التأكيد على أهمية إيجاد أرضية مشتركة على الرغم من اختلاف وجهات النظر. قدمت المديرية التنفيذية للجنة مكافحة الإرهاب توصيات حاسمة بشأن تدابير منع ومكافحة استخدام الذكاء الاصطناعي والتقنيات الجديدة لأغراض إرهابية. وتضمنت هذه التوصيات بناء قدرات أنظمة العدالة الجنائية على مجابهة الجرائم المتعلقة بالذكاء الاصطناعي المستندة إلى تكنولوجيا الاتصالات والمعلومات، وتحسين المساءلة في قطاع التكنولوجيا من خلال ضمان تحمل الشركات لمسؤولية الممارسات التي تمكِّن من إساءة استخدام منصاتها - مثل الخوارزميات الضارة والمجالات غير المعتدلة وبيع الخدمات للجماعات الإرهابية - ووضع "معيار فني يمثل الحد الأدنى" على المستوى العالمي للحكومات من أجل منع ومكافحة الإرهاب القائم على تكنولوجيا الاتصالات والمعلومات بصورة فعالة.

هذه الوثيقة هي ترجمة غير رسمية مقدَّمة للأغراض الإعلامية فقط. وفي حالة وجود أي تعارض أو غموض، فإن النسخة الأصلية باللغة الإنجليزية هي التي تسود.

التوصيات

أوصى الخبراء والمشاركون بالتوصيات التالية أثناء الحوار، وقد صُنِّفَت إلى سبع مجالات مواضيعية لمجابهة التحديات والفرص التي يفرضها الذكاء الاصطناعي والتقنيات الجديدة في مكافحة الإرهاب.

1. وضع التشريعات والسياسات
• وضع تشريع وطني قوي لتنظيم استخدام الذكاء الاصطناعي والتقنيات الجديدة، بما يضمن معالجة مخاوف الاستخدام المزدوج (للتطبيقات النافعة والضارة) من أجل منع إساءة الاستخدام من قِبل الجماعات الإرهابية. • سنّ وتحديث قواني لتجريم إساءة استخدام الذكاء الاصطناعي والتقنيات الجديدة للأغراض الإجرامية، ومنها الإرهاب، بشكل صريح. • مواءمة التشريعات الخاصة بالذكاء الاصطناعي والتقنيات الجديدة عبر البلدان لضمان الاتساق. • إنشاء معايير مشتركة للأدلة الجنائية الرقمية والأدلة الإلكترونية. • ضمان موازنة التشريعات واللوائح بحرص من أجل تجنب التنظيم المفرط، مما قد يؤدي إلى إعاقة التقدم التكنولوجي والتنمية. بالنظر إلى المعدل المتسارع لتطور التقنيات، يجب أن يظل التشريع مرناً وقابلاً للتعديل، حيث تعاني الأطر القانونية التقليدية عادةً في ملاحقة الابتكار. وينبغي السعي لتحقيق هذا الاتزان من خلال التعاون العالمي والالتزام بالحقوق الأساسية.
2. حقوق الإنسان وحماية البيانات
• ضمان امتثال تدابير مكافحة الإرهاب لحقوق الإنسان، مع إعطاء الأولوية لحماية البيانات الشخصية والتمسك بالعدل والمساواة والإنصاف. • تنفيذ تدابير فعالة لحماية البيانات والمعلومات الشخصية بأسلوب يرتكز إلى حقوق الإنسان. • معالجة التداعيات الأخلاقية وتحيز الخوارزميات والمخاوف الأساسية المتعلقة بالخصوصية عند استغلال الذكاء الاصطناعي في مكافحة الإرهاب.
3. بناء القدرات لأنظمة إنفاذ القانون والعدالة
• تزويد وكالات إنفاذ القانون وتدريبها على مكافحة الإرهاب والأنشطة المتطرفة المدفوعة بالذكاء الاصطناعي، مع ضمان الاتساق مع المعايير الدولية لحقوق الإنسان. • بناء قدرات أنظمة العدالة الجنائية على مجابهة الجرائم القائمة على تكنولوجيا الاتصالات والمعلومات والمتعلقة بالذكاء الاصطناعي. • توفير التدريب الشامل والموارد من أجل تجهيز وكالات إنفاذ القانون للتحديات التي تفرضها التقنيات الناشئة.
4. التثقيف وتوعية الجمهور
• إعطاء الأولوية للاستثمارات في مجال التعليم والمعرفة الرقمية لتمكين المواطنين، وبخاصة الشباب، من التحليل النقدي للمعلومات، والتعرف على المعلومات المضللة ومجابهة الدعاية المتطرف الكاذبة. • دمج الذكاء الاصطناعي والتقنيات الجديدة ضمن المناهج التعليمية لمساعدة الأفراد في التعرف على المحتوى المتطرف وفهم أخطاره. • دعم مبادرات التعليم العام لبناء القدرة على الصمود في مواجهة المعلومات المضللة وحملات الدعاية الكاذبة القائمة على تقنيات الذكاء الاصطناعي.

