مكتب الأمم المتحدة
لمكافحة الإرهاب
مركز الأمم المتحدة لمكافحة الإرهاب

الإنتربول

بتمويل من
الاتحاد الأوروبي

أمن الفضاء الإلكتروني والتكنولوجيات الجديدة

تصميم استجابات السياسات الوطنية لمكافحة الإرهاب للحد من استخدام التكنولوجيات الجديدة لأغراض إرهابية

إخلاء مسؤولية

لا تعكس الآراء والاستنتاجات والنتائج والتوصيات المُعبَّر عنها في هذه الوثيقة بالضرورة آراء منظمة الأمم المتحدة أو المنظمة الدولية للشرطة الجنائية (الإنتربول) أو حكومات الاتحاد الأوروبي أو أياً من الكيانات الوطنية أو الإقليمية أو الدولية المشاركة فيها.

لا تنطوي التسميات المستخدمة في هذا المنشور ولا المواد المعروضة فيه على الإعراب عن أي رأي كان من جانب الأمانة العامة للأمم المتحدة إزاء الوضع القانوني لأي بلد أو إقليم أو مدينة أو منطقة أو للسلطات القائمة فيها أو إزاء تعيين حدودها أو تخومها.

يسمح باقتباس محتويات هذا المنشور أو إعادة إنتاجها شريطة الاعتراف بمصدر المعلومات. كما يود المؤلفون الحصول على نسخة من الوثيقة التي استخدمت هذا المنشور أو اقتبست عنه.

شكر وتقدير

هذا التقرير نتاج مبادرة مشتركة بين مركز الأمم المتحدة لمكافحة الإرهاب التابع لمكتب الأمم المتحدة لمكافحة الإرهاب والإنتربول من أجل تعزيز قدرات سلطات إنفاذ القانون وسلطات العدالة الجنائية على مكافحة استخدام التكنولوجيات الجديدة لأغراض الإرهاب. وقد مُوّلت هذه المبادرة المشتركة بمساهمات سخية من الاتحاد الأوروبي.

المحتويات

توطئة مشتركة

جذب التقدم المحرز في مجال تكنولوجيا المعلومات والاتصالات كلّاً من الجماعات الإرهابية والجماعات المتطرفة العنيفة لاستغلال هذا التقدم في تسهيل قيامهم بمجموعة واسعة من الأنشطة التي تشمل التحريض ونشر التشدد والتجنيد والتدريب والتخطيط وجمع المعلومات والتواصل والتحضير والدعاية والتمويل. ويستمر الإرهابيون في استكشاف آفاق تكنولوجيّة جديدة، في حين أن الدول الأعضاء ما زالت تعرب عن قلقها المتزايد حيال استخدام التكنولوجيات الجديدة لأغراض إرهابية.

طالبت الدول الأعضاء خلال الاستعراض السابع لاستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب مكتبَ الأمم المتحدة لمكافحة الإرهاب والكيانات الأخرى المنضوية في ميثاق الأمم المتحدة العالمي لتنسيق مكافحة الإرهاب "بتقديم دعمٍ مشتركٍ للإجراءات والنهج المبتكرة لبناء قدرات الدول الأعضاء، متى طلبت، على التعامل مع التحديات التي تنجم عن التكنولوجيات الجديدة واستغلال الفرص التي تقدمها في الوقاية والحد من الإرهاب ومكافحته، بما في ذلك الجوانب المرتبطة بحقوق الإنسان."

وفي تقريره المقدم للأمانة العامة عن أنشطة منظومة الأمم المتحدة في تطبيق استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب (A/77/718)، يشدد الأمين العام على أن "[...] التكنولوجيات الجديدة والناشئة توفر فرصاً غير مسبوقة لتحسين رفاه البشرية بالإضافة إلى أدوات جديدة لمكافحة الإرهاب. [...] وعلى الرغم من تعزيز الجهود وتضافرها، إلا أن استجابة المجتمع الدولي غالباً ما تكون متأخرة. وبعض هذه الاستجابات تحُدّ من حقوق الإنسان على نحو غير مبرر، ويشمل ذلك على وجه التحديد كلّاً من الحق في الخصوصية وحق حرية التعبير، بما في ذلك الحق في التماس المعلومات وتلقيها."

ونسعى من خلال التقارير السبعة المشمولة في هذه الخلاصة – وهي نتاج الشراكة بين مركز الأمم المتحدة لمكافحة الإرهاب والمنظمة الدولية للشرطة الجنائية المندرجة تحت مبادرة التكنولوجيا لمكافحة الإرهاب (CT TECH) المشتركة والممولة من الاتحاد الأوروبي إلى دعم سلطات إنفاذ القانون والعدالة الجنائية التابعة للدول الأعضاء في مكافحة استغلال التكنولوجيات الجديدة والناشئة لأغراض الإرهاب وفي الاستفادة من التكنولوجيات الجديدة والناشئة لمحاربة الإرهاب كجزء من هذه الجهود، مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.

إن مكتبينا على استعداد لمواصلة دعم الدول الأعضاء وغيرها من الشركاء في الوقاية والحد من الإرهاب ومكافحته بكافة أشكاله ومظاهره، والاستفادة من الآثار الإيجابية للتكنولوجيا في مكافحة الإرهاب.

فلاديمير فورونكوف
وكيل الأمين العام، مدير مكتب الأمم المتحدة
لمكافحة الإرهاب
المدير التنفيذي لمركز الأمم المتحدة لمكافحة الإرهاب

ستيفن كافانا
المدير التنفيذي
للخدمات الشرطية في الإنتربول

شكر وتقدير

تم تطوير هذه الوثيقة بمساهمة مجموعة واسعة من أصحاب المصلحة كما تمت مراجعتها من قبلهم. يود مكتب الأمم المتحدة لمكافحة الإرهاب أن يعرب عن امتنانه على وجه الخصوص للمساهمة التي قدمها كل من:

- **السيدة ماريانا غونزاليس كامبل** – استشارية في منع التطرف العنيف، منظمة البلدان الأمريكية
- **السيد مايكل أوكيف** – متخصص في مكافحة الإرهاب، فرع منع الإرهاب التابع لمكتب الأمم المتحدة المعني بالمخدرات والجريمة
- **السيد فيكتور كيبكويتش** – معاون لشؤون البرامج، المركز العالمي للأمن التعاوني
- **السيد وينثروب ويلز** – مدير البرنامج المعهد الدولي للعدالة وسيادة القانون

مصطلحات وتعاريف

اكتشاف الشذوذ	عملية التنقيب عن البيانات لتحديد نقاط البيانات التي تقع خارج القاعدة أو التي تنحرف عنها.
منطقة المسؤولية	المجال أو الإقليم الذي تقع تحت مسؤولية أو ضمن اختصاص مزاول المهنة.
الذكاء الاصطناعي	المفهوم العام لوصف منهج متخصص يعنى بتطوير الأدوات التكنولوجية التي تستطيع ممارسة أعمال بشرية مثل التخطيط والتعلم والاستدلال والتحليل.
إجراءات العدالة الجنائية	العملية القانونية التي تُوجّه من خلالها التهم الجنائية ضد شخص أو كيان ما والإجراءات التي تتخذها المحكمة، إضافة إلى إصدار الأحكام، والتصويبات وإعادة التأهيل.
شبكة الإنترنت الخفية	الجزء المشفر من الإنترنت الذي يتم الوصول إليه باستخدام برمجيات هي بحد ذاتها غير جنائية، كمتصفح "تور" مثلاً. ولكن مما لا شك فيه أن شبكة الإنترنت الخفية تحتوي على العديد من المواقع والخدمات الجنائية التي تستضيفها هذه الشبكات[1].
نزع التطرف	العملية التي تهدف إلى حمل شخص ما، أظهر علامات تدل على تجنيده لصالح التطرف، على التخلي عن المفاهيم المتطرفة[2].

1 المركز الأوروبي للجرائم الإلكترونية، "تقييم تهديدات الجريمة المنظمة عبر الإنترنت لعام 2019" (يوروبول، 2019)، 4، https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf.

2 لورينزو فيدينو وكليفورد بينيت، "مراجعة لأفضل الممارسات عبر الأطلسي لمكافحة التطرف في السجون وعودة الإرهابيين" (المؤتمر الثالث للشبكة الاستشارية للمركز الأوروبي لمكافحة الإرهاب حول الإرهاب والدعاية، لاهاي، هولندا: يوروبول، 2019)، 8، https://www.europol.europa.eu/cms/sites/default/files/documents/a_review_of_transatlantic_best_practices_for_countering_radicalisation_in_prisons_and_terrorist_recidivism.pdf.

فك الارتباط	العملية التي يجري من خلالها تدريب شخص ما، أظهر علامات تجنيده لصالح التطرف، إما على ترك مجموعته أو رفض العنف، ولا تهدف بالضرورة إلى تغيير وجهات نظرهم أو الفكر المتطرف[3].
الأدلة	هي مصطلح رسمي للمعلومات التي تشكل جزءاً من المحاكمة، أي أنها تُستخدم لإثبات أو دحض الجريمة المزعومة. كل الأدلة هي عبارة عن معلومات، لكن ليست كل المعلومات أدلة؛ وهكذا فإن المعلومات هي الشكل الخام الأصلي للأدلة[4].
الممارسة القائمة على الأدلة	استخدام البيانات الفعلية والنوعية كوسيلة لوضع السياسات وتنفيذها[5].
الاستخبارات	الحصيلة الناتجة عن تجميع وتحديث ونشر وتحليل وتفسير المعلومات التي جُمعت من مجموعة كبيرة من المصادر بهدف إعلام صناع القرار بالتخطيط للأهداف التي تساعد في اتخاذ القرارات والاجراءات على المستوى الاستراتيجي والعملياتي والتكتيكي. كما يجب جمع وحفظ واستخدام ومشاركة المعلومات الاستخباراتية بما يتوافق مع التزامات الدول الأعضاء ذات الصلة بموجب القانون الدولي لحقوق الإنسان.
التحقيقات الجنائية	عملية جمع المعلومات (أو الأدلة) لتحديد ارتكاب جريمة ما، وتحديد الجاني بالإضافة لتقديم الأدلة التي من شأنها دعم جهة الادعاء في الاجراءات القانونية.
إجراءات إنفاذ القانون	يصف عادة إجراءات إنفاذ القانون المتخذة ضد تهديد ما، التي يمكن أن تتضمن احتجاز فرد (أو عدة أفراد)، وتعطيل أنشطة الجهات الفاعلة المهددة؛ (أي إزالة المحتوى ومصادرة الموجودات)، وما إلى ذلك.
معالجة اللغات الطبيعية	مجموعة فرعية من أنظمة الذكاء الاصطناعي تبحث في مقدرة الآلة على التحليل والتعامل مع اللغات البشرية كمصدر للمدخلات ومصدر للمخرجات معاً (بدلاً من البيانات أو الرموز على سبيل المثال)[6].
التكنولوجيات الجديدة	بينما تشمل المصطلحات التكنولوجية الجديدة مجموعات واسعة من التكنولوجيات المختلفة[7]، بما يخدم هذه الوثيقة، تشير تلك التكنولوجيات إلى حسن وإساءة استخدامها، مثل الإنترنت ووسائل التواصل الاجتماعي والعملات المشفرة وتقنية التعرف على الوجه وشبكات الإنترنت الخفية[8].

3 فيدينو وبينيت، Vidino and Bennett 8.

4 المبادئ التوجيهية للمديرية التنفيذية للجنة مكافحة الإرهاب لتسهيل الاستخدام والمقبولية كدليل في المحاكم الجنائية الوطنية للمعلومات التي يجري جمعها ومعالجتها وحفظها ومشاركتها من قبل الجيش لمحاكمة الجرائم الإرهابية (2021).

5 ريبيكا فريز Freese، "مكافحة الإرهاب القائمة على الأدلة أم التحليق بلا هدف؟ كيف نفهم ونحقق ما ينجح، وجهات نظر حول الإرهاب 8، رقم. 1 (2014): 37.

6 روس جروتزماخر، "قوة معالجة اللغات الطبيعية"، مراجعة الأعمال بجامعة هارفارد، 19 نيسان/أبريل 2022، https://hbr.org/2022/04/the power-of-natural-language-processing؛ بن لوتكيفيتش وإد بيرنز، "ما هي معالجة اللغة الطبيعية؟ مقدمة في البرمجة اللغوية العصبية"، ذكاء المؤسسات الاصطناعي، الذي أتيح في 30 نيسان/أبريل 2023، https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP.

7 الذكاء الاصطناعي، وإنترنت الأشياء، وتقنيات سلسلة الكتل، والأصول المشفرة، والطائرات بدون طيار والأنظمة الجوية بدون طيار، والحمض النووي، وبصمات الأصابع، وتكنولوجيا الفضاء الإلكتروني، وميزة التعرف على الوجه، والطباعة الثلاثية الأبعاد.

8 وثيقة برنامج التكنولوجيا لمكافحة الإرهاب – الملحق الأول توصيف الإجراءات.

استخبارات المصادر المفتوحة	المعلومات الاستخباراتية التي جُمعت من مصادر عامة متاحة[9].
إعادة التأهيل	عملية شاملة تفضي بصورة مثالية إلى إعادة تأهيل الشخص الذي يعيش حياة يسودها الاكتفاء الذاتي وحرية الاختيار، دون الامتثال للأفكار المتطرفة أو المشاركة في الأنشطة المستوحاة من التطرف (بما في ذلك العنف).
إعادة الإدماج	عملية شاملة تعمل على إعادة دمج الشخص في الحياة الاجتماعية و/أو العملية.
الأمن بالتصميم	تنصيب الإجراءات الأمنية على أنها شيء يجري بناؤه/تصميمه بحيث يكون مجهزاً للدفاع ضد أي تهديد ضمن هيكله/بنائه/إطاره الحالي[10].
الأمن الافتراضي	برنامج/سياسة تصل إلى العميل الذي حصل بالفعل على التدابير الأساسية لضمان أمانه (عوضاً عن العميل الذي يحتاج لتنفيذ التدابير الأمنية كل على حدة)[11].
استخبارات وسائل التواصل الاجتماعي	المعلومات الاستخباراتية التي يجري تجميعها من خلال وسائل التواصل الاجتماعي.
إجراءات التشغيل الموحدة	سلسلة من الخطوات المحددة مسبقاً التي توجه تنفيذ السياسات.
الإرهاب	الأعمال الإجرامية، بما فيها الأعمال المرتكبة ضد المدنيين بنية التسبب بالموت أو أذية جسدية أو احتجاز الرهائن، وتهدف إلى إثارة حالة من الرعب بين العامة أو بين مجموعة محددة من الناس وترويع السكان أو إجبار حكومة أو منظمة دولية على القيام بعمل ما أو الامتناع عنه، وهو ما يشكل جرائم تقع ضمن نطاق المعاهدات والبروتوكولات الدولية المتعلقة بالإرهاب وتأتي وفقاً لتعريفها[12].
الأصول الافتراضية	الأصول الافتراضية/المشفرة التي تشير إلى أشكال العملات الرقمية وأصول أخرى غيرها[13].
زيتابايت	زيتابايت واحد يساوي مليار تيرابايت.

9 روب فلاندرز وآخرون، استخبارات تهديدات الفضاء الإلكتروني في الحكومة: دليل لصناع القرار والمحللين، الطبعة الثانية. (المملكة المتحدة، 2019)، 22-24، https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf.

10 المفوضية الأوروبية، الأمن بالتصميم: حماية الأماكن العامة من الهجمات الإرهابية (لكسمبرغ: الاتحاد الأوروبي، 2022)، 23، https://publications.jrc.ec.europa.eu/repository/bitstream/JRC131172/JRC131172_01.pdf.

11 وكالة أمن الفضاء الإلكتروني وأمن البنية التحتية وآخرون، "تحويل توازن مخاطر أمن الفضاء الإلكتروني: مبادئ وأساليب الأمن بالتصميم والأمن الافتراضي"، 13 نيسان/أبريل 2023، 5-6، https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_Security-by-design-default_508_0.pdf.

12 انظر قرار مجلس الأمن 1566 (2004)، الفقرة 3.

13 فرقة العمل المعنية بالإجراءات المالية، "الأصول الافتراضية"، فرقة العمل المعنية بالإجراءات المالية، أتيحت في 7 أيار/مايو 2023، https://www.fatf-gafi.org/en/topics/virtual-assets.html.

ملخص تنفيذي

تُعد هذه الوثيقة الواردة تحت عنوان "تصميم استجابات السياسات الوطنية لمكافحة الإرهاب للحد من استخدام التكنولوجيات الجديدة لأغراض إرهابية" إطاراً شاملاً صمم بهدف مساعدة صنّاع السياسات وأصحاب المصلحة في مجال مكافحة الإرهاب على فهم أثر التكنولوجيات الجديدة على الإرهاب وصياغة استجابات فعالة لسياسات مكافحة الإرهاب. وتشمل طيفاً واسعاً من الاعتبارات الأساسية التي تساهم في وضع استجابات السياسات الوطنية لمكافحة الإرهاب للحد من استخدام التكنولوجيات الجديدة لأغراض إرهابية. وتقدم ممارسات مفيدة ورؤى عملية لمساندة صنّاع السياسات والعاملين في تطوير السياسات والاستراتيجيات الفعالة لمكافحة الإرهاب. يبحث هذا الدليل في الاستراتيجيات والسياسات القائمة لمكافحة الإرهاب ويحدد الثغرات في الطريقة التي تعالج من خلالها استخدام الإرهابيين للتكنولوجيات الجديدة.

تشتمل المنهجية المتبعة في تطوير هذا الدليل على البحث والتحليل واستشارة أصحاب المصلحة ذوي الصلة والخبراء، وركز البحث على تحديد التحديات الرئيسة والفرص التي تطرحها التكنولوجيات الجديدة في سياق الإرهاب والاستجابات الحالية لسياسات واستراتيجيات مكافحته. ويتضمن ذلك مراجعة المطبوعات الحالية ودراسة الحالات وأفضل الممارسات، ومن خلال هذه المصادر يجري تحديد العناصر الرئيسية والاستراتيجيات الفعالة لتطوير الاستجابات لسياسات مكافحة الإرهاب. يقدم الدليل تحليلاً تفصيلياً للتحديات المفروضة نتيجة استغلال الإرهابيين للتكنولوجيات الجديدة، ويقدم توصيات عملية لكيفية الرد عليها. كما يتضمن ممارسات وأمثلة لاستجابات السياسات الناجحة في عدة دول أعضاء. وفي حين أن المصطلحات المتعلقة بالتكنولوجيات الجديدة تغطي طيفاً واسعاً من التكنولوجيات المختلفة، يركز هذا الدليل بصورة أساسية على استخدام وسوء استخدام التكنولوجيات الجديدة مثل الإنترنت ووسائل التواصل الاجتماعي والعملات المشفرة وميزة التعرف على الوجه وشبكة الإنترنت الخفية.

يشير التقرير إلى أن التكنولوجيا تتطور بخطىً أسرع مما يمكن للسياسات الوطنية أن تواكبها، ويقدّم، بناءً على ذلك، إطاراً لتقييم فعالية تلك السياسات وتطوير التعديلات للحفاظ على أهميتها. كما يشدد على أن العديد من سياسات مكافحة الإرهاب القائمة لا تأخذ في الحسبان عوامل التمكين التكنولوجية مثل الذكاء الاصطناعي وشبكة الإنترنت الخفية والتطبيقات المشفرة الآمنة والأصول الرقمية. ويركز أيضاً بشكل خاص على استخدام التكنولوجيات الحديثة لأغراض إرهابية ويسلط الضوء على الاستخدامات المحتملة للتكنولوجيا الجديدة بهدف مكافحة الإرهاب. يتمحور هذا الدليل حول أربعة اعتبارات جوهرية وهي: الوعي والتدخلات لمواجهة التهديد والقدرات الوطنية والتعاون، وكل منها يرفدنا بالمكونات المشتركة التي تساهم في عملية رسم سياسات تمكّن الاستجابات الفاعلة لاستخدام التكنولوجيات الجديدة لأغراض إرهابية.

يشدد الدليل على أهمية السياسات الشاملة التي تحدد الولايات المؤسسية، والمسؤوليات التنظيمية، وآليات التعاون والتنسيق بين المنظمات، إضافة إلى تخصيص الموارد لتعزيز إطار القدرات الوطنية. ويذكر أيضاً أن أهمية صياغة ممارسات وأدوات وأساليب جديدة هي من أهم التحديات التي تواجه أوساط إنفاذ القانون. وبناءً عليه، لا بد من تنسيق الجهود بين مختلف الهيئات الحكومية، ووكالات إنفاذ القانون، والجيش، وأصحاب المصلحة الآخرين لضمان الأمن القومي مع حماية الحقوق والحريات الفردية.

تتمثل إحدى الافتراضات الرئيسية الخاصة بالمنهج والمطبقة هنا في المشهد الديناميكي للتكنولوجيات الجديدة الذي يتطلب أن يكون تصميم استجابات سياسات مكافحة الإرهاب بحاجة أيضاً إلى مراعاة تقييم فعالية استراتيجية مكافحة الإرهاب. وهذا التقييم ضروري لإجراء تعديلات تستند إلى آلية للتعليقات المستمرة والتعاون بين الهيئات الحكومية والقطاع الخاص والمجتمع المدني. ويشير الدليل إلى ضرورة معالجة المسائل الرئيسية في إطار سياسة مكافحة الإرهاب من أجل تقييم التهديدات التكنولوجية والتصدي لها، بما في ذلك فهم القدرات التكنولوجية والدوافع الإرهابية، والتركيز على جمع المعلومات الاستخباراتية عن التهديدات.

تشكل عملية صياغة استجابات السياسات الوطنية لمكافحة الإرهاب للحد من استخدام التكنولوجيات الجديدة لأغراض إرهابية مورداً أساسياً للحكومات وصنّاع السياسات والعاملين في وضع استراتيجيات وسياسات فعالة وشاملة لمكافحة الإرهاب. ويوفر الدليل إطاراً شاملاً يتصدى للتحديات التي يطرحها استغلال الإرهابيين للتكنولوجيات الجديدة ويقدم توصيات عملية بشأن كيفية الاستجابة. فبتركيزه على استخدام التكنولوجيات الجديدة لأغراض إرهابية يساعد البلدان على الحفاظ على الحس السلطوي والتصدي الفاعل للتهديدات الجديدة.

[أولا]
خلفية

1 - 1 لمحة عامة

تولي الدول الأعضاء في الأمم المتحدة أهمية كبيرة لمعالجة تأثير التكنولوجيات الجديدة على مكافحة الإرهاب. خلال الاستعراض السابع لاستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب (A/RES/75/291)[14] في تموز/يوليه 2021، عبرت الدول الأعضاء عن قلقها العميق بشأن "استخدام الإنترنت وغيرها من تكنولوجيات المعلومات والاتصالات، بما في ذلك منصات التواصل الاجتماعي، لأغراض إرهابية، بما في ذلك الانتشار المستمر للمحتوى الإرهابي"، وطالبت مكتب الأمم المتحدة لمكافحة الإرهاب وغيره من الكيانات المنضوية تحت الميثاق العالمي لمكافحة الإرهاب "بالدعم المشترك للإجراءات والنهج المبتكرة بهدف بناء قدرة الدول الأعضاء، بناءً على طلبها، على التعامل مع التحديات والفرص التي توفرها التكنولوجيا الجديدة، بما في ذلك الجوانب المتعلقة بحقوق الإنسان، في منع الإرهاب ومكافحته". وتطالب قرارات مجلس الأمن رقم 2178 (2014)[15] ورقم 2396 (2017)[16] الدول الأعضاء بالتعاون عند اتخاذ إجراءات وطنية لمنع الإرهابيين من استغلال التكنولوجيا ووسائل الاتصال لأغراض إرهابية. كما يشجع قرار مجلس الأمن رقم 2396 (2017) الدول الأعضاء على **تعزيز التعاون مع القطاع الخاص، خاصة مع شركات تكنولوجيا المعلومات والاتصالات**، في جمع البيانات والأدلة الرقمية في قضايا تتعلق بالإرهاب.

أشار فريق الدعم التحليلي ورصد الجزاءات، في تقريره الثلاثين إلى مجلس الأمن التابع للأمم المتحدة[17]، إلى أن "كثيرا من الدول الأعضاء أبرزت الدور المتنامي لوسائل التواصل الاجتماعي وغيرها من التكنولوجيات عبر الإنترنت في تمويل الإرهاب ونشر الدعاية"، حيث ذكرت تلك الدول منصات مثل تيليجرام، روكيت، تشات، هوب، وتامتام، من ضمن منصات أخرى. كما تمت الإشارة في التقرير إلى أن **مؤيدي تنظيم الدولة الإسلامية (داعش) يستخدمون منصات على شبكة الويب المظلم** لتخزين المواد التدريبية والوصول إليها والتي ترفض مواقع أخرى استضافتها، بالإضافة إلى استخدامها **للحصول على تكنولوجيات جديدة**.

وتمت مناقشة مكافحة استخدام التكنولوجيات الجديدة والناشئة لأغراض إرهابية في الاجتماع الخاص المكرس للجنة مكافحة الإرهاب التابعة لمجلس الأمن في الأمم المتحدة، والمنعقد في 28-29 تشرين الأول/أكتوبر 2022 في نيودلهي، وأسفر عن اعتماد وثيقة غير ملزمة، تُعرف باسم إعلان نيودلهي[18].

14 استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: الاستعراض السابع (A/RES/75/291)، N2117570.pdf (un.org).

15 قرار مجلس الأمن رقم 2178 (2014)، undocs.org (2014)20%S/RES/2178.

16 قرار مجلس الأمن رقم 2396 (2017)، http://undocs.org/S/RES/2396(2017).

17 التقرير الثلاثون لفريق الدعم التحليلي ورصد الجزاءات المقدم عملا بالقرار 2610 (2021) بشأن تنظيم الدولة الإسلامية: (داعش) وتنظيم القاعدة وما يرتبط بهما من أفراد وجماعات ومؤسسات وكيانات (undocs.org) S/2022/547.

18 إعلان دلهي، https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_special_meeting_outcome_document.pdf.

أشارت اللجنة إلى "**قلقها حيال الاستخدام المتزايد، من قبل الإرهابيين وأنصارهم، في مجتمع عالمي، لشبكة الإنترنت وتقنيات المعلومات والاتصالات الأخرى**، بما في ذلك منصات وسائل التواصل الاجتماعي، لأغراض إرهابية"، وأقرت "**بضرورة تحقيق توازن بين تعزيز الابتكار ومنع ومكافحة استخدام التكنولوجيات الجديدة والناشئة، مع اتساع تطبيقها، لأغراض إرهابية**"، مؤكدة "**ضرورة الحفاظ على الاتصال العالمي والحركة الحرة والآمنة للمعلومات بما ييسر التنمية الاقتصادية، والتواصل، والمشاركة والوصول إلى المعلومات**".

1 – 2 مبادرة التكنولوجيا لمكافحة الإرهاب

مبادرة التكنولوجيا لمكافحة الإرهاب هي مبادرة مشتركة بين منظمة الإنتربول ومكتب الأمم المتحدة لمكافحة الإرهاب/مركز الأمم المتحدة لمكافحة الإرهاب، تم تنفيذها ضمن برنامج الأمم المتحدة العالمي لمكافحة الإرهاب حول أمن الفضاء الإلكتروني والتكنولوجيات الجديدة. وتهدف إلى تعزيز قدرات سلطات إنفاذ القانون والعدالة الجنائية في الدول الشريكة المحددة لمواجهة استغلال التكنولوجيات الجديدة والناشئة لأغراض إرهابية، بالإضافة إلى دعم وكالات إنفاذ القانون في الدول الشريكة في الاستفادة من التكنولوجيات الجديدة والناشئة في مكافحة الإرهاب.

ولتحقيق الهدف العام، تطبق المبادرة نتيجتين بارزتين مع ست مخرجات أساسية.

الشكل 1

الجدول 1 – المدخلات والمخرجات لمبادرة التكنولوجيا لمكافحة الإرهاب

النتيجة 1: استجابات سياساتية فعالة لمكافحة الإرهاب تجاه التحديات والفرص المتعلقة باستخدام التكنولوجيا الجديدة في مكافحة الإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.	
المخرج 1 – 1	تطوير المنتجات المعرفية لتصميم استجابات السياسات الوطنية لمكافحة الإرهاب للتصدي للتحديات والفرص التي توفرها التكنولوجيات الجديدة في مكافحة الإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.
المخرج 1 – 2	زيادة الوعي والمعرفة بالممارسات الجيدة بشأن تحديد المخاطر والفوائد المرتبطة بالتكنولوجيات الجديدة والإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.
المخرج 1 – 3	زيادة قدرات دول شريكة محددة على تطوير استجابات سياساتية وطنية فعالة لمكافحة الإرهاب من أجل مكافحة استخدام الإرهابيين للتكنولوجيات الجديدة والاستفادة من هذه التكنولوجيات الجديدة لمكافحة الإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.
النتيجة 2: زيادة القدرة التشغيلية لأجهزة إنفاذ القانون والعدالة الجنائية في مواجهة استغلال التكنولوجيا الجديدة لأغراض إرهابية واستخدام التكنولوجيا الجديدة لمنع الإرهاب ومكافحته مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.	
المخرج 2 – 1	تطوير أدوات وإرشادات عملية لإنفاذ القانون بشأن مكافحة استغلال التكنولوجيات الجديدة لأغراض إرهابية واستخدام هذه التكنولوجيات الجديدة لمنع الإرهاب ومكافحته مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.
المخرج 2 – 2	تعزيز مهارات مؤسسات إنفاذ القانون والعدالة الجنائية في الدول الشريكة لمكافحة استغلال التكنولوجيات الجديدة لأغراض إرهابية واستخدام هذه التكنولوجيات الجديدة لمكافحة الإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.
المخرج 2 – 3	زيادة التعاون وتبادل المعلومات بين أجهزة الشرطة الدولية بشأن مكافحة استخدام الإرهابيين للتكنولوجيات الجديدة واستخدام هذه التكنولوجيات الجديدة لمكافحة الإرهاب.

1 – 3 أغراض الوثيقة واستخداماتها

الهدف من هذه الوثيقة هو تزويد الدول الأعضاء بالأدوات الضرورية والفهم اللازم لإجراء تقييم للتهديدات في مناطق مسؤولياتهم، والعمل على التخفيف منها والتصدي لها بفعالية. كما تهدف إلى تقديم التوجيه بخصوص كيفية إجراء تقييم للتهديدات على الصعيد الوطني، ورفع مستوى الوعي وتقديم توجيهات غير ملزمة للممارسات الجيدة الخاصة بوضع وتنفيذ عملية تقييم المخاطر والتهديدات المتعلقة باستخدام التكنولوجيات الجديدة لأغراض إرهابية. من شأن هذا الفهم أن يساعد صنّاع السياسات على تحسين كفاءاتهم في تخطيط استجابات السياسات لتهديدات مكافحة الإرهاب، ولا سيما فيما يتعلق باستخدام وسوء استخدام التكنولوجيا الجديدة للأنشطة الضارة.

1 – 3 – 1 نطاق العمل

يقدم هذا الدليل تحليلاً تفصيلياً للتحديات المفروضة نتيجة استغلال الإرهابيين للتكنولوجيات الجديدة ويقدم توصيات عملية بكيفية الرد عليها. ويتضمن ممارسات وأمثلة لاستجابات السياسات الناجحة لعدد من الدول الأعضاء. وفي حين أن المصطلحات المتعلقة بالتكنولوجيات الجديدة تغطي مجموعة كبيرة من التكنولوجيات المختلفة، نجد أن هذا الدليل يركز على وجه الخصوص على استخدام وسوء استخدام التكنولوجيات الجديدة مثل الإنترنت ووسائل التواصل الاجتماعي والعملات المشفرة وميزة التعرف على الوجه وشبكة الإنترنت الخفية.

1 – 3 – 2 الجمهور المستهدف

هذه الوثيقة موجهة في المقام الأول لصنّاع السياسات والمسؤولين الحكوميين والعاملين في مجال مكافحة الإرهاب ووكالات إنفاذ القانون ووكالات الاستخبارات وأصحاب المصلحة ذوي الصلة المشاركين في بذل الجهود اللازمة لمكافحة الإرهاب. ويهدف الدليل إلى تقديم المعلومات والتوجيهات الشاملة بخصوص تشكيل استراتيجيات وسياسات فعّالة للتعامل مع التحديات الناشئة التي يفرضها الإرهابيون الذين يستفيدون من التكنولوجيات الجديدة، وجرى تصميمه لتلبية الاحتياجات والمسؤوليات المحددة لهذه الفئات المستهدفة. كما يزود أصحاب المصلحة الآخرين ذوي الصلة بالإرشادات العملية وأفضل الممارسات مثل المنظمات الدولية والدبلوماسيين وصنّاع السياسات والباحثين والأكاديميين المتخصصين في مجالات مكافحة الإرهاب والتكنولوجيا ورسم السياسات، بالإضافة إلى الخبراء العاملين في مجال التعاون والتنسيق الدولي لمكافحة الإرهاب، وأعضاء القطاع الخاص وشركات التكنولوجيا.

1 – 3 – 3 المزايا

تعكس هذه الوثيقة احتياجات ووجهات نظر شريحة كبيرة من أصحاب المصلحة بمن فيهم الخبراء العاملين في مجال مكافحة الإرهاب، والمسؤولين الحكوميين ووكالات الاستخبارات وإنفاذ القانون والباحثين الأكاديميين ومنظمات المجتمع المدني. أما الهدف الرئيسي من الوثيقة فهو زيادة قدرة صنّاع السياسات على التفاعل مع التكنولوجيات الجديدة كجزء أساسي من تخطيطهم الاستراتيجي ضد الأعمال الإرهابية، سواء أكان ذلك من خلال التصدي لاستغلال هذه التكنولوجيات أو استخدامها لمواجهة الأعمال الإرهابية.

يقدم الدليل إطاراً شاملاً ويغطي نطاقاً واسعاً من الاعتبارات الأساسية لصياغة استجابات السياسات الوطنية لمكافحة الإرهاب للحد من استخدام التكنولوجيات الجديدة لأغراض إرهابية. ويشمل أيضاً الممارسات الجيدة التي تبين الكيفية التي استخدمت بها الدول الأعضاء المختلفة للتكنولوجيات الجديدة في التصدي للإرهاب أو كيفية استجابتها لاستخدام التكنولوجيات الجديدة لأغراض إرهابية. تقدّم هذه الممارسات رؤى عملية تساعد صنّاع السياسات والعاملين في هذا المجال على تطوير سياسات واستراتيجيات فعالة لمكافحة الإرهاب. ويركز الدليل بالتحديد على استخدام التكنولوجيات الجديدة لأغراض إرهابية التي تتطور بصورة سريعة وتطرح تحديات وتهديدات جديدة. كما يسلط الضوء على بعض الاستخدامات المحتملة للتكنولوجيا الجديدة في مكافحة الإرهاب. ومن خلال تقديم الإرشادات بشأن كيفية مواجهة هذه التحديات، سيساعد الدليل الدول الأعضاء للبقاء في الطليعة والتصدي بفعالية للتهديدات الجديدة.

1 – 3 – 4 أوجه القصور

تعاني وثيقة "تصميم استجابات السياسات الوطنية لمكافحة الإرهاب للحد من استخدام التكنولوجيات الجديدة لأغراض إرهابية" من عدة قيود. وفي حين أن الدليل مصمم ليكون مرناً وقابلاً للتكيف مع مختلف السياقات الوطنية، فإنه يقر بمستوى نضج قدرات الدول الأعضاء المختلفة على تحديد الاستجابات والاحتياجات والأولويات المختلفة، ويشجع صنّاع السياسات والعاملين في هذا المجال على تكييف نهجهم وفقاً لذلك. ويستند الدليل إلى المشهد التكنولوجي وبيئة التهديد بدءاً من تاريخ نشره. ومع ظهور تكنولوجيات جديدة وتطور التكنولوجيات القائمة، ستنشأ حاجة إلى تطوير تفكير استراتيجي يراعي احتياجات الميدان وظروفه بما يتناسب مع السمات المستقبلية للتكنولوجيا الجديدة التي لم يتطرق لها الدليل.