هذه الوثيقة هي ترجمة غير رسمية مقدَّمة للأغراض الإعلامية فقط. وفي حالة وجود أي تعارض أو غموض، فإن النسخة الأصلية باللغة الإنجليزية هي التي تسود.

- تعزيز مبادرات توعية الجمهور، والتي تشمل المعرفة الإعلامية وتمييز المحتوى المولّد عبر الإنترنت، لمكافحة المعلومات المضللة.

5. التعاون الدولي والشراكات الدولية

- تحسين التعاون الدولي من أجل مواجهة استخدام للذكاء الاصطناعي والتقنيات الجديدة عبر الحدود الوطنية لأغراض شريرة.
- دعم إنشاء وكالة أمنية دولية، مثل "السيبر-بول"، قياساً على الإنتربول، لمكافحة الجرائم السيبرانية والإرهاب على المستوى العالمي.
- تيسير التعاون بين السلطات الوطنية والجهات الإقليمية والمنظمات الدولية، من أجل مشاركة المعلومات الاستخباراتية والممارسات الفُضلى والخبرات التقنية.
- تشجيع التعاون المتعدد الأطراف وزيادة الشراكات بين القطاعين العام والخاص من أجل تعزيز الشفافية والمساءلة في جهود مكافحة الإرهاب.
- تعزيز التعاون عبر الحدود لضمان فعالية الجهود واتساقها في مكافحة الإرهاب والتطرف العنيف.

6. التعاون مع القطاع التقني

- تعزيز التعاون الوثيق بين الحكومات وقطاع تكنولوجيا الاتصالات والمعلومات وصناعة التكنولوجيا من أجل إنشاء ضمانات تحول دون إساءة استخدام الذكاء الاصطناعي من قبل المنظمات الإرهابية.
- تحسين المساءلة في قطاع التقنية، مما يضمن تحمُّل الشركات لمسؤولية الممارسات التي تُمكِّن إساءة الاستخدام، مثل الخوارزميات الضارة والمجالات غير المعتدلة، ومبيعات الخدمات للجماعات الإرهابية.
- وضع "معيار فني يمثل الحد الأدنى" على المستوى العالمي للحكومات من أجل منع ومكافحة الإرهاب القائم على تكنولوجيا الاتصالات والمعلومات بصورة فعالة.
- تشجيع التعاون مع شركات التكنولوجيا من أجل تحسين الكشف عن التهديدات وتجنب المخاطر المرتبطة بأدوات الذكاء الاصطناعي ومنصاته.

7. دور الجمعيات البرلمانية

- الاستفادة من الجمعيات البرلمانية في زيادة الوعي، وتعزيز المعايير الدولية، ومناصرة المساعدات الفنية في تدابير مكافحة الإرهاب.
- ينبغي أن يتولى البرلمانيون قيادة جهود تيسير وتعزيز التعاون الدولي في مكافحة الإرهاب على جميع المستويات، مع ضمان اتساق الجهود الوطنية مع المعايير الدولية.

الخلاصة وإجراءات المتابعة

أبرزت مناقشات الخبراء ومساهمات المشاركين أثناء الحوار التحديات الناشئة التي يفرضها الذكاء الاصطناعي والتقنيات الناشئة في مكافحة الإرهاب. ظهرت التوصيات الرئيسية عبر العديد من المجالات الحاسمة، ومنها التطوير التشريعي وضمانات حقوق الإنسان، وبناء القدرات في مجال إنفاذ القانون، وتثقيف الجمهور والتعاون الدولي ودور الجمعيات البرلمانية. وتهدف هذه التوصيات إلى ضمان استجابة متوازنة ومنسّقة ومتماشية مع حقوق الإنسان للفرص والمخاطر التي تمثلها تلك التقنيات في منع ومكافحة الإرهاب والتطرف العنيف.

هذه الوثيقة هي ترجمة غير رسمية مقدَّمة للأغراض الإعلامية فقط. وفي حالة وجود أي تعارض أو غموض، فإن النسخة الأصلية باللغة الإنجليزية هي التي تسود.