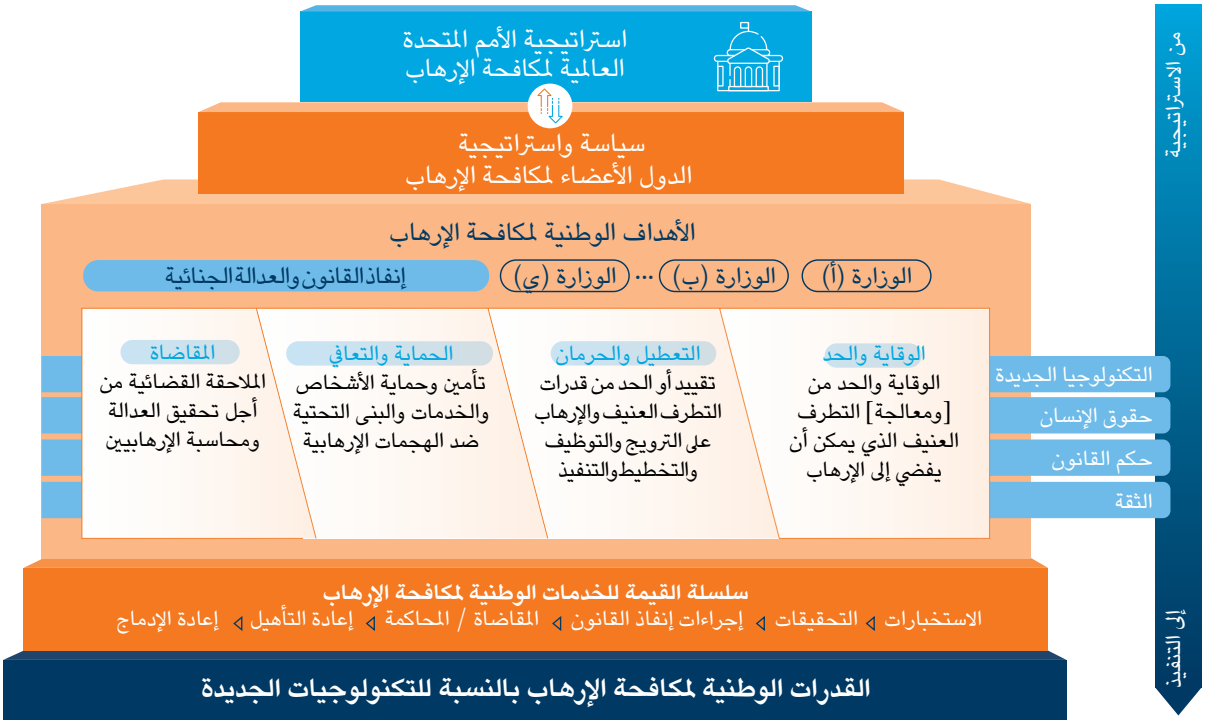
[ثانيا]
النهج

2 – 1 لمحة عامة

يسعى التقرير إلى دعم وتمكين الدول الأعضاء لإجراء تقييمات فعالة للتهديد في مجال مكافحة استخدام التكنولوجيات الجديدة لأغراض إرهابية، والتي تتماشى مع استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.

2 – 2 الإطار التوجيهي

الشكل 2



يعتبر الإطار التوجيهي نموذجاً مفاهيمياً يهدف إلى توجيه تطوير التقرير ومواءمته وإثرائه. ويسعى لضمان الترابط، بداية من الاستراتيجية حتى التنفيذ، بين استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب وأهداف السياسات والاستراتيجية الوطنية لمكافحة الإرهاب في الدول الأعضاء ونتائجها وخدماتها وقدراتها من منظور إنفاذ القانون والعدالة الجنائية، فيما يتعلق بالتكنولوجيات الجديدة.

تحدد استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، التي اعتمدتها الجمعية العامة، إجراءات واسعة للدول الأعضاء لمواجهة التهديدات الإرهابية، والتي تندرج تحت أربع ركائز رئيسية:

الركيزة الأولى:	إجراءات لمعالجة الظروف المؤدية إلى انتشار الإرهاب
الركيزة الثانية:	إجراءات للوقاية والحد من الإرهاب ومكافحته
الركيزة الثالثة:	الإجراءات الرامية إلى بناء قدرة الدول على منع الإرهاب ومكافحته وتعزيز دور منظومة الأمم المتحدة في هذا الصدد
الركيزة الرابعة:	الإجراءات الرامية إلى ضمان احترام حقوق الإنسان للجميع وسيادة القانون كأساس جوهري في مكافحة الإرهاب

يتم تشجيع الدول الأعضاء على تطوير أطرها الوطنية القانونية والسياساتية لمكافحة الإرهاب بما يتماشى مع استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب. حيث يجب عليها أن تضمن توافق قوانينها وسياساتها واستراتيجياتها وإجراءاتها في مكافحة الإرهاب مع التزاماتها بموجب القانون الدولي، بما في ذلك القانون الدولي لحقوق الإنسان، والقانون الدولي للاجئين، والقانون الإنساني الدولي. وينبغي لأطر القوانين والسياسات الوطنية لمكافحة الإرهاب في الدولة العضو أن تسعى عموما للحد من التطرف العنيف الذي قد يفضي إلى الإرهاب ومعالجته، والحد من الأنشطة الإرهابية أو تقييدها، واتخاذ الإجراءات الملائمة لحماية الأشخاص الخاضعين لسلطة الدولة والخدمات والبنية التحتية من تهديد الهجمات الإرهابية المتوقعة بالقدر الممكن والمعقول، وضمان محاسبة الإرهابيين على أفعالهم.

ولتحقيق النتائج والأهداف في مجال مكافحة الإرهاب، تمتلك سلطات إنفاذ القانون والعدالة الجنائية الوطنية في الدول الأعضاء مجموعة من الأدوات تحت تصرفها. تشمل ما يلي على سبيل المثال لا الحصر:

الجدول 2 – خدمات إنفاذ القانون والعدالة الجنائية الوطنية الرفيعة المستوى في مكافحة الإرهاب

الخدمات	الوصف
إجراءات العدالة الجنائية	هي إجراءات قانونية لتوجيه تهم الإرهاب لفرد أو كيان وجلسة المحكمة والحكم أو القرار والعقوبة وكذلك الإصلاح وإعادة التأهيل.
الاستخبارات / التحريات الجنائية	هي ناتج جمع المعلومات ومعالجتها ونشرها وتحليلها وتفسيرها والتي جمعت من مصادر متعددة، بهدف إفادة صناع القرار لأغراض التخطيط لاتخاذ القرارات أو الإجراءات – على المستوى الاستراتيجي أو التشغيلي أو التكتيكي. يجب جمع الاستخبارات والتحريات وحفظها واستخدامها ومشاركتها وفقًا لالتزامات الدول الأعضاء المعنية بموجب القانون الدولي لحقوق الإنسان.
التحقيقات الجنائية	هي عملية جمع المعلومات (أو الأدلة) لتقرير ارتكاب الجريمة من عدمه، وتحديد الجاني وتقديم الأدلة التي تدعم إجراءات العدالة الجنائية.
إجراءات إنفاذ القانون	تصف عادة إجراءات إنفاذ القانون المتخذة حيال تهديد ما، والتي قد تشمل احتجاز الفرد (أو الأفراد)، وإعاقة أنشطة الجهات المهددة (مثل إزالة المحتوى، وحجز الأصول).. إلخ.
إعادة التأهيل	في سياق العدالة الجنائية، يُستخدم مصطلح "إعادة التأهيل" للإشارة إلى التدخلات التي يديرها نظام الإصلاحيات بهدف تغيير آراء الجاني أو سلوكه لتقليل احتمالية معاودة ارتكاب الجريمة، وتهيئة ودعم إعادة الاندماج في المجتمع.
إعادة الإدماج	عملية شاملة لإعادة إدماج الشخص في بيئة اجتماعية و/أو وظيفية.

يعتمد الاستخدام والنشر الفعال لمثل هذه الخدمات والأدوات على مجموعة من القدرات الأساسية. ويتم غالبا تعريف القدرات المطلوبة لتمكين الخدمات وتقديمها وعرضها ضمن نموذج القدرات. حيث يمثل نموذج القدرات تحليلا وظيفيا للوظائف الرئيسية إلى مجموعات منطقية ومتناهية الصغر تدعم تنفيذ الخدمات والأنشطة. ويوضح نموذج القدرات المتطلبات من الأشخاص (الهيكل التنظيمي والمهارات) والعمليات والتكنولوجيا والبنية التحتية والتمويل.

ويعمل الإطار التوجيهي على ضمان التوافق بين الاستراتيجية والتنفيذ في كلا الاتجاهين "التنازلي" و "التصاعدي".

2 – 3 المنهجية

الشكل 3

تتضمن المنهجية المتبعة في وضع هذه الوثيقة والمعنونة بـ "تصميم استجابات السياسات الوطنية لمكافحة الإرهاب للحد من استخدام التكنولوجيات الجديدة لأغراض إرهابية" البحث والتحليل والاستشارة مع الخبراء وأصحاب المصلحة، والتي تشمل وثائق مشروع التكنولوجيا لمكافحة الإرهاب واستشارة أصحاب المصلحة والتحليل الداخلي والبحث المكتبي واجتماعات فريق الخبراء والتنسيق مع كيانات الاتفاق العالمي لتنسيق مكافحة الإرهاب التابعة للأمم المتحدة، والإطار التوجيهي على النحو المبين أعلاه في القسم 2 – 2. يركز البحث على تحديد التحديات والفرص الرئيسية التي تقدمها التكنولوجيات الجديدة في سياق الإرهاب، وكذلك الاستجابات الحالية لاستراتيجيات وسياسات مكافحته.

وتضمنت الخطوة الأولى تنفيذ بحث مكثّف للتحديات والفرص التي تطرحها التكنولوجيات الجديدة في سياق مكافحة الإرهاب. انطوى البحث المكتبي هذا على مراجعة المطبوعات الحالية ودراسات الحالات وأفضل الممارسات وذلك لتحديد العناصر الرئيسية والاستراتيجيات الفعّالة لتطوير استجابات سياسات مكافحة الإرهاب، بما فيها تحليل التكنولوجيات الجديدة وإمكانية استغلالها من قبل الإرهابيين، فضلاً عن إمكانية استخدامها من قبل العاملين في مجال مكافحة الإرهاب. وتضمنت الخطوة الثانية التعريف بالممارسات الجيدة ضمن الاستجابات الحالية لسياسات واستراتيجيات مكافحة الإرهاب التي تتصدى لتحديات الإرهاب التكنولوجي الجديد. أما الخطوة الثالثة فقد اشتملت على وضع مسودة دليل جرت مشاركتها مع أصحاب المصلحة والخبراء للحصول على الملاحظات. وقد أُدرجت هذه الملاحظات في الدليل النهائي، حيث جرى تحديد الاعتبارات الرئيسية والعناصر المشتركة، بما يكفل أن تعكس أحدث الأفكار والممارسات الجيدة في الميدان. واستناداً إلى الأبحاث والتحليلات والاستشارات، ووضع إطار شامل لتصميم استجابات السياسات الوطنية لمكافحة الإرهاب للحد من استخدام التكنولوجيات الجديدة لأغراض إرهابية.

يتضمن هذا الإطار عدة اعتبارات تهدف إلى التعامل مع الثغرات في استراتيجيات مكافحة الإرهاب فيما يخص التكنولوجيا الجديدة. ويسعى أيضاً لتقديم أمثلة عن ممارسات جيدة بهدف وضع بروتوكولات وسياسات لمكافحة الإرهاب للتصدي للتهديدات الناجمة عن التكنولوجيا الجديدة التي يمكن أن تستغلها جهات إرهابية.

تضمنت مصادر البحث المكتبي التقييمات الوطنية للتهديدات والمخاطر للدول الأعضاء، ومنظمات حكومية دولية، ووثائق من القطاعين العام والخاص بشأن تقييم التهديدات، ومصادر أكاديمية. ونظرًا لكون هذه الوثيقة الخاصة تركز على تطبيقات تقييم التهديدات والمخاطر فيما يتعلق بالتكنولوجيا الجديدة، تجدر الإشارة إلى أن بعض النماذج التي استمدت هذه الوثيقة المعلومات منها كانت أيضًا متأثرة بأطر تقييم التهديدات ضمن عالم الأمن السيبراني.

2 – 3 – 1 اجتماعات ومشاورات فريق الخبراء

تم تطوير هذا الدليل بمشاركة الخبراء من خلال جلسات اجتماع فريق الخبراء بالإضافة إلى استشارات ومراجعات فردية. جمع اجتماع فريق الخبراء بين مجموعة من الخبراء والممارسين من وكالات مكافحة الإرهاب وإنفاذ القانون، وحقوق الإنسان، والقطاع الخاص، والجهات الأكاديمية، والمجتمع المدني، لمناقشة طرق مواجهة استخدام التكنولوجيات الجديدة لأغراض إرهابية وتوظيف هذه التكنولوجيات كجزء من هذا الجهد، وتحديد الممارسات الجيدة في هذا الصدد، إضافة إلى مناقشة المخاطر والتحديات والممارسات غير الجيدة التي تتطلب التنبه والحذر. وقد خضع الدليل لمزيد من التهذيب بمشاركة ميثاق الأمم المتحدة العالمي لتنسيق مكافحة الإرهاب ومجموعته العاملة في مواجهة التهديدات الناشئة وحماية البنية التحتية الحيوية، والتي تعمل على تعزيز التنسيق والترابط لدعم جهود الدول الأعضاء في منع التهديدات الإرهابية الناشئة والاستجابة لها، مع احترام حقوق الإنسان وسيادة القانون كأساس جوهري، بالتوافق مع القانون الدولي، بما في ذلك حقوق الإنسان والقانون الإنساني وقانون اللاجئين.

2 – 3 – 2 مراجعة الوثيقة المرجعية

تم تطوير هذا الدليل بناءً على الأبحاث والأدلة الإرشادية والمنشورات الحالية وتم أخذها في الاعتبار والبناء عليها واستكمالها، وتتضمن ما يلي:

الجدول 3 – المراجع

1 Amritt, Carl, Eliot Bradshaw, and Alyssa Schulenberg. "Threat Assessment and Management: Practices Across the World." Domestic Preparedness, February 1, 2023. https://www.domesticpreparedness.com/preparedness/threat-assessment-and-management-practices-across-the-world.

2 Bloom, Mia, Hicham Tiflati, and John Horgan. "Navigating ISIS's Preferred Platform: Telegram." Terrorism and Political Violence 31, no. 6 (November 2, 2019): 1242–54. https://doi.org/10.1080/09546553.2017.1339695.

3 "Counter Terrorism Legal Framework: Lessons Learned from IDLO Policy Dialogues in Collaboration with UNODC." Development Law Update, no. 2 (2007). https://www.files.ethz.ch/isn/138640/14.pdf.

4 Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency, Australian Cyber Security Centre, Canadian Centre for Cyber Security, New Zealand Computer Emergency Response Team, United Kingdom National Cyber Security Centre, Germany Federal Office for Information Security (BSI), and Netherlands' National Cyber Security Centre. "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default," April 13, 2023. https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf.

5 European Commission. A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, Belgium: European Commission, 2020. https://home-affairs.ec.europa.eu/system/files/2020-12/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf.

6 European Commission. "Cyber Resilience Act," September 15, 2022. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

7 European Commission. Security by Design: Protection of Public Spaces from Terrorist Attacks. Luxembourg: European Union, 2022. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC131172/JRC131172_01.pdf.

8 European Commission: Cordis. "Detecting and Analysing Terrorist-Related Online Contents and Financing Activities." Accessed April 23, 2023. https://cordis.europa.eu/project/id/700367.

9 European Commission: Cordis. "Retrieval and Analysis of Heterogeneous Online Content for Terrorist Activity Recognition." Accessed April 23, 2023. https://cordis.europa.eu/project/id/700024.

10 European Cybercrime Centre (EC3). "Internet Organized Crime Threat Assessment 2019." Europol, 2019. https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf.

الجدول 3 – المراجع

European Union. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, Pub. L. No. 2002/475/JHA, 088 OJ L 6 (2017). http://data.europa.eu/eli/dir/2017/541/oj/eng. 11

Financial Action Task Force (FATF). "Virtual Assets." Financial Action Task Force (FATF). Accessed May 7, 2023. https://www.fatf-gafi.org/en/topics/virtual-assets.html. 12

Finland Ministry of the Interior. National Counter-Terrorism Strategy 2022–2025. Publications of the Ministry of the Interior, 2022:38. Helsinki, Finland: Finland Ministry of the Interior, 2022. https://julkaisut.valtioneuvosto.fi/handle/10024/164447. 13

Flanders, Rob, Lucy Johnson, Matthew Trevelyan, Anna Whitmore, Lisa Lesowiec, and Rajinder Tumber. Cyber Threat Intelligence in Government: A Guide for Decision Makers and Analysts. 2nd ed. United Kingdom, 2019. https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf. 14

Freese, Rebecca. "Evidence-Based Counter-terrorism or Flying Blind? How to Understand and Achieve What Works." Perspectives on Terrorism 8, no. 1 (2014): 37–56. http://www.jstor.org/stable/26297099. 15

Government of Australia. Safeguarding Our Community Together: Australia's Counter-Terrorism Strategy 2022. Australia: The Commonwealth of Australia, 2022. https://www.nationalsecurity.gov.au/what-australia-is-doing-subsite/Files/safeguarding-community-together-ct-strategy-22.pdf. 16

Gruetzemacher, Ross. "The Power of Natural Language Processing." Harvard Business Review, April 19, 2022. https://hbr.org/2022/04/the-power-of-natural-language-processing. 17

Interior Ministry of Spain. National Counter-Terrorism Strategy, 2019. https://www.dsn.gob.es/eu/file/4271/download?token=-K6uOf-C. 18

Joint Counter-terrorism Assessment Team (JCAT). "Counter Terrorism Guide for Public Safety Personnel." Government. Director of National Intelligence. Accessed April 10, 2023. https://www.dni.gov/nctc/jcat/index.html. 19

Lutkevich, Ben, and Ed Burns. "What Is Natural Language Processing? An Introduction to NLP." Enterprise AI. Accessed April 30, 2023. https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP. 20

National Cyber Security Centre. "Secure by Default." National Cyber Security Centre, March 7, 2018. https://www.ncsc.gov.uk/information/secure-default. 21

New Zealand Security Intelligence Service. "How You Can Help: Public Contribution Form." Accessed April 23, 2023. https://providinginformation.nzsis.govt.nz/. 22

الجدول 3 – المراجع

New Zealand Transport Agency. "Risk Register." Government. Waka Kotahi NZ Transport Agency. Accessed April 1, 2023. https://www.nzta.govt.nz/roads-and-rail/rail/operating-a-railway/risk-management/risk-register.	23
OSCE Transnational Threats Department. "Status of the Universal Anti-Terrorism Conventions and Protocols as Well as Other International and Regional Legal Instruments Related to Terrorism and Co-Operation in Criminal Matters in the OSCE Area." Organization for Security and Co-Operation in Europe (OSCE), July 2018. https://www.osce.org/files/f/documents/5/8/17138_0.pdf.	24
OSCE Transnational Threats Department. Status of the Universal Anti-Terrorism Conventions and Protocols as Well as Other International and Regional Legal Instruments Related to Terrorism and Co-Operation in Criminal Matters in the OSCE Area." Organization for Security and Co-Operation in Europe (OSCE), July 2018. https://www.osce.org/files/f/documents/5/8/17138_0.pdf.	25
Romyn, David, and Mark Kebbell. "Terrorists' Planning of Attacks: A Simulated 'Red-Team' Investigation into Decision-Making." Psychology, Crime & Law 20, no. 5 (May 28, 2014): 480–96. https://doi.org/10.1080/1068316X.2013.793767.	26
Schneier, Bruce, and Tarah Wheeler. "Hacked Drones and Busted Logistics Are the Cyber Future of Warfare." Brookings. Tech Stream (blog), June 4, 2021. https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/.	27
Spulak, Robert G. "Science Technology and Innovation in Combating Terrorism.," February 2015. https://www.osti.gov/biblio/151395.	28
Talley, Ian. "Islamic State Turns to NFTs to Spread Terror Message." Wall Street Journal, September 4, 2022, sec. Politics. https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800.	29
Terrell Hanna, Katie. "What Is the Dark Web (Darknet)?" WhatIs.com. Accessed May 7, 2023. https://www.techtarget.com/whatis/definition/dark-web.	30
The Commonwealth of Australia. 2017 Foreign Policy White Paper. Edited by Morris Walker Pty Ltd. Australia, 2017. https://www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf.	31
UKC3. "Cyber Cluster Operating Framework." UK Cyber Cluster Collaboration (blog). Accessed March 30, 2023. https://ukc3.co.uk/cyber-cluster-operating-framework/.	32
United Kingdom. CONTEST: The United Kingdom's Strategy for Countering Terrorism. United Kingdom: The Crown, 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf.	33
United Kingdom Department for and Business, Energy and Industrial Strategy. National Security and Investment Bill, Pub. L. No. BEIS006(F)-20-CCP (2020). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934276/nsi-impact-assessment-beis.pdf.	34

الجدول 3 – المراجع

35 United Nations Counter–Terrorism Centre (UNCCT). “Summary of Discussions: International Conference on National and Regional Counter–Terrorism Strategies– January 31–February 1, 2013.” Conference Summary. Bogota, Colombia, 2013. https://www.un.org/counter–terrorism/sites/www.un.org.counter–terrorism/files/bogota_jan–feb2013.pdf.

36 United Nations Counter–Terrorism Centre and United Nations Interregional Crime and Justice Research Institute. “Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter–Terrorism Agencies in South Asia and South–East Asia.” Joint Report. United Nations, 2021. https://unicri.it/News/–Countering–Terrorism–Online–with–Artificial–Intelligence.

37 United Nations Counter–Terrorism Centre and United Nations Interregional Crime and Justice Research Institute. “Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter–Terrorism Agencies in South Asia and South–East Asia.” Joint Report. United Nations, 2021. https://unicri.it/News/–Countering–Terrorism–Online–with–Artificial–Intelligence.

38 United Nations Office of Counter–Terrorism. “International Legal Instruments.” Accessed April 25, 2023. https://www.un.org/counter–terrorism/international–legal–instruments.

39 United Nations Office on Drugs and Crime. “Counter–Terrorism Module 12 Key Issues: Accountability, Oversight of Intelligence Gathering Methods.” United Nations Office on Drugs and Crime (UNDOC), July 2018. https://www.unodc.org/e4j/en/terrorism/module–12/key–issues/accountability–oversight–of–intelligence–gathering–methods.html.

40 United Nations: Office on Drugs and Crime. “International Legal Framework.” Accessed April 25, 2023. https://www.unodc.org/unodc/en/terrorism/expertise/international–legal–framework.html.

41 United Nations Security Council Counter–Terrorism Committee Executive Directorate (CTED). “CTED Analytical Brief: Countering Terrorist Narratives Online and Offline.” United Nations, 2020. https://www.un.org/securitycouncil/ctc/content/cted–analytical–brief–%E2%80%93–countering–terrorist–narratives–online–and–offline.

42 United States. National Strategy for Counter–terrorism of the United States of America. Washington, DC: The White House, 2018. https://purl.fdlp.gov/GPO/gpo109871.

43 Vidino, Lorenzo, and Clifford Bennett. “A Review of Transatlantic Best Practices for Countering Radicalization in Prisons and Terrorist Recidivism.” The Hague, Netherlands: Europol, 2019. https://www.europol.europa.eu/cms/sites/default/files/documents/a_review_of_transatlantic_best_practices_for_countering_radicalisation_in_prisons_and_terrorist_recidivism.pdf.

[ثالثا]
مقدمة

3 – 1 لمحة عامة

نظراً لتسارع التقدم في مجال التكنولوجيا، يسعى الإرهابيون بصورة متزايدة لاستغلال هذه الابتكارات لتطوير خططهم التدميرية. وقد فرض الانتشار السريع لمنصات التواصل وشبكات التواصل الاجتماعي وتقنيات التشفير والتكنولوجيات الناشئة تحديات كبيرة لسلطات إنفاذ القانون، غير أن إدخال التكنولوجيا وضمها إلى ترسانة المجموعات الإرهابية فرض تحديات غير مسبوقة، ما اضطر الحكومات إلى إعادة تقييم استراتيجياتها وتبني أساليب تتكيف مع آخر المستجدات.

يتعين على الدول الأعضاء عند تشكيل سياسات مكافحة الإرهاب الإقرار بالحاجة الماسة لفهم إمكانية استغلال الإرهابيين للتكنولوجيات الناشئة والقدرة على التنبؤ بها والاستجابة لها بفاعلية. تركز هذه السياسات على مجموعة من الجوانب، بما فيها الوعي والتدخل في حال التهديد والقدرات الوطنية لمكافحة الإرهاب والتعاون ومبادرات بناء القدرات. وتسعى الحكومات لتبقى في الصدارة من خلال تبني سياسات وطنية شاملة ورشيدة لمكافحة الإرهاب، والعمل على التخفيف المسبق للمخاطر المتعلقة باستخدام الإرهابيين للتكنولوجيات الجديدة، وفي الوقت نفسه ضمان الأمان والخصوصية والحقوق الأساسية والحريات المدنية لمواطنيها.

3 – 2 التكنولوجيات الجديدة ومكافحة الإرهاب

يقود التقدم في التكنولوجيا الرقمية والبيانات وشبكة الإنترنت اليوم إلى عالم شديد الترابط، حيث يمكن الوصول إلى المعلومات ومشاركتها واستلامها بصورة لحظية تقريبا. حيث كان ما يقرب من 70 في المائة من سكان العالم يستخدمون الإنترنت بحلول عام 2022[19]، أكثر من 93 في المائة هم من مستخدمي وسائل التواصل الاجتماعي[20]. ويُقدر عالميًا أنه قد تم إنشاء أكثر من 97 زيتابايت[21] من المعلومات في عام 2022[22]. وفي حين توفر مثل هذه التكنولوجيات فرصة لتحويل المجتمع نحو الصالح العام، فإن الجهات الإرهابية تستغل هذه التكنولوجيا لأغراضها الشنيعة. حيث يفرض استخدام التكنولوجيات الجديدة لأغراض إرهابية تحديات كبيرة أمام الدول الأعضاء في التصدي للإرهاب، وخاصة عند استخدام تكنولوجيات تسمح بإخفاء الهوية والقدرة على التنسيق والعمل عن بُعد.

من ناحية أخرى، تتيح التكنولوجيات الجديدة فرصا كبيرة كعامل مضاعفة لقدرات سلطات إنفاذ القانون ومكافحة الإرهاب. على سبيل المثال، يمكن لهذه التكنولوجيات أن تتيح لسلطات إنفاذ القانون القيام بالمزيد باستخدام موارد أقل، وتسريع اتخاذ القرارات في الوقت المناسب، وتوليد رؤى جديدة، وإجراء عمليات التعطيل عن بُعد.

19 تقرير التواصل العالمي للاتحاد الدولي للاتصالات 2022، https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/index/.

20 بيانات دومو لا تنام أبدًا، Data Never Sleeps 10.0 | Domo.

21 الزيتابايت يساوي مليار تيرابايت.

22 ستاتيستا، Total data volume worldwide 2010–2025 | Statista.

وتتوقف مكافحة استخدام الجهات الإرهابية للتكنولوجيات الجديدة على فهم طريقة استخدام الجهات الإرهابية لهذه التكنولوجيات، وتطوير إطار قانوني واستجابات سياسية فعّالة، وبناء القدرة التشغيلية للتصدي لاستخدام مثل هذه التكنولوجيات لأغراض إرهابية، بما في ذلك توظيف التكنولوجيات الجديدة واعتمادها.

3 – 2 – 1 التحديات – استخدام التكنولوجيات الجديدة لأغراض إرهابية

إن التقدم في تكنولوجيا المعلومات والاتصالات وتوافرها جعلها مغرية للجماعات الإرهابية وجماعات التطرف العنيف لاستغلال الإنترنت ووسائل التواصل الاجتماعي في تيسير مجموعة واسعة من الأنشطة، بما في ذلك التحريض، والتطرف، والتجنيد، والتدريب، والتخطيط، وجمع المعلومات، والتواصل، والتحضير، والترويج، والتمويل. وتستغل الجماعات الإرهابية ببراعة أيضا عدم المساواة بين الجنسين والمعايير والأدوار المتعلقة بالجنسين، بما في ذلك العنف الذكوري، وتتلاعب بها لخدمة أغراضها. على سبيل المثال، عملت "داعش" ببراعة على توظيف النساء من خلال وسائل التواصل الاجتماعي، معدلة رسائلها لجذب النساء اللاتي يتحدثن لغات مختلفة ويعيشن في سياقات اجتماعية واقتصادية وثقافية متنوعة في أوروبا الغربية وآسيا الوسطى والشرق الأوسط وشمال أفريقيا، مستغلة غالبا تجارب النساء في عدم المساواة بين الجنسين. كما يستخدم الإرهابيون الاتصالات المشفرة والشبكة المظلمة لمشاركة المحتوى الإرهابي والخبرات، مثل تصاميم الأجهزة المتفجرة المرتجلة واستراتيجيات الهجوم، وكذلك لتنسيق الهجمات وتيسيرها وتوفير الأسلحة والوثائق المزورة. وفي الوقت ذاته قد تعني التطورات في مجالات الذكاء الاصطناعي والتعلم الآلي والجيل الخامس من الاتصالات والروبوتات والبيانات الضخمة والمرشحات الخوارزمية والتكنولوجيا الحيوية والسيارات ذاتية القيادة والطائرات بدون طيار أنه عندما تصبح هذه التكنولوجيات متوفرة تجارياً وميسورة التكلفة وسهلة الاستخدام، قد يستغلها الإرهابيون أيضاً لتوسيع نطاق هجماتهم وخطورتها.

3 – 2 – 2 الفرص – إنفاذ القانون في مكافحة الإرهاب

توفر التكنولوجيات الجديدة فرصا لا حصر لها لوكالات إنفاذ القانون لمكافحة الإرهاب بفاعلية، مع الحفاظ على ممارسات مسؤولة تجاه القوانين الدولية لحقوق الإنسان. يمكن لسلطات إنفاذ القانون توظيف التكنولوجيات الجديدة لاكتشاف الأنشطة الإرهابية والتحقيق فيها وملاحقتها قضائيا ومحاكمتها بطرق جديدة أكثر فاعلية.

تسمح استخبارات المصادر المفتوحة بالجمع السريع للمعلومات حول الأهداف المعنية، مما يجعل أنشطة إنفاذ القانون أكثر فاعلية. وتتيح قدرات تحليل البيانات المتقدمة والذكاء الاصطناعي معالجة كميات هائلة من المعلومات وتحليلها، مما يمكن أجهزة إنفاذ القانون من تحديد الأنماط وكشف التهديدات المحتملة والاستجابة الاستباقية لأنشطة الإرهاب. كما تساعد نظم المراقبة المتقدمة، بما في ذلك التعرف على الوجوه والتكنولوجيات البيومترية، في التعرف على المشتبه بهم وتتبعهم، مما يعزز كفاءة التحقيقات ومنع الهجمات المحتملة وملاحقة الإرهابيين. علاوة على ذلك، تساعد أدوات التحليل الجنائي الرقمية في استخراج الأدلة الحاسمة من الأجهزة الإلكترونية، مما يمكن أجهزة إنفاذ القانون من كشف الروابط الخفية وتعطيل الشبكات الإرهابية ومحاكمة الإرهابيين.

يمكن أن يساهم استغلال التكنولوجيات الجديدة في تحديد أولويات موارد إنفاذ القانون المحدودة بطريقة أكثر فاعلية. ولكن من الأهمية بمكان أن توظف هذه التكنولوجيات بشكل أخلاقي مع الامتثال الصارم للخصوصية وحقوق الإنسان وسيادة القانون. ويجب تطبيق إجراءات الشفافية والمساءلة لضمان الاستخدام المسؤول ومنع أي إساءة استخدام محتملة لهذه الأدوات القوية. كما يجب إجراء برامج تدريب شاملة لتزويد موظفي إنفاذ القانون بالمهارات اللازمة لتوظيف التكنولوجيات الجديدة بشكل فعال لا يتجاوز حدود الأطر القانونية والأخلاقية. يمكن لأجهزة إنفاذ القانون من خلال استغلال التكنولوجيا الجديدة بشكل مسؤول، تعزيز جهودها في مجال مكافحة الإرهاب وحماية أمن المجتمعات وسلامتها.

3 – 2 – 3 حقوق الإنسان والتكنولوجيات الجديدة

يمثل الإرهاب تحديا خطيرا لمبادئ حكم القانون بذاتها، ولحماية حقوق الإنسان، وتطبيقها بشكل فعال. حيث يمكن للإرهاب أن يؤدي إلى زعزعة استقرار الحكومات المشكلة بشكل شرعي، وتقويض دعائم المجتمع المدني المتعدد الأطياف، وتهديد الأمن والسلام، وتعريض التنمية الاجتماعية والاقتصادية للخطر. وتتحمل الدول مسؤولية اتخاذ الإجراءات المناسبة لحماية الأفراد الخاضعين لسيادتها من تهديد الهجمات الإرهابية المتوقعة بشكل معقول. ويشمل واجب الدول في حماية حقوق الإنسان الالتزام باتخاذ الإجراءات اللازمة والكافية لمنع الأنشطة التي تعرض هذه الحقوق للخطر ومحاربتها والمعاقبة عليها، كالتهديدات

الموجهة للأمن القومي أو الجرائم العنيفة، بما في ذلك الإرهاب. ويجب أن تتوافق جميع هذه الإجراءات بذاتها مع القوانين الدولية لحقوق الإنسان ومعايير سيادة القانون.

وفي سياق استخدام التكنولوجيات الجديدة لمكافحة الأنشطة الإرهابية، يجب على الدول ضمان احترام القوانين والسياسات والممارسات المعنية للحقوق: كحق الخصوصية، وحقوق حرية التعبير وحرية التجمع، وحرية الفكر والوجدان والدين، وحق الفرد في الحرية والأمن، وحق الحصول على محاكمة عادلة بما في ذلك قرينة البراءة، ومبدأ عدم التمييز. كما يجب أن تلتزم الدول أيضا بمنع التعذيب والمعاملة القاسية أو اللاإنسانية أو المهينة منعا قاطعا.

وقد أكدت كل من الأمم المتحدة والانتربول والاتحاد الأوروبي مرارا وتكرارا على الارتباط المتبادل بين التكنولوجيات الجديدة ومكافحة الإرهاب وحقوق الإنسان، بما في ذلك المساواة بين الجنسين. وتُسلط استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب ومختلف قرارات الجمعية العامة ومجلس الأمن الضوء على التزامات الدول الأعضاء في إطار القانون الدولي لحقوق الإنسان والقانون الإنساني الدولي والقانون الدولي للاجئين عند مكافحة الإرهاب. وتقر استراتيجية الأمم المتحدة لمكافحة الإرهاب، على وجه الخصوص، بأن "إجراءات مكافحة الإرهاب الفعالة وحماية حقوق الإنسان ليست أهدافا متعارضة، بل هي متكاملة وتعزز بعضها البعض" وتتطلب إجراءات لضمان احترام حقوق الإنسان للجميع وسيادة القانون كأساس جوهري للحرب ضد الإرهاب. وبشكل خاص، شجعت الاستراتيجية الدول الأعضاء على معالجة استخدام الإنترنت وغيرها من تكنولوجيا المعلومات والاتصالات، ومنها منصات التواصل الاجتماعي، لأغراض إرهابية، بما في ذلك استمرار انتشار المحتوى الإرهابي، مع احترام القانون الدولي، متضمنا القانون الدولي لحقوق الإنسان، وحق حرية التعبير.

3 - 2 - 4 النوع الاجتماعي والتكنولوجيا وتقييم التهديدات

يشير النوع الاجتماعي إلى الأدوار والسلوكيات والأنشطة والصفات التي تعتبرها المجتمعات المختلفة، في فترة زمنية معينة، ملائمة للرجال والنساء والفتيان والفتيات. بالإضافة إلى الصفات والفرص الاجتماعية المرتبطة بكون الإنسان ذكرا أو أنثى، يرتبط النوع الاجتماعي أيضا بالعلاقات بين النساء والرجال والفتيان والفتيات. ويشكل النوع الاجتماعي جزءا من السياق الاجتماعي الثقافي الأوسع، ويتقاطع مع عوامل الهوية الأخرى، بما في ذلك الجنس والطبقة الاجتماعية والعرق ومستوى الفقر والإثنية والتوجه

الجنسي والعمر، من ضمن عوامل أخرى. ويختبر الرجال والنساء والفتيان والفتيات، وكذلك الأشخاص ذوو الهوية الجنسية أو التعبير الجنسي المختلف، يختبرون الأمن بطرق مختلفة وفقًا لاحتياجاتهم وجوانب ضعفهم وقدراتهم الخاصة[23]. وبالنسبة لاستخدام التكنولوجيات الجديدة تحديدا، في حين يمكن لغياب البنى الهيكلية الهرمية على الإنترنت أن يزيل القيود المتعلقة بالنوع الاجتماعي، ويوفر فرصا لتمكين النساء، فأنه يزيد من احتمالية تجنيدهن أو مشاركتهن النشطة في مجموعات التطرف العنيفة أو المجموعات الإرهابية عبر الإنترنت[24]. كما تشير الأدلة إلى أن المجموعات الإرهابية تستغل النوع الاجتماعي في رسائلها عبر الإنترنت؛ على سبيل المثال، استخدم تنظيم "داعش" رسائل متناقضة متعلقة بالنوع الاجتماعي بطريقة استراتيجية في تجنيده واتصالاته، حيث قام بتغيير خطابه وفقا لجمهوره المستهدف[25]. يتمثل أحد الجوانب المهمة الأخرى المتعلقة بالنوع الاجتماعي والتكنولوجيات الجديدة في الفجوة الرقمية بين الجنسين، حيث تقدر إمكانية وصول النساء إلى الإنترنت عالميا بـ 85 في المئة من إمكانية وصول الرجال، بوجود عدد تقديري يبلغ نحو 1,7 مليار امرأة في الجنوب العالمي محرومة من فرصة الوصول إلى الانترنت. تشكل هذه الفجوة قلقا حول حقوق الإنسان يكمن في جميع جوانب أمن الفضاء الإلكتروني، بما في ذلك التعرض المحتمل للمخاطر وعدم الأمان أو المشاركة في الحوكمة[26].

إن تضمين الجوانب المتعلقة بالنوع الاجتماعي في تقييم التهديدات الإرهابية والاستجابة لها ضروري للغاية لتقييم نوايا الإرهابيين والأهداف المحتملة، ولتصميم استجابات مناسبة تلبي الاحتياجات وجوانب الضعف لدى الأشخاص من الجنسين، مع مراعاة العوامل المتقاطعة، كالعمر، والإعاقة، والإثنية، واللغة، والجنسية، والهوية العرقية، والدين، والتوجه الجنسي، أو أي عامل هوية آخر أو مجموعة منها.

23 مركز جنيف للرقابة الديمقراطية على القوات المسلحة، ومنظمة الأمن والتعاون في أوروبا/مكتب المؤسسات الديمقراطية وحقوق الإنسان، وهيئة الأمم المتحدة للمرأة، مجموعة أدوات النوع الاجتماعي وإصلاح قطاع الأمن (جنيف: مركز جنيف للرقابة الديمقراطية على القوات المسلحة، 2008). https://www.dcaf.ch/gender-and-security-toolkit.

24 المديرية التنفيذية للجنة مكافحة الإرهاب، "الأبعاد الجنسانية للرد على المقاتلين الإرهابيين الأجانب العائدين – وجهات نظر بحثية"، شباط/فبراير 2019.

25 نيللي لحود، "التمكين أو القهر: تحليل لرسائل داعش المتعلقة بالنوع الاجتماعي" (هيئة الأمم المتحدة للمرأة، حزيران/يونيه 2018).

26 مركز جنيف للرقابة الديمقراطية على القوات المسلحة، "المساواة بين الجنسين والأمن السيبراني وحوكمة قطاع الأمن – فهم دور النوع الاجتماعي في إدارة الأمن السيبراني". كانون الثاني/يناير 2023.

[رابعا]
استعراض السياسات الوطنية لمكافحة الإرهاب

4 – 1 لمحة عامة

الغرض من إنشاء وثيقة لصياغة استجابات السياسات الوطنية لمكافحة الإرهاب للحد من استخدام التكنولوجيات الجديدة لأغراض إرهابية هو تمكين صنّاع السياسات من تطوير و/أو تحديث السياسات والاستراتيجيات لمكافحة الإرهاب بطريقة تأخذ بالحسبان تعقيدات التطورات التكنولوجية. تتيح التكنولوجيات الجديدة فرصاً عديدة كالقدرة على تحديد الأولويات والاستثمار في مجال الابتكار، وتحديث القدرات الخاصة بمكافحة الإرهاب وذلك باستخدام تكنولوجيات جديدة، فضلاً عن زيادة التعاون الشامل بين القطاعين العام والخاص. ويمكن للجهات الإرهابية الاستفادة من تلك التكنولوجيات وإساءة استخدامها بطرق مؤذية، إذ تعمل المنظمات الإرهابية على استخدامها بدمج الأنشطة التي تجري في العالم الافتراضي مع أنشطة العالم الحقيقي. وتتضمن التحديات التي تفرضها التكنولوجيات الجديدة استخدام الإنترنت ووسائل التواصل الاجتماعي وشبكة الإنترنت الخفية، بالإضافة لاستخدام وسوء استخدام الأصول الافتراضية لأغراض إرهابية (مثل عملية تبييض الأموال). ويتيح استخدام التكنولوجيات الجديدة لأغراض إرهابية إمكانية التعرض لهجمات عبر الفضاء الإلكتروني من قبل الجهات الإرهابية.

وإذ تقر هذه الوثيقة بأن التطورات الحاصلة في عالم التكنولوجيات الجديدة تحدث بوتيرة أسرع بكثير مما تستطيع السياسات الوطنية مجاراتها، فإنها تسعى لتقديم إطار لتقييم كفاءة السياسات في التصدي للتهديدات التي يفرضها استخدام التكنولوجيات الجديدة لأغراض إرهابية، وتعمل أيضاً على إدخال تعديلات على السياسات للحفاظ على استمرار مواكبتها وذلك من خلال الإطار ذاته. ويعد دور السياسات الوطنية لمكافحة الإرهاب مهماً في وضع نهج حكومي مشترك وشامل للوقوف في وجه التهديدات الإرهابية عن طريق ولاية واضحة رفيعة المستوى. كما تؤدي تلك السياسات دوراً مهماً في تنسيق الأهداف الحكومية، وتحقيق التكامل مع سياسات الأمن الوطني وأمن الفضاء الالكتروني والجرائم الإلكترونية ذات الصلة. وهنا يمكن القول إن السياسات تحتاج إلى تعريف ولاياتها المؤسساتية ومسؤولياتها التنظيمية وآليات التعاون والتنسيق بين المؤسسات، فضلاً عن تخصيص الموارد في سبيل دعم مقومات إطار القدرات الوطنية. ولا بد من التشديد على أن دورها في مكافحة الإرهاب مهم جداً للتنسيق مع أصحاب المصلحة والمؤسسات غير الحكومية، كونها تحتاج إلى الدعم والتنسيق والتواصل والتعاون مع القطاع الخاص والعامة والشركاء الدوليين.

4 – 2 التكنولوجيات الجديدة: استخدامها من قبل الإرهابيين ولغايات مكافحة الإرهاب

لنتمكن من تطوير سياسات مكافحة الإرهاب التي ترتبط بالتكنولوجيات الجديدة لا بد لنا من الإحاطة بها بالكامل بالنظر إلى استخدام التكنولوجيات الجديدة ومكافحة الإرهاب، ويتعين على العاملين في هذا المجال فهم الطرق التي يمكن أن يستخدم بها الإرهابيون تلك التكنولوجيات لأغراض إرهابية، والطرق التي يتعين عليهم إدراكها في سبيل التصدي لهذه الأغراض. يسلط الجدول المبين أدناه الضوء على التكنولوجيات الجديدة وامكانية استخدامها لأغراض إرهابية، بالإضافة إلى إمكانية استخدام العاملين في التصدي للإرهاب. من شأن فهم الطرق التي يمكن أن تستخدم بها تلك التكنولوجيات في الاستجابة للإرهاب أن تزيد من معرفة العاملين في دمج هذه الطرق كجزء من استجابات السياسات للإرهاب.

من الضروري التنويه إلى وجوب استمرار تقييم المعلومات الواردة في الجدول لضمان دقتها وصلتها بالوقائع الخاصة بأولئك الذين يعتمدون عليها في بحثهم، علماً أن محتوى الجدول يتسم بالدقة حتى تاريخ كتابة هذا التقرير. ونظراً لاستمرارية تطور هذه التكنولوجيات الجديدة، سيستمر ظهور طرق جديدة يمكن استخدام هذه التكنولوجيات من خلالها لأغراض إرهابية، وبالتالي ظهور طرق أخرى للتصدي لها.

الجدول 4 – أمثلة عن الاستخدامات الخبيثة للتكنولوجيا والفرص المتاحة لإنفاذ القانون

نوع التكنولوجيا	الاستخدام لأغراض إرهابية	استخدام إنفاذ القانون لمكافحة الإرهاب
الإنترنت	• تجنيد منظمات إرهابية عبر دعاية تنشر على الإنترنت • نشر معلومات على الإنترنت حول كيفية تنفيذ هجمات إرهابية[27] • تمويل الإرهاب • خلق النزعة الأصولية للقيام بأعمال إرهابية • جمع الاستخبارات حول الأهداف المحتملة للاعتداءات • نشر محتوى إرهابي وروايات مشوّهة • التواصل والتنسيق وغير ذلك من وسائل دعم الأعمال والأنشطة الإرهابية • العمليات المعلوماتية المدعومة سيبرانياً	• مكافحة التطرف العنيف والروايات الإرهابية[28] • تجميع وتحليل استخبارات الوسائط المفتوحة • منصات مشاركة المعلومات لصالح أصحاب المصلحة • تحديد المحتوى الإرهابي على شبكة الإنترنت وإيقاف نشره • فرق إحالة تبلّغ عن المحتوى المتطرف للشركات التقنية التي ستقوم بمعالجة ذلك المحتوى على منصتها • تحديد المجموعات الإرهابية الناشئة ومقاصدها

27 الاتحاد الأوروبي، "توجيه (الاتحاد الأوروبي) 2017/541 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 15 آذار/مارس 2017 بشأن مكافحة الإرهاب واستبدال القرار الإطاري للمجلس JHA/2002/475 وتعديل قرار المجلس JHA/2005/671" قانون رقم JHA/2002/475، Pub. L. No. 2002/475/JHA, 088 OJ L 6 (2017), 88/7–8. http://data.europa.eu/eli/dir/2017/541/oj/eng.

28 المديرية التنفيذية للجنة مكافحة الإرهاب التابعة لمجلس الأمن التابع للأمم المتحدة، "موجز تحليلي للمديرية التنفيذية للجنة مكافحة الإرهاب: مكافحة الروايات الإرهابية الافتراضية وغير الافتراضية" (الأمم المتحدة، 2020)، https://www.un.org/securitycouncil/ctc/content/cted-analytical- brief-%E2%80%93-countering-terrorist-narratives-online-and-offline.

الجدول 4 – أمثلة عن الاستخدامات الخبيثة للتكنولوجيا والفرص المتاحة لإنفاذ القانون

نوع التكنولوجيا	الاستخدام لأغراض إرهابية	استخدام إنفاذ القانون لمكافحة الإرهاب
وسائل التواصل الاجتماعي	• تجنيد منظمات إرهابية عبر دعاية تنشر على وسائل التواصل الاجتماعي • حملات تضليل إعلامي • نشر محتوى إرهابي وروايات مشوهة، ودعاية و/أو ومواد تُنشر كدعاية على وسائل التواصل عبر قنوات مشفرة[29]. (انظر قرار مجلس الأمن 2396) • خلق النزعة الأصولية للقيام بأعمال إرهابية • السماح لخدمات الرسائل المشفرة بإجراء اتصالات يصعب رصدها من قبل أشخاص ليسوا من ضمن المحادثة	• جمع/رصد استخبارات وسائل التواصل الاجتماعي • مكافحة التطرف العنيف والروايات الإرهابية • إحالة التقارير التي تبلغ عن المحتوى الإرهابي للشركات التقنية • منع إنشاء حسابات جديدة للإرهابيين
شبكة الإنترنت الخفية	• منتديات قرصنة يمكن من خلالها الحصول على البرمجيات الضارة ودفع الفدية وبرامج خبيثة أخرى لإطلاق هجمات في الفضاء الإلكتروني • حيازة الأسلحة • التجنيد • الاتصالات المشفرة بين الأعضاء	• تجميع وتحليل استخبارات الوسائط المفتوحة
الأصول الافتراضية (العملات الرقمية والرموز غير القابلة للاستبدال وأنظمة السداد عبر الهاتف الذكي وغيرها)	• استخدام العملات الرقمية/الرموز غير القابلة للاستبدال لتمويل الإرهاب • استخدام العملات الرقمية/الرموز غير القابلة للاستبدال في نشاطات تبييض الأموال	• استخدام الرموز غير القابلة للاستبدال في وظائف السرد المضاد للدعاية الإرهابية (داعش هي مثال عن مجموعة إرهابية تستخدم تلك الرموز لنشر دعايتها)[30] • يمكن أن يعزز جمع الأموال/التمويل الجماهيري في الأصول الافتراضية جهود القاعدة الشعبية في مكافحة الإرهاب (على سبيل المثال شراء تجهيزات مطلوبة محلياً)
ميزة التعرف على الوجوه	• غير معروفة حالياً – غير متاحة	• اكتشاف الشذوذ (عملية التنقيب عن البيانات لتحديد نقاط البيانات التي تقع خارج القاعدة أو التي تنحرف عنها) • قاعدة بيانات الإرهابيين العالمية

29 ميا بلوم، هشام تيفلاتي، وجون هورغان، "التنقل في منصة داعش المفضلة: تيليجرام"، الإرهاب والعنف السياسي 31، العدد. 6 (2 تشرين الثاني/نوفمبر 2019): 1242–54، https://doi.org/10.1080/09546553.2017.1339695.

30 إيان تالي، "الدولة الإسلامية تلجأ إلى الرموز غير القابلة للاستبدال لنشر رسالة إرهابية"، وول ستريت جورنال، 4 أيلول/سبتمبر 2022، القسم الثاني. السياسة، https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800.

الجدول 4 – أمثلة عن الاستخدامات الخبيثة للتكنولوجيا والفرص المتاحة لإنفاذ القانون

نوع التكنولوجيا	الاستخدام لأغراض إرهابية	استخدام إنفاذ القانون لمكافحة الإرهاب
الطباعة الثلاثية الأبعاد	• تصنيع الأسلحة أو أجزاء منها	• يمكن أيضا استخدام الطباعة الثلاثية الأبعاد لطباعة الأجزاء التي يمكن استخدامها لمكافحة الإرهاب، مثل أجزاء الطائرات بدون طيار، والتي بدورها يمكن استخدامها في الاستخبارات والمراقبة والاستطلاع
الذكاء الاصطناعي/ التعلم الآلي	• حملات التضليل والهجمات السيبرانية المدعومة بالذكاء الاصطناعي[31] • أسلحة مدعومة بالذكاء الاصطناعي[32] • حملات الهندسة الاجتماعية[33] • يمكن استخدامه لترقية عمليات الاستغلال الخبيث أو كتابة برامج ضارة للهجمات السيبرانية المتطورة	• استخدام الذكاء الاصطناعي/التعلم الآلي لأتمتة المراقبة والتحليل في CTI (على سبيل المثال، الفرز الآلي للمنشورات على وسائل التواصل الاجتماعي/المنتديات عبر الإنترنت)[34] • تحليل البيانات الضخمة المدعوم بالذكاء الاصطناعي[35] • استخدام تقنيات معالجة اللغة الطبيعية للكشف عن الرموز والأنماط التي تستخدمها الجماعات الإرهابية على الإنترنت • مراقبة المعلومات الخاطئة والمضللة[36]

4 – 3 المعيار المرجعي

تهدف هذه الوثيقة إلى الاستفادة من الممارسات الجيدة الحالية في إطار سياسات مكافحة الإرهاب للمساعدة على زيادة تطوير استخدامها واستجابتها للتكنولوجيات الجديدة الموجودة بين أيدي الإرهابيين. ولإعداد هذه الوثيقة، أجريت عدة دراسات استقصائية في القطاعين العام والخاص لوثائق متعددة تتعلق بالسياسات والاستراتيجيات المتبعة في مكافحة الإرهاب. والغرض من ذلك هو تقييم ما إذا كانت هناك ممارسات جيدة ضمن السياسات الحالية ينبغي محاكاتها في السياسات المستقبلية، والتوصل إلى فهم أفضل لحالة سياسات مكافحة الإرهاب فيما يتعلق بكيفية معالجتها للتكنولوجيات الجديدة. ومن خلال مسح وثائق مكافحة الإرهاب المتاحة للجمهور، هناك فرصة لزيادة تعزيز استجابات السياسات العامة للتصدي لاستخدام التكنولوجيات الجديدة لأغراض إرهابية.

31 مركز الأمم المتحدة لمكافحة الإرهاب ومعهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة، "الخوارزميات والإرهاب: الاستخدام الخبيث للذكاء الاصطناعي لأغراض إرهابية"، تقرير مشترك، (الأمم المتحدة، 2021)، 39–40، https://www.un.orgsites/www.un.orgfiles/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

32 انظر مثلا، المرجع نفسه، 33–35.

33 المرجع نفسه، 45.

34 مركز الأمم المتحدة لمكافحة الإرهاب ومعهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة، "مكافحة الإرهاب عبر الإنترنت بالذكاء الاصطناعي: نظرة عامة على وكالات إنفاذ القانون ومكافحة الإرهاب في جنوب آسيا وجنوب شرق آسيا"، تقرير مشترك (الأمم المتحدة، 2021)، 20–21 و23–30، https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence.

35 المرجع نفسه، 17.

36 مركز الأمم المتحدة لمكافحة الإرهاب ومعهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة، "مكافحة الإرهاب عبر الإنترنت بالذكاء الاصطناعي: نظرة عامة على وكالات إنفاذ القانون ومكافحة الإرهاب في جنوب آسيا وجنوب شرق آسيا"، 27–28.

4 – 4 نتائج عامة

كثيراً ما تطرقت العديد من استراتيجيات مكافحة الإرهاب التي جرى استقصاؤها من أجل إنشاء هذه الوثيقة، أثناء مناقشة التكنولوجيات الجديدة إلى مسائل عدة مثل استخدام شبكة الإنترنت ووسائل التواصل الاجتماعي لأغراض إرهابية. وفي حين أن هذا هو الحال، لم تتطرق الكثير من تلك الاستراتيجيات إلى العوامل التكنولوجية التمكينية المستخدمة أو محتملة الاستخدام من قبل الإرهابيين لأنواع جديدة من العمليات، مثل استخدام الذكاء الاصطناعي وشبكة الإنترنت الخفية والتطبيقات المشفرة السرية والأصول الرقمية. يمكن أن يعزى ذلك إلى حقيقة مفادها أن العديد من تلك الاستراتيجيات لم يجرِ تحديثها بوتيرة سريعة لمواكبة التطورات واحتمال زيادة استخدام تلك التكنولوجيات.

وكان من الواضح عند استقصاء استراتيجيات وسياسات مكافحة الإرهاب نشرت في بلدان مختلفة أنها اعترفت بالعصر الرقمي والتعقيدات التي رافقته. ومن ناحية أخرى، لا تقدم العديد من الوثائق الاستراتيجية أي إطار عمل واضح وتفصيلي ليصار إلى اعتماده في التعامل مع التهديدات التي فرضتها التكنولوجيات الجديدة الموجودة بين أيدي الجهات الإرهابية، ولا تتطرق حتى لإمكانية تقديم تلك التكنولوجيات المساعدة لوكالات إنفاذ القانون وأصحاب المصلحة الآخرين في التصدي للإرهاب. ومع أن هذه الوثائق الاستراتيجية تبحث في أهمية مشاركة المعلومات، إلا أن ثمة ثغرات توجد في هذه الوثائق بخصوص أفضل الممارسات في عملية التشارك المعلوماتي كأن تكون، على سبيل المثال، فعّالة وآمنة (من منظور الأمن المعلوماتي/العملياتي) وقانونية (ضمن سياق مشاركة البيانات).

4 - 4 - 1 قضايا أساسية تنبغي معالجتها

عند وضع استراتيجية شاملة لمكافحة الإرهاب وسياسة تتصدى لاستخدام التكنولوجيات الجديدة لأغراض إرهابية، ينبغي معالجة عدد من القضايا الأساسية لضمان جهوزية البلدان بشكل كاف لمواجهة التهديدات الحالية والمستقبلية.

تتسم القدرة على التقييم والاستجابة للتهديدات ضمن سياسة مكافحة الإرهاب بأهمية عالية، إذ يشمل ذلك فهم القدرات التكنولوجية الانكشاف التكنولوجي في الأنشطة الاقتصادية والاجتماعية التي يمكن استغلالها، والدوافع الإرهابية. وكجزء من عملية التقييم هذه، لابد من تشديد التركيز على عملية جمع الاستخبارات المتعلقة بالتهديدات (على سبيل المثال عبر وسائل مثل استخبارات الاشارات واستخبارات المصادر المفتوحة واستخبارات وسائل التواصل الاجتماعي) لتمكين العاملين من الاستجابة لتلك التهديدات بصورة استباقية وفعالة.

وهنا، تتمثل إحدى القضايا الرئيسية التي ينبغي معالجتها في التعاون الشامل لعدة قطاعات (مع التركيز على مشاركة المعلومات) فيما بين أصحاب المصلحة، بما في ذلك التشارك مع أصحاب المصلحة الوطنيين وشبه الوطنيين والمحليين. ويعد التعاون عبر القطاعات بين وكالات القطاع العام المعنية بإنفاذ القانون والقطاع الخاص، والأوساط الأكاديمية، والمنظمات غير الربحية أمراً بالغ الأهمية في العصر الرقمي وعصر التكنولوجيات الجديدة، لا سيما في وقت تتطور فيه التكنولوجيات باستمرار. ومع أن استراتيجيات مكافحة الإرهاب التي شملتها الدراسة الاستقصائية لهذا التقرير تتضمن عنصر مشاركة المعلومات، إلا أنها لا تتناول كيفية المشاركة.

ومن القضايا الأساسية الأخرى التي تتناولها هذه الوثيقة كيفية تحسين تدريب أصحاب المصلحة على استخدام التكنولوجيات الجديدة للاستجابة للتهديدات الإرهابية. فقدرة أصحاب المصلحة هؤلاء على مواكبة التحديات واغتنام الفرص التي تطرحها تلك التكنولوجيات ستمكنهم من الاستجابة بصورة أفضل لمشهد التهديدات المتطور والمتغير باستمرار بصورة فعّالة.

4 - 4 - 2 صياغة ممارسات وأدوات وطرق جديدة

تُعد صياغة ممارسات وأدوات وأساليب متطورة للتصدي لاستخدام التكنولوجيا الجديدة لأغراض إرهابية مثل الحصول على المعلومات والرصد وفرض استخدام وسائل التواصل الاجتماعي، وإحباط التحريض الذي يؤدي إلى الإرهاب، والمشاركة في الجهود الاستباقية لإحباط الهجمات المحتملة أحد أهم التحديات التي تواجه دوائر إنفاذ القانون. وهذا يتطلب إثراء مجموعة أدوات وكالة إنفاذ القانون للتمكين من فهم وإدارة وتنفيذ أنشطتها في السياق التكنولوجي. وتفتقر العديد من البلدان إلى توجيهات واضحة بشأن كيفية التصرف ضد الأنشطة الإرهابية على الإنترنت، في الوقت الذي ما تزال فيه هناك حاجة إلى تنفيذ آليات قضائية وإنفاذية هامة، بما في ذلك صياغة تشريعات وقوانين إنفاذ لمكافحة التطرف والتحريض عبر الإنترنت.

ويجب أن يجري كل ذلك بطريقة تحمي حقوق الخصوصية، وحرية التعبير والتجمعات، والحق في عدم التمييز، والحقوق الأساسية الأخرى، أو إذا لزم الأمر، تقييد هذه الحقوق بما يتفق تماما مع مبدأي الشرعية والتناسب.

[خامساً]
اعتبارات استجابة السياسات الوطنية لمكافحة الإرهاب

5 – 1 لمحة عامة

يهدف هذا الفصل إلى معالجة الثغرات التي تعاني منها استراتيجيات مكافحة الإرهاب فيما يتعلق بالتكنولوجيات الجديدة، وتقديم أمثلة عن الممارسات الجيدة في سياسات مكافحة الإرهاب بهدف رسم سياسات وبروتوكولات تتصدى للتهديدات التي تطرحها التكنولوجيات الجديدة. وتسلط الأهداف الأخرى الضوء على استخدام التكنولوجيات الجديدة في التصدي للإرهاب وتحسين الاستجابات الأمنية والإجراءات المضادة في سياق مكافحة الإرهاب. تستند اعتبارات استجابة السياسات الوطنية لمكافحة الإرهاب إلى نهج متعدد الأوجه يحيط بالأبعاد الرئيسية لسياسات مكافحة الإرهاب، بهدف ضمان فعالية الأمن الوطني المترافقة مع الرقابة المطلوبة لحماية حقوق الأفراد وحرياتهم.

تتطلب اعتبارات استجابة السياسات الوطنية لمكافحة الإرهاب تضافر جهود الهيئات الحكومية ووكالات إنفاذ القانون والجيش أصحاب المصلحة الآخرين لضمان أمن وأمان المواطنين على التوازي مع حماية الحقوق والحريات الفردية.

حقوق الإنسان التي يحيق بها خطر داهم في ظل مكافحة الإرهاب والتكنولوجيات الجديدة هي الخصوصية وحرية التعبير وخطر التمييز، ولكن قد لا يمكن فرض قيود على الحد من التمييز، وهو ما يعد بالفعل سبباً جذرياً وحاسماً للإرهاب. يجب أن يؤسس القانون للقيود المفروضة على حقوق الخصوصية وحرية التعبير أو يجب أن تتماشى هذه القيود مع القانون، وبالتوافق مع المادتين 17 و 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية. إضافة إلى ذلك، يجب أن يكون وجود أية قيود أمراً ضرورياً ويتناسب مع الهدف الشرعي المراد تحقيقه.

يقدم الجدول البياني (الشكل 4) النموذج الذي تستند إليه اعتبارات استجابات السياسات الوطنية لمكافحة الإرهاب. تظهر الصفوف العليا من الجدول الرقابة وقياس التأثير والفعالية، وتسلط الضوء على الاعتبارات الشاملة التي ينبغي دمجها في كليّة استجابات سياسات مكافحة الإرهاب، وكل من العناصر التي تؤلف هذه الاستجابات. يتبع هذين الاعتبارين الشاملين أربعة اعتبارات متكاملة وهي: الوعي والتدخل في حال التهديد والقدرات الوطنية والتعاون. وكل من هذه الاعتبارات المتكاملة تشكل المبدأ التوجيهي للمكونات الشاملة لاستجابة السياسات الوطنية لمكافحة الإرهاب الواردة أدناه، بما في ذلك مشاركة المعلومات، والابتكار، وإدارة البيانات، والإطار القانوني، والتدريب والإعداد. ومن خلال مزج هذه المكونات الأساسية يمكن تحقيق الأهداف المذكورة في الاعتبارات الأربعة الشاملة.

الشكل 4

5 - 1 - 1 الرقابة

عند صياغة استجابات سياسات مكافحة الإرهاب من الأهمية بمكان التفكير في الرقابة على السياسات لضمان أن تكون جميع الأمور المتعلقة بدعم البيانات والخصوصية وحقوق الإنسان موجودة طوال فترة تنفيذ سياسة مكافحة الإرهاب. يجب أن تتألف إجراءات الرقابة من خطوات متعددة ضمن استجابات السياسات لمكافحة الإرهاب بما يضمن تحقيق هذه الاعتبارات خلال العملية، وخاصة أثناء فترة جمع المعلومات الاستخباراتية ومكونات إدارة البيانات.

هناك نوعان من الإشراف يوصى بتنفيذهما ضمن سياسات مكافحة الإرهاب وهما: الرقابة القضائية وغير القضائية[37]. تشرك الرقابة القضائية المحاكم في عملية الرقابة ومساءلة أصحاب المصلحة على الأفعال التي يقومون بها كجزء من عملية جمع المعلومات الاستخباراتية وكاستجابة لهذه المعلومات التي حُصِّلت[38]. أما الرقابة غير القضائية فيمكن للجان البرلمانية أن تقوم بمهمة تنفيذها، ووكالات حماية البيانات وإنفاذ القانون المحلي وهيئات الرقابة على الاستخبارات بمهمة الإشراف عليها[39]. إضافة إلى ذلك، تلعب المنظمات الدولية ومنظمات المجتمع الأهلي دوراً في مراقبة مدى امتثال استجابات الحكومات للالتزامات القانونية الدولية. وفي كلتا الحالتين، يتعين على الهيئة التي تقوم بالرقابة أن تكون مستقلة عن صنّاع السياسات[40].

ينبغي أن يتضمن التعاون مع القطاع الخاص، ولا سيما فيما يتعلق بجمع البيانات والمعلومات الاستخباراتية، درجة من الشفافية مع العامة في مجال جهود المراقبة الشبكية، وذلك كجزء من جهود الرقابة ككل[41].

37 مكتب الأمم المتحدة المعني بالمخدرات والجريمة، "وحدة مكافحة الإرهاب 12 القضايا الرئيسية: المساءلة والإشراف على أساليب جمع المعلومات الاستخبارية"، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، تموز/يوليه 2018، https://www.unodc.org/e4j/en/error/module-12/key-issues/accountability-oversight-of-intelligence-gathering-methods.html.

38 مكتب الأمم المتحدة المعني بالمخدرات والجريمة.

39 المرجع نفسه.

40 المرجع نفسه.

41 حكومة أستراليا، حماية مجتمعنا معاً: استراتيجية أستراليا لمكافحة الإرهاب 2022 (أستراليا: كومنولث أستراليا، 2022)، 29، https://www.nationalsecurity.gov.au/what-australia-is-doing-subsite/Files/safeguarding-community-together-ct-strategy-22.pdf.

5 - 1 - 2 قياس التأثير والفعالية

يحتّم استمرار التطور في مجال التكنولوجيا تطور سياسة مكافحة الإرهاب للاستجابة بأفضل صورة لمشهد التهديد الحالي. وبهذا النحو، ينبغي بناء إطار لسياسة مكافحة الإرهاب لتقييم كفاءة وتأثير سياسات مكافحة الإرهاب والإجراءات ذات الصلة في القدرة على التخفيف والاستجابة للتهديدات الإرهابية. وتتمثل إحدى الطرق في استراتيجية الولايات المتحدة لمكافحة الإرهاب بإجراء تحليلات سنوية بخصوص كل من فعالية الاستراتيجية في تحقيق أهداف مكافحة الإرهاب وإحراز تقدم في تناول هذه الأهداف بما أن ذلك يرتبط بالتهديدات الجديدة والحالية[42].

توصى الدول الأعضاء أن تقوم بتحديد أهدافها المرجوة ونتائجها الاستراتيجية قبل تقييم تأثير وكفاءة استجابات مكافحة الإرهاب[43]. ويتمثل أحد أكثر العوامل أهمية في تقييم التهديدات والاستجابات في مدى تلبية استجابة السياسات أو عدم تلبيتها للأهداف المنشودة فيما يخص الإجراءات أو السياسات. يتعين على الدول الأعضاء أن تنظر في القياسات الكمية والنوعية في تقييم تأثير وكفاءة خيارات السياسات في التصدي للتهديدات الإرهابية.

توجد اعتبارات أخرى يتعين على صنّاع السياسة بتقييمها عند النظر في التأثير والفعالية. وأحد هذه الاعتبارات هو التقييد المفروض على السياسات ذات الصلة بالتطورات التكنولوجية وغير التكنولوجية بدءاً من التقييم الأخير لهذه السياسات. وينبغي معالجة تكلفة تنفيذها (من خلال القوة العاملة وموارد أخرى مثلاً) وخاصة فيما يتعلق بالفائدة منها والأمور الأخرى التي تقدمها عندما يجري تقييم تأثيراتها وفعاليتها[44].

عند تقييم تأثير وفعالية سياسات مكافحة الإرهاب يوصى باستخدام عملية الممارسة القائمة على الأدلة لتقديم قياسات محددة لتأثير السياسات ومستوى فعاليتها من خلال العوامل المختلفة بما يمكّن من اتخاذ قرارات مستقبلية بشأن السياسات[45]. هناك عاملان ينبغي النظر فيهما عند تصميم تقييم الممارسة القائمة على الأدلة: أهداف السياسات (والوسائل الخاصة التي تمكّن من قياس كيفية الحصول على تلك السياسات أو الفشل في الحصول على هدف معين) والآثار المحتملة لها (والفترات التي تقدم من خلالها هذه الآثار نفسها)[46]. ولتقييم هذه العوامل والسياسات ككل، يجب دراسة طرق البحث التقييمية التي يجري من خلالها تقييم الموارد والعمليات والنتائج المتأتية من السياسات في ضوء العوامل السابقة[47]. ومن خلال هذه التقييمات يمكن لصنّاع السياسة معرفة كيفية ومكان تطبيق التعديلات على استجابات سياسات مكافحة الإرهاب للوصول إلى ارتباط وكفاءة أكبر.

42 الولايات المتحدة، الاستراتيجية الوطنية لمكافحة الإرهاب في الولايات المتحدة الأمريكية (واشنطن العاصمة: البيت الأبيض، 2018)، 11، https://purl.fdlp.gov/GPO/gpo109871.

43 وزارة الأعمال التجارية والطاقة والاستراتيجية الصناعية في المملكة المتحدة، "مشروع قانون الأمن القومي والاستثمار"، منشور رقم 7 ،(2020) BEIS006(F)-20-CCP https://assets.publishing.service.gov.uk/Government/uploads/system/uploads/attachment_data/file/934276/nsi-impact-assessment-beis.pdf.

44 وزارة شؤون الأعمال في المملكة المتحدة والطاقة والاستراتيجية الصناعية، 30.

45 فريز Freese، "مكافحة الإرهاب القائمة على الأدلة أم التغاضي عن الرؤية؟ كيف نفهم ونحقق ما ينجح، 37-38.

46 المرجع نفسه، 41.

47 المرجع نفسه، 45-46.

5 – 2 الاعتبارات الجوهرية لاستجابات سياسات مكافحة الإرهاب بخصوص التكنولوجيات الجديدة

تحيط الاعتبارات الجوهرية التالية بالعوامل المهمة الضرورية لتطوير استجابات سياسات مكافحة الإرهاب الشاملة. وبالتركيز على هذه الاعتبارات الجوهرية يمكن لصنّاع السياسة في مجال مكافحة الإرهاب أن يطوروا سياسات تخلق توازناً بين الحاجة إلى التصدي للضرورات الأمنية وحماية الحقوق الفردية، في الوقت الذي يجري فيه التصدي لاستخدام التكنولوجيات الجديدة لأغراض إرهابية. يستكشف هذا القسم الاعتبارات الجوهرية التي ينبغي النظر فيها عند صياغة استجابات سياسات مكافحة الإرهاب في معرض التحديات التي تطرحها التكنولوجيات الجديدة. وبفهم وتناول هذه الاعتبارات الجوهرية يستطيع صنّاع السياسة تطوير سياسات متينة وقابلة للتكيف وتستطيع أن تتواكب مع استغلال الإرهابيين للتكنولوجيات الجديدة، بما يضمن أمن وأمان المجتمعات في العصر الرقمي.

5 – 2 – 1 الوعي

ينبغي تطبيق الوعي في سياسات مكافحة الإرهاب على مستوى أصحاب المصلحة ومن خلال أفراد العامة، إذ يتعين على العاملين مثلاً أن يتمتعوا بالفهم العميق ليس فقط لكيفية تحديد التهديدات والسلوكيات المهدِّدة والاستجابة لها فقط، وإنما تثقيف العامة أيضاً والاستجابة لمخاوفهم بشأن التهديدات[48]. وإذا ما نظرنا إلى ارتباط الوعي بسياسات مكافحة الإرهاب على وجه الخصوص، نجد أن يشتمل على تدريب العاملين وأفراد العامة ليكونوا قادرين على تحديد النشاط الإرهابي الذي يتأتى من أنواع التكنولوجيات الجديدة والطرق التي يستطيع العاملون من خلالها استخدام التكنولوجيات الجديدة للاستجابة للإرهاب بصورة فاعلة.

يتمثل جزء من الوعي المتزايد في مجال الاستجابات والسياسات الخاصة بمكافحة الإرهاب بتقديم المعلومات بشكل أسهل، وخاصة لأفراد العامة الذي قد يرغبون بالإبلاغ عن معلومات حساسة معينة بخصوص التهديدات[49]. وعلى هذا النحو، يحتاج العامة لمعرفة السلوكيات أو الأفعال التي تنطوي على تهديد والقنوات التي يمكنهم اللجوء إليها للإبلاغ عن حوادث يتعين على العاملين أو أي أصحاب مصلحة آخرين ذوي صلة جرى تدريبهم أن يتعاملوا معها. يمكن تحقيق ذلك من خلال التدريب على تحديد إشارات تدل على السلوك التهديدي أو سلوكيات تذكّر بالتحريض على القيام بأعمال إرهابية. يجب توخي الحذر عند إجراء التدريبات على هذه الأمور للتأكد من عدم سماح تحديد السلوكيات التهديدية بالتمييز بين الأفراد على أساس النوع الاجتماعي أو العرق أو اللون أو اللغة أو الدين أو الرأي السياسي وغير ذلك من الآراء أو الأصول الاجتماعية أو الوطنية أو حالات أخرى. إضافة إلى ذلك، يجب أن تكون المنصة التي يتمكن العامة من خلالها من مشاركة المعلومات الخاصة بالتهديدات مع السلطات المسؤولة سهلة الوصول والاستخدام منعاً لمشكلة عدم الإبلاغ بسبب صعوبتها.

يتعين على وكالات إنفاذ القانون وأصحاب المصلحة الآخرين، إضافة إلى الوعي العام، أن تكون مدرّبة على تحديد السلوك التهديدي أو السلوكيات التي تحرض على القيام بأعمال إرهابية. وعلاوة على ذلك، عليهم أن يتلقوا التدريبات على كيفية الاستجابة بالشكل الصحيح للتقارير التي يتلقونها (من العامة على سبيل المثال) أو من جمع المعلومات الاستخباراتية التي تتعلق بالسلوك التهديدي أو السلوكيات التي تذكّر بالتحريض على الأعمال الإرهابية. ويجب التشديد خلال هذه التدريبات على أن جمع المعلومات الاستخباراتية وخطة الاستجابة للكشف عن التهديدات يجب أن تجري دون تمييز بين الأفراد على أساس النوع الاجتماعي أو العرق أو اللون أو اللغة أو الدين أو الآراء السياسية وغيرها أو الأصول الاجتماعية أو الوطنية أو حالات أخرى.

48 الفريق المشترك لتقييم مكافحة الإرهاب، "دليل مكافحة الإرهاب لموظفي السلامة العامة"، مدير الحكومة للاستخبارات الوطنية، متاح بدءاً من 10 نيسان/أبريل 2023، https://www.dni.gov/nctc/jcat/index.html.

49 كارل أمريت، وإليوت برادشو، وأليسا شولينبرج، "تقييم التهديدات وإدارتها: الممارسات في جميع أنحاء العالم"، الاستعداد المحلي، 1 شباط/فبراير 2023، https://www.domesticpreparedness.com/preparedness/threat-assessment-and-managementpractices-across-the-world.

5 – 2 – 2 التدخلات لمواجهة التهديد

يشير مفهوم "التدخلات لمواجهة التهديد" إلى الممارسات والإجراءات المتخذة لمنع التهديدات الإرهابية والكشف عنها والاستجابة لها من خلال استخدام التكنولوجيات الجديدة. وتتضمن هذه التدخلات استخدام التكنولوجيات والأدوات والاستراتيجيات المتقدمة لتحديد وتتبع وتحييد التهديدات المحتملة. فقد تتضمن التدخلات، على سبيل المثال، استخدام الذكاء الاصطناعي والتعلم الآلي وتحليلات البيانات الضخمة بهدف تحليل وتفسير أحجام هائلة من البيانات وتحديد الأنماط والاتجاهات التي قد تشير إلى التهديدات المحتملة. تلعب التدخلات في حال التهديد دوراً حاسماً في مكافحة الإرهاب وتتطلب استخدام تكنولوجيات وأدوات متطورة. ومن الضروري أن تُنفذ بصورة تحترم حقوق الأفراد وحرياتهم وتتماشى مع المعايير القانونية والأخلاقية فيما يتعلق على الأقل بالحظر المطلق للتمييز على أساس النوع أو العرق أو اللون أو اللغة أو الدين أو الرأي السياسي أو أي نوع آخر من الآراء أو الأصول الوطنية أو الاجتماعية أو حالات أخرى.

ترتبط قدرة أية دولة على إجراء تقييم فعال للتهديدات والاستجابة لها بشكل وثيق بقدرتها على تنفيذ سياسات مكافحة الإرهاب ضد تلك التهديدات. ويتعين على العاملين وأصحاب المصلحة الآخرين ذوي الصلة أن يكونوا قادرين على القيام بالتدخلات لمواجهة التهديد ضمن إطار الاستجابة للتهديدات وذلك منعاً لها من أن تؤتي ثمارها.

هناك وسائل متعددة يستطلع أصحاب المصلحة من خلالها المشاركة في عمليات التدخل في حال التهديد من خلال القطاعات المختلفة. ففي الشراكة بين القطاعين والخاص مثلاً يمكن تحقيق هذا التدخل من خلال عمل القطاع العام جنباً إلى جنب مع شركات التكنولوجيا لمنع وتعطيل الاستخدام الإرهابي لمنصات الشبكة. ويمكن تحقيق التدخل في مواجهة التهديدات ضمن القطاع العام من خلال التعاون بين الدول الأعضاء ووكالات إنفاذ القانون لرصد الاستخدام الإرهابي للمنصات الرقمية والتصدي له.

تتمثل إحدى طرق تنفيذ التدخلات لمواجهة التهديد ضمن استراتيجية الدول الأعضاء لمكافحة الإرهاب في تنفيذ استجابة استباقية تتصدى للتهديدات قبل أن تصبح حقيقة واقعة. يمكن تحقيق ذلك من خلال عدة إجراءات وقائية. وهذه الأخيرة قد تشتمل على إجراءات أمنية يجري إدخالها في السياسات نفسها (السلامة الافتراضية والسلامة بالتصميم) أو وسائل تقوم بالتصدي للاعبين الإرهابيين قبل أن شن أي هجوم من خلال أي إجراء كبرامج نزع التطرف، وسنتطرق إلى كل منها بعد قليل[50].

5 – 2 – 3 القدرات الوطنية

تصف القدرات الوطنية الطريقة التي تقيس قدرات بلد ما في مجال الجهود المبذولة في مكافحة الإرهاب بالنظر إلى الموارد التي يملكها الكيان (مادية، تكنولوجية، بشرية، وغيرها). وعند تصميم استجابة سياسات مكافحة الإرهاب يجب أن تقيّم القدرات الوطنية بما يجعل السياسات متوافقة مع الدولة المحددة. ولأن كل دولة تمتلك موارد ومهارات بمستويات مختلفة لن يكون هناك اتباع لنمط سياساتي ضخم وذي جدوى وفعالية مع جميع الدول الأعضاء، فبهذا النحو يكون تقييم القدرات الوطنية جزءاً من تصميم استجابة سياسات مكافحة الإرهاب التي تتوافق وبشكل مباشر مع حاجات الدول الأعضاء التي وضعت من أجلها.

يأخذ تقييم القدرات الوطنية لدولة ما في الحسبان كلاً من الموارد الحالية والموارد المتاحة التي تكتسب من خلال وسائل كالتعاون مع القطاعات الأخرى و/أو الدول الأعضاء. ومع زيادة التقدم التكنولوجي تزداد أهمية حفاظ الدول الأعضاء على قدراتها وتطويرها لكي تكون دائماً في جهوزية كافية لمواجهة التحديات الجديدة واستخدام التكنولوجيات الجديدة في إيجاد فرص جديدة لمكافحة الأعمال الإرهابية. وكما سنذكر لاحقاً، ثمة وسائل يمكن من خلالها زيادة القدرات الوطنية للدول الأعضاء وذلك بالتدريب وإعداد العاملين والجهات المعنية ذات الصلة ومن خلال وسائل أخرى كمشاركة المعلومات والابتكار.

50 وكالة أمن الفضاء الإلكتروني وأمن البنية التحتية وآخرون، "تحويل توازن مخاطر أمن الفضاء الإلكتروني: مبادئ وأساليب للأمن بالتصميم والأمن الافتراضي"؛ فيدينو وبينيت Vidino and Bennett، "مراجعة لأفضل الممارسات عبر الأطلسي لمكافحة التطرف في السجون والعودة الإرهابية".

5 – 2 – 4 التعاون

التعاون أمر مهم في إنشاء نهج عام وحكومي شامل في مواجهة التهديدات الإرهابية بتفويض واضح وعالي المستوى، ولأهداف التنسيق الحكومية والتكامل مع أصحاب المصلحة الآخرين ذوي الصلة. تحتاج السياسات إلى تحديد آلية التعاون مع المؤسسات، كما أن السياسات الوطنية لمكافحة الإرهاب ضرورية في مجال التعاون مع المنظمات وأصحاب المصلحة غير الحكوميين. ويتعين على هذه السياسات أن تدعم التعاون والتواصل والتنسيق مع القطاع الخاص والعامة والشركاء الدوليين.

لا بد من أن تركز سياسات مكافحة الإرهاب على التعاون بين أصحاب المصلحة بما أن التكنولوجيا تمكّن التهديدات الإرهابية على نحو متزايد من الانتشار عبر الحدود وفي المجالات المختلفة (العمل الرقمي في مقابل الضرر الجسدي). يتضمن هذا التنسيق ما بين الوكالات ضمن الدول الأعضاء، وبين الدول الأعضاء، وكذلك الشراكات بين المنظمات غير الحكومية والمجتمع المدني، وبين تطور تكتيكات مشاركة المعلومات. وهنا لا بد أن يشتمل التعاون على التعاون ما بين القطاعات في القطاع العام، وعناصر القطاع الخاص كشركات التكنولوجيا، والتشاور مع الخبراء من العالم المهني والوسط الأكاديمي.

يتطلب التهديد باستخدام التكنولوجيات الجديدة لأغراض إرهابية جهوداً شاملة ومتضافرة بين أصحاب المصلحة ذوي الصلة. ويتعين على الدول الأعضاء الانخراط مع العامة لتعزيز التعليم ونشر الوعي. ويعتبر الانخراط مع المجتمعات أمراً مهماً في بناء الثقة. أما الممارسات الجيدة فهي تشير إلى حاجة الكيانات الحكومية التي تعمل مع مختلف الجهات (بما فيها الشركات وقادة المجتمع والمدارس والمؤسسات الدينية، وغيرها) أن تحدد نقاط الضعف وتتصدى لها. ويمكن لاستخدام اللغة المشتركة أن يساهم في تخفيف المخاوف والانحيازات إلى الحد الأدنى، فضلاً على قدرتها على تعليم العامة أفضل الطرق للاستفادة من خدماتها في تعزيز العلاقات المبنية على الشفافية والإشراف.

5 – 3 المكونات الرئيسية الشاملة لسياسات مكافحة الإرهاب في التصدي للتكنولوجيات الجديدة

ينبغي دمج المكونات الأساسية الشاملة في إطار سياسة مكافحة الإرهاب عند التصدي للتحديات التي تطرحها التكنولوجيات الجديدة. تغطي هذه المكونات مشاركة المعلومات والابتكار وإدارة البيانات واستخدام الأطر القانونية وبناء القدرات. وتشير الطبيعة الشاملة لهذه المكونات إلى الطرق التي تعزز فيها كل من هذه المكونات قدرة السياسات على تحقيق الأهداف المحددة في الاعتبارات الجوهرية الأربعة. وبالاعتراف بهذه المكونات الأساسية ودمجها يمكن لسياسات مكافحة الإرهاب أن تتصدى بفعالية للتهديدات والمخاطر الاستثنائية المرتبطة باستخدام التكنولوجيات الجديدة لأغراض إرهابية.

5 – 3 – 1 مشاركة المعلومات

تتمثل إحدى الممارسات الأساسية التي ينبغي التركيز عليها كجزء من سياسات مكافحة الإرهاب ضمن مجال التعاون بمشاركة المعلومات التي تشير إلى الاستخبارات وجمع المعلومات من مصادر مفتوحة والتحليل ونشر المعلومات مع أصحاب المصلحة، بما فيها إنفاذ القانون والهيئات الحكومية. وقد يشتمل ذلك على مشاركة المعلومات والتشاور مع أفراد من الوسط الأكاديمي، والقطاع الخاص والمنظمات غير الحكومية كجزء من التعاون بين القطاعات.

وقد تظهر بعض التحديات الأساسية عند صياغة استجابات سياسة مكافحة الإرهاب وبالتحديد عند مناقشة مسألة مشاركة المعلومات. تتمثل أولى هذه التحديات بالسهولة والفعالية التي يجري مشاركة المعلومات من خلالها. ولضمان مشاركة المعلومات بين أصحاب المصلحة بصورة فعالية ينبغي وجود مصطلحات مشتركة بين أصحاب المصلحة تتعلق بكيفية تقييم التهديدات الإرهابية وكيفية الاستجابة لها. ويجب ان تشمل لغة الاستجابة المشتركة أنواع المسؤوليات المخصصة لمختلف أصحاب المصلحة.

أما المكون الثاني الأساسي في تطوير ممارسات مشاركة المعلومات فيتمثل بتحديد الوسائل التي يمكن مشاركة المعلومات من خلالها، إذ يجب أن تجري عملية مشاركة المعلومات بين أصحاب المصلحة في المواقع المختلفة عبر وسيلة آمنة لتمكين هؤلاء من الحفاظ على الأمن التشغيلي في تقييم والاستجابة للتهديدات. وإضافة إلى المشاركة المعلوماتي بين أصحاب المصلحة والعاملين من الضروري توفير طريقة سهلة وتتمكن العامة من خلالها التواصل مع هيئات إنفاذ القانون ذات الصلة. أحد الأمثلة عن ذلك هو منصة يقدم الجمهور عبرها تقييمهم لخطورة المعلومات الخاصة بالتهديدات ويتشاركونها مع السلطات ذات الصلة[51].

5 – 3 – 2 الابتكار

يستكشف الإرهابيون بشكل مستمر طرقاً جديدة لاستغلال التكنولوجيا لتحقيق أهدافهم. ونتيجة لذلك، يجب أن تتطور سياسات وإجراءات واستراتيجيات مكافحة الإرهاب أيضاً لمواكبة هذه التهديدات. وهذا يتطلب الابتكار في مجال التكنولوجيا والسياسات. هناك أنواع متعددة للابتكار وذات صلة بسياسات مكافحة الإرهاب، بما فيها الابتكار التشغيلي والابتكار التكنولوجي، الذي يكون الهدف منه تعزيز جمع المعلومات وقدرات إنفاذ القانون لضمان الاستجابة السريعة والفعالة للإرهاب[52].

تصوغ الابتكارات التكنولوجية كلاً من التهديدات المحتملة والطرق الجديدة لمكافحة تلك التهديدات. وينبغي تقييم الطريقة التي تواكب (أو تفشل) فيها السياسات النمو وذلك كجزء من تقييم كفاءة سياسات مكافحة الإرهاب (كما ذكرنا في القسم 5 – 1 – 2). يجب أن تعترف أي سياسة لمكافحة الإرهاب بالابتكارات التكنولوجية الموجودة حتى تاريخ نشرها كما يجب أن تحاول التنبؤ بالابتكارات المستقبلية المحتملة التي تتطلب استجابة ما[53]. يصف الابتكار التشغيلي كيفية تعديل أصحاب المصلحة لنهجهم في تقييم التهديدات وتكتيكات الاستجابة بطريقة يستفيدون فيها من الابتكار التكنولوجي والابتكار الاستراتيجي/التكتيكي/المنهجي بشكل أكثر عمومية[54]. غالباً ما يتطلب الابتكار تعاوناً بين الهيئات الحكومية والشركات الخاصة والمؤسسات الأكاديمية. ويجب أن تنظر استجابة سياسات الدول الأعضاء في دفع الابتكار وتمكينه، وهو ما يتطلب موارد استثمارية ودعماً لتطوير وتنفيذ التكنولوجيات الابتكارية. وينبغي أن تكون الحكومات والمنظمات الخاصة راغبة بالاستثمار في البحث والتطوير، وبتقديم الدعم لتنفيذ الإجراءات الجديدة. وفضلاً على ذلك، تحتاج السياسات مع إيقاع التغيير السريع إلى بناء أطر خاصة بالسياسة تكون قادرة على التكيف مع التهديدات المتغيرة. ويشتمل هذا على "مسح أفقي" عبر حكومي[55]، على مستوى السياسة وإدارة الابتكار على المستوى المؤسسي.

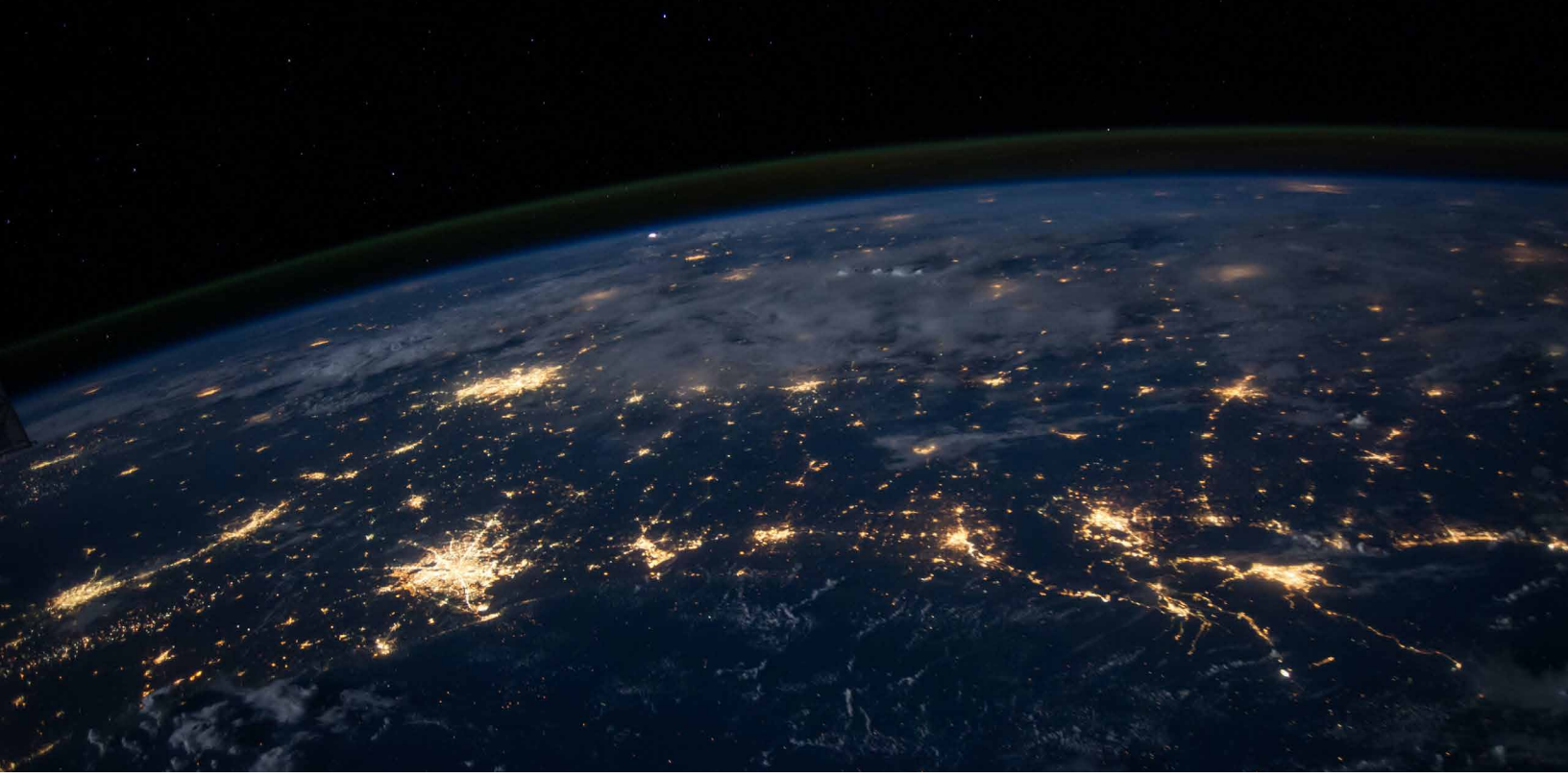
51 كيف يمكنك المساعدة: نموذج المساهمة العامة، دائرة الاستخبارات الأمنية النيوزيلندية، وأصبح متاحاً في 23 نيسان/أبريل 2023، https://providinginformation.nzsis.govt.nz/.

52 روبرت جي. سبولاك، "العلوم والتكنولوجيا والابتكار في مكافحة الإرهاب." شباط/فبراير 2015، https://www.osti.gov/biblio/1513954.

53 انظر على سبيل المثال، المملكة المتحدة، المسابقة: استراتيجية المملكة المتحدة لمكافحة الإرهاب (المملكة المتحدة: 2018، The Crown)، 24، https://assets.publishing.service.gov.uk/Government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf.

54 سبولاك، "العلم والتكنولوجيا والابتكار في مكافحة الإرهاب".

55 عرّفت مراجعة جون داي المسح الأفقي بأنه: فحص منهجي للمعلومات لتحديد التهديدات المحتملة والمخاطر والقضايا الناشئة والفرص، بما يتجاوز الفترة البرلمانية، ما يسمح باستعداد أفضل ودمج التخفيف والاستغلال في عملية صنع السياسات.



5 - 3 - 3 إدارة البيانات

يشير مصطلح "إدارة البيانات" في سياق مكافحة الإرهاب والتكنولوجيات الجديدة إلى العمليات والأنظمة المستخدمة في جمع وتحليل وتخزين ومشاركة المعلومات المرتبطة بالتهديدات الإرهابية. وقد أصبحت إدارة البيانات أحد المكونات الأساسية لجهود مكافحة الإرهاب وخاصة مع ازدياد استخدام التكنولوجيات الجديدة كالذكاء الاصطناعي والتعلم الآلي وتحليل البيانات الضخمة.

تعد الإدارة الفعالة للبيانات أمراً ضرورياً لمكافحة الإرهاب وتتطلب استخدام تكنولوجيات وأدوات جديدة لجمع وتحليل ومشاركة المعلومات بصورة آمنة وفي الوقت المناسب. فهي تمكّن وكالات الاستخبارات وإنفاذ القانون من تحديد وتتبع التهديدات المحتملة ورصد أنشطة الإرهابيين المعروفين وشركائهم، والحد من أو تعطيل الهجمات الإرهابية، وهو ما يتضمن جمع وتحليل مجموعة كبيرة من البيانات. ويتطلب تمكين التعاون عبر القطاعات وبين أصحاب المصلحة في مناطق متعددة و/أو الدول الأعضاء أن يجري تناول البيانات التي تتعلق بالتهديدات ذات الصلة بشكل ملائم. ويشمل ذلك أموراً من قبيل التنظيم المناسب ونمط توثيق المعلومات بحيث يسهل الوصول إليها وتشاركها بشكل آمن بين أصحاب المصلحة في مختلف القطاعات وعبر الدول الأعضاء. إضافة إلى ذلك، يجب أن تتناول سياسات مكافحة الإرهاب طرق حماية البيانات لضمان عدم انتهاك خصوصية الأفراد و/أو وقف جمع البيانات عند حدود معينة حماية لحقوق الإنسان.

يجب أن تحدد سياسات مكافحة الإرهاب العملية والسياسات التي يُستخدم من خلالها تحليل البيانات وقواعد البيانات كوسيلة لجمع المعلومات وتحليل التهديدات الإرهابية وذلك كجزء من إدارة البيانات. وعلى سياسات مكافحة الإرهاب النظر في الطرق التي تستخدم فيها التكنولوجيات الجديدة كالذكاء الاصطناعي في فرز ومعالجة وتحليل البيانات التي قام أصحاب المصلحة بجمعها بخصوص التهديدات[56]. وينبغي توخي الحذر لضمان ألا تتعدى البيانات التي جمعت وجرى الاحتفاظ بها على حقوق الخصوصية الفردية وألا تتميز بين الأفراد على أساس النوع أو العرق أو اللون أو اللغة أو الدين أو الرأي السياسي أو أية آراء أخرى، أو الأصول الاجتماعية أو الوطنية، أو أية حالات أخرى. وضمن ممارسة عملية مشاركة المعلومات بين أصحاب المصلحة، وخاصة أصحاب المصلحة عبر حدود متعددة، يجب أن تّرسم السياسات بما يضمن تشارك البيانات بطريقة آمنة لا تؤثر على الأمن التشغيلي لأولئك الذين يتعاملون مع التهديدات. كما ينبغي أن تجري بطريقة تحافظ على خصوصية الأفراد الذين جرى جمع بياناتهم بحيث لا يتمكن إلا العاملون على حالات معينة الوصول إليها وتنفيذ التشفير وإجراءات أمنية أخرى لحماية البيانات من الوصول غير المصرح به أو القرصنة، والالتزام بالقواعد والقوانين الخاصة بحماية البيانات.

56 المملكة المتحدة، المسابقة: استراتيجية المملكة المتحدة لمكافحة الإرهاب، 24.

5 – 3 – 4 الإطار القانوني

يشير الإطار القانوني في سياق مكافحة الإرهاب والتكنولوجيات الجديدة إلى مجموعة من القوانين والأنظمة والسياسات التي تحكم عمليات وكالات إنفاذ القانون وجمع واستخدام والاحتفاظ ومشاركة المعلومات المرتبطة بالتهديدات الإرهابية، فضلاً عن استخدام التكنولوجيات الجديدة لمكافحة الإرهاب. يعد الإطار القانوني أمراً أساسياً لضمان تماشي جهود مكافحة الإرهاب مع المعايير القانونية والأخلاقية وحماية حقوق وخصوصية الأفراد، وتجنب إساءة استخدام السلطة من قبل وكالات الاستخبارات وإنفاذ القانون. وهذا يتضمن إيجاد توازن دقيق بين الحاجة إلى إجراءات فعالة لمكافحة الإرهاب وحماية حقوق الأفراد وحرياتهم. ويلعب الإطار القانوني دوراً حاسماً في ضمان فعالية جهود مكافحة الإرهاب وقانونيتها واحترامها لحقوق وحريات الأفراد مع الاستفادة من التكنولوجيات الجديدة لمكافحة التهديدات المستمرة للإرهاب.

من المهم إيجاد تعريف عملي للإرهاب يمكن استخدامه كأساس للإجراءات القانونية بما فيها الاعتبارات الخاصة بالطرق التي قد يستغل الإرهابيون من خلالها التكنولوجيات الحديثة[57]. وتطرح الطبيعة العالمية للعصر الرقمي صعوبات استثنائية في قدرة الدول على رسم وتنفيذ سياسات مكافحة الإرهاب، بما أن الإرهاب في عصر التكنولوجيات الجديدة يمكن أن يتخطى حدوداً عديدة. وحتى لو قامت الجهة الإرهابية بأعمال ضمن الحدود الوطنية لدولة ما إلا أنها يمكن أن تدفع الآخرين للانخراط في التحريض على الإرهاب وتعزز الأعمال الإرهابية داخل حدود دولة أخرى. عند النظر في الإطار القانوني الذي يحيط بسياسة مكافحة الإرهاب يجب أن يكون التركيز على حماية حقوق الإنسان. ويجب أن تتضمن الأطر القانونية التي تعمل بموجبها سياسات مكافحة الإرهاب افتراضاً مسبقاً ضد استخدام الأدلة التي جرى تحصيلها بشكل غير قانوني في المحاكم كجزء من حماية حقوق الإنسان والخصوصية طوال عملية الاستجابة لمكافحة الإرهاب.

5 – 3 – 5 بناء القدرات

عند تصميم سياسات مكافحة الإرهاب من المهم أن نعمل على بناء إطار ضمن السياسات لمعالجة أمور تتعلق بالتدريب والإعداد. وهنا يشير التدريب إلى تدريب أصحاب المصلحة والعاملين ذوي الصلة وأفراد العامة. والهدف من تدريب صنّاع القرار وأصحاب المصلحة الآخرين هو مساعدتهم على تطوير المعرفة والقدرات اللازمة للاستجابة للتهديدات الإرهابية. ويمكن أن يشتمل ذلك على جلسات تثقيفية ومحاكاة ودورات لتجديد المعلومات، ووسائل أخرى لتمكينهم من فهم دورهم في التصدي للتهديدات الإرهابية التي تنتج عن التكنولوجيات الجديدة وضمان أن تبقى طبيعة الاستجابة لهذه التهديدات متواكبة مع التطورات المستمرة في المجال التكنولوجي. علاوة على ذلك، فإن تدريب العاملين وأفراد العامة كجزء من الاستجابة لسياسات مكافحة الإرهاب يرفع من وعي هذه المجموعات ويساعد في زيادة تمكين القدرات الوطنية للاستجابة للتهديدات الإرهابية والأعمال الإرهابية[58]. فإنشاء وتنفيذ البرامج المتخصصة في تدريب العاملين على إزالة نزعة التطرف و/أو جهود فك الارتباط مع الجهات الإرهابية المعروفة على سبيل المثال قد يتطلب التدخل الضروري في مواجهة الإرهاب للحد من أعمال إرهابية قد تقوم بها تلك الجهات[59].

57 فريز Freese، "مكافحة الإرهاب القائمة على الأدلة أم التغاضي عن الرؤية؟ كيف نفهم ونحقق ما ينجح، 43.

58 كومنولث أستراليا، الكتاب الأبيض للسياسة الخارجية لعام 2017، أد. موريس ووكر بي تي واي المحدودة (أستراليا، 2017)، 38، https://www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf.

59 فيدينو وبينيت Vidino and Bennett، "مراجعة لأفضل الممارسات عبر الأطلسي لمكافحة التطرف في السجون والعودة الإرهابية"، 7–8.

[سادساً]
الممارسات الجيدة في استجابة سياسات مكافحة الإرهاب

6 – 1 لمحة عامة

أجريت مشاورات مع مصادر من المنظمات الدولية، والدول الأعضاء، والأوساط الأكاديمية، والقطاع الخاص لتصميم نموذج لاستجابات سياسات مكافحة الإرهاب يمكنه أن يتعامل بفعالية مع الفرص المحتملة والتحديات المطروحة نتيجة استخدام التكنولوجيات الجديدة. وفيما يلي بعض النتائج المتعلقة بالممارسات التي يمكن ادراجها ضمن استجابات سياسات مكافحة الإرهاب. تهدف مجموعة النتائج المختارة إلى معالجة عنصري بناء سياسات ناجحة لمكافحة الإرهاب قادرة على الاستجابة لاستخدام التكنولوجيات الجديدة لأغراض إرهابية والطرق التي يمكن لصنّاع السياسات وغيرهم من العاملين من خلالها تحسين قدرتهم على التصدي لهذه التهديدات. تُعرض هذه النتائج في الأقسام التالية من منظور الاعتبارات الأربعة التي تعد جزءاً لا يتجزأ من سياسات مكافحة الإرهاب (القسم 5 – 2)، المأخوذة من النموذج الوارد في القسم 5 – 1. وضمن هذه الاعتبارات، تغطي الموارد المذكورة هنا بعض الممارسات الجيدة في إطار المكونات الرئيسية لسياسات مكافحة الإرهاب بخصوص التكنولوجيات الجديدة (القسم 5 – 3).

6 – 2 الوعي

يأتي الوعي في سياق توفير الأدوات والمعرفة والمشاركة للعاملين وأفراد العامة، من أجل التعرف على التهديدات والإبلاغ عنها أو الاستجابة لها، كما رأينا في القسم 5 – 2 – 1. وتقترح منظمة الأمن والتعاون في أوروبا نهجاً يمكن اتباعه في برامج التدريب والإعداد. يتضمن أول هذه البرامج مجموعة من الندوات التي تهدف بشكل خاص إلى زيادة الوعي بالاستجابة لمكافحة الإرهاب بين أفراد العامة[60]. أما بالنسبة للعاملين في مجال مكافحة الإرهاب، فتوصي منظمة الأمن والتعاون في أوروبا بإجراء "تدريبات محاكاة الجاهزية"، التي تستخدم لتشكيل مجموعات عمل من الخبراء في الحكومة والقطاع الخاص والأوساط الأكاديمية (وغيرها)، وتشكل منتدى يمكن من خلاله مناقشة السيناريوهات المحتملة، مما يوفر وسيلة لتطوير قدرة الدولة على الاستجابة للأعمال الإرهابية[61]. كما يوصي معهد بروكينغز بإجراء محاكاة "للعبة الحرب" يشارك فيها العاملون في وكالات وقطاعات مختلفة بالإضافة إلى جلسات التدريب و"تدريبات محاكاة الجاهزية"[62]. وتهدف مثل هذه التمارين إلى التدرب على الاستجابات للهجمات (بما في ذلك خطط

60 إدارة التهديدات العابرة للحدود الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا، "مرجع منظمة الأمن والتعاون في أوروبا لمكافحة الإرهاب" (منظمة الأمن والتعاون في أوروبا، تموز/يوليه 2020)، 25.

61 إدارة التهديدات عبر الوطنية لمنظمة الأمن والتعاون في أوروبا، 25–26.

62 بروس شنايير وتارا ويلر Schneier and Wheeler ، "الطائرات بدون طيار المخترقة والخدمات اللوجستية المحطمة هي المستقبل الفضائي الإلكتروني للحرب"، بروكينغز، تيك ستريم (مدونة)، 4 حزيران/يونيه 2021، https://www.brookings.edu/techstream/hacked-drones-and-busted-logging-are-the-cyber-future-of-warfare.

العمل البديلة)[63]. والهدف هنا مشابه لهدف تمارين الفريق الأحمر، والتي بالإضافة إلى سماحها بممارسة إجراءات الاستجابة، تساعد أيضًا أولئك الذين يصممون سياسات الاستجابة على فهم الثغرات التي ينبغي النظر فيها لتحسين سياسات الاستجابة[64].

يتم التأكيد في مناقشات تدريبات محاكاة الجاهزية في منظمة الأمن والتعاون في أوروبا واستراتيجية مكافحة الإرهاب في الولايات المتحدة على ضمان أن تكون مسائل حماية البنية التحتية الحيوية من الهجمات الإرهابية جزءاً من جدول الأعمال الأوسع بالخاص بمكافحة الإرهاب، لاسيما وأن هذه البنى الأساسية عرضة للهجمات الإلكترونية[65].

ينبغي أن تراعي المخرجات السياساتية المطلوبة ما يلي:

- الفهم العميق لكشف التهديدات والاستجابة لها من قبل أصحاب المصلحة؛
- توعية أفراد العامة بالتهديدات واستجابات السياسات لهذه التهديدات؛
- تعزيز الوعي من خلال برامج التدريب والإعداد، مثل:
  - تثقيف العاملين وأفراد العامة؛
  - المحاكاة واختبارات الفرق الحمراء؛
  - تدريبات محاكاة الجاهزية؛
  - محاكاة "لعبة الحرب".

6 – 3 التدخلات لمواجهة التهديد

تتمثل إحدى الوسائل التي يمكن من خلالها لدولة عضو أن تنفذ إجراءات التدخل في حال التهديد باتباع نهج استباقي للأمن كما ذكرنا سابقاً. ينطوي هذا النهج على التدخل في حالات التهديدات في مرحلة مبكرة بما فيه الكفاية وفي أقرب مكان ممكن من مصدر التهديد لمنع الأعمال الإرهابية من أن تؤتي ثمارها[66].

يمكن تحقيق التدخل في حال التهديد من خلال تطبيق مبادئ الأمن بالتصميم والأمن الافتراضي. يشير مفهوم الأمن بالتصميم إلى فكرة أن يكون أحد الأهداف عند بناء منتج ما أو رسم سياسة ما هو تصميمه وفقاً لإجراءات أمنية تتخذ بطريقة تسمح بالتصدي للتهديد بفعالية[67]. ولا بد من الإشارة إلى أن المفوضية الأوروبية تؤيد نهج الأمن بالتصميم في نقاشاتها حول حماية الأماكن العامة[68].

وتجدر الإشارة إلى أنه من خلال منشور صدر حديثاً أولت كل من وكالة أمن الفضاء الإلكتروني وأمن البنية التحتية في الولايات المتحدة، والمكتب الاتحادي الألماني لأمن المعلومات، وثماني هيئات أخرى للأمن وأمن الفضاء الإلكتروني في الدول الأعضاء، أهمية كبيرة للأمن بالتصميم ضمن سياق التكنولوجيا بالتحديد[69].

63 شنايير و ويلر. Schneier and Wheeler.

64 ديفيد رومين ومارك كيبيل، "تخطيط الإرهابيين للهجمات: تحقيق محاكاة "الفريق الأحمر" في صنع القرار"، علم النفس والجريمة والقانون 20، العدد 20. 5 (28 أيار/مايو 2014): 483، https://doi.org/10.1080/1068316X.2013.793767.

65 إدارة التهديدات العابرة للحدود الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا، "مرجع منظمة الأمن والتعاون في أوروبا لمكافحة الإرهاب"، 26؛ الولايات المتحدة، الاستراتيجية الوطنية للولايات المتحدة الأمريكية لمكافحة الإرهاب، 19–20.

66 المركز الوطني للأمن الفضائي الإلكتروني، "الأمن الافتراضي"، المركز الوطني للأمن الفضائي الإلكتروني، 7 آذار/مارس 2018، https://www.ncsc.gov.uk/information/secure-default.

67 المفوضية الأوروبية، الأمن بالتصميم: حماية الأماكن العامة من الهجمات الإرهابية، 23؛ الأمن الفضائي الإلكتروني والبنية التحتية ووكالة الأمن وآخرون، "تحويل توازن مخاطر الأمن الفضائي الإلكتروني: مبادئ وأساليب للأمن بالتصميم والأمن الافتراضي،" 3–4.

68 المفوضية الأوروبية، الأمن بالتصميم: حماية الأماكن العامة من الهجمات الإرهابية.

69 وكالة الأمن الفضائي الإلكتروني وأمن البنية التحتية وآخرون، "تحويل توازن مخاطر الأمن الفضائي الإلكتروني: مبادئ وأساليب للأمن بالتصميم والأمن الافتراضي.

تناقش هذه الهيئات أيضاً أهمية الأمن الافتراضي إضافة إلى الأمن بالتصميم، وهو ما يشير إلى كون "المنتج" النهائي (التكنولوجي، أو في هذه الحالة، السياسة) منتج آمن ويوفر وسائل الدفاع كجزء من طبيعة المنتج/السياسة بحد ذاته عند إصداره[70]. واستنادا إلى المفاهيم المقدمة في هذين المثالين للأمن بالتصميم والأمن الافتراضي، يمكننا تطبيق ذلك على تصميم سياسات مكافحة الإرهاب من خلال وسائل مثل وضع إجراءات تشغيل موحدة للاستجابة لأشكال محددة من التكنولوجيا يمكن تكييفها بسهولة لتلائم سيناريوهات متعددة. ويمكن تنفيذ هذه المفاهيم أيضاً من خلال التركيز على استخدام العاملين للتكنولوجيا كوسيلة لتأمين الأنظمة كأنظمة البنية التحتية الحيوية لدولة عضو.

في ورقة بحثية قُدمت في مؤتمر نظمته وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون، يقترح المؤلفون عدة خطوات يمكن بموجبها اتخاذ نهج استباقي في معرض التصدي لنزعة التطرف الإرهابي وخاصة في السجون من خلال تغييرات تطرأ على السياسات[71]. ومن بين توصياتها، تقترح الورقة مشاركة المعلومات بين السجون والهيئات الحكومية الأخرى كوسيلة للكشف عن علامات التطرف بين السجناء على النحو الذي يحدده العاملون الذين خضعوا للتدريب على تحديد ومعالجة مثل هذا السلوك[72]. أما في حال اكتشاف مثل هذا السلوك، يدعو الاقتراح إلى أن يخضع