من أجل النهوض بتنفيذ هذه التوصيات، سوف يستمر مكتب برامج إشراك البرلمانيين في منع الإرهاب ومكافحته التابع لمكتب الأمم المتحدة لمكافحة الإرهاب في تيسير التعاون بين الهيئات البرلمانية والحكومات الوطنية ووكالات الأمم المتحدة وغيرهم من أصحاب المصلحة. سوف يدعم هذا التنسيق المستمر تطوير استراتيجيات وسياسات تدمج الذكاء الاصطناعي والتقنيات الناشئة ضمن جهود مكافحة الإرهاب ومنع التطرف العنيف، مع التركيز على بناء القدرات والمساعدات الفنية.

تطلعاً نحو المستقبل إلى عامي 2025 و2026، سوف يهدف مكتب برامج إشراك البرلمانيين في منع الإرهاب ومكافحته التابع لمكتب الأمم المتحدة لمكافحة الإرهاب، بالمشاركة مع وحدة أمن الفضاء الإلكتروني والتقنيات الجديدة التابعة لمكتب الأمم المتحدة لمكافحة الإرهاب/مركز الأمم المتحدة لمكافحة الإرهاب، إلى تنظيم مؤتمر برلماني عالمي بشأن الذكاء الاصطناعي والتقنيات الناشئة. وسوف يسعى المؤتمر إلى أن يكون بمثابة منصة للحوار البرلماني، وأن يركز على الاستجابات الفعالة للتقاطع بين الذكاء الاصطناعي والتقنيات الجديدة ومكافحة الإرهاب.

بالإضافة إلى ذلك، سوف يهدف مكتب الأمم المتحدة لمكافحة الإرهاب إلى تنظيم سلسلة من أنشطة التوعية وبناء القدرات للبرلمانيين والموظفين ذوي الصلة من البرلمانات الوطنية والجمعيات البرلمانية المشاركة. وسوف تسعى هذه الأنشطة إلى تحسين فهمهم للذكاء الاصطناعي والتقنيات الجديدة في سياق مكافحة الإرهاب/منع التطرف العنيف، مما يمكنهم من اتخاذ قرارات مستنيرة، وموافقة لحقوق الإنسان، في عملهم التشريعي والسياسي.

سيكون الدخول في شراكة مع الجمعيات البرلمانية، وبخاصة المشاركين في آلية التنسيق للجمعيات البرلمانية المعنية بمكافحة الإرهاب، من الأمور الأساسية في تنفيذ تلك المبادرات. وسوف يعمل مكتب الأمم المتحدة لمكافحة الإرهاب عن كثب مع تلك الجمعيات لتوفير الدعم المخصص والخبرات والإرشاد للبرلمانات الوطنية، لمضان مشاركتها النشطة في النهوض بجهود مكافحة الإرهاب.

أخيراً، سوف تُعطَى الأولوية لنشر توصيات الخبراء من أجل ضمان اتساق جهود جميع الشركاء وأصحاب المصلحة والجمعيات البرلمانية ذات الصلة، لتعزيز استجابة عالمية منسقة للتحديات التي تفرضها التقنيات الناشئة في مجال مكافحة الإرهاب.

من المخطط انعقاد الحوار البرلماني (الخامس) بشأن السياسات خلال الربع الثاني من عام 2025، وسيتم تأكيد التوقيت ومكان الانعقاد والموضوع الرئيسي.

الاتصالات

البيانات الصحفية

https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20241205_press_release_4th_policy_dialogue_rome.pdf

https://www.oscepa.org/en/news-a-media/press-releases/press-2024/under-osce-pa-leadership-legislators-from-across-the-globe-discuss-preventing-and-countering-the-use-of-ai-by-terrorists-at-policy-dialogue-in-rome

https://www.shura.qa/ar-qa/Pages/MediaCenter/News/07122024

https://pam.int/the-fourth-parliamentary-policy-dialogue /

https://turkpa.org/news/1766-turkpa-attended-6th-meeting-of-coordination-mechanism-for-parliamentary-assemblies-on-counter-terrorism-and-4th-parliamentary-policy-dialogue-organized-by-unoct

https://italyun.esteri.it/en/news/dalla_rappresentanza/2024/12/closing-remarks-delivered-by-permanent-representative-amb-maurizio-massari-at-fourth-parliamentary-policy-dialogue-on-countering-the-use-of-artificial-intelligence-and-new-technologies-for-terrorist /

هذه الوثيقة هي ترجمة غير رسمية مقدَّمة للأغراض الإعلامية فقط. وفي حالة وجود أي تعارض أو غموض، فإن النسخة الأصلية باللغة الإنجليزية هي التي تسود.

التغريدات

https://x.com/UN_OCT/status/1865127801377927552

https://x.com/oscepa/status/1864327102989734107

هذه الوثيقة هي ترجمة غير رسمية مقدَّمة للأغراض الإعلامية فقط. وفي حالة وجود أي تعارض أو غموض، فإن النسخة الأصلية باللغة الإنجليزية هي التي تسود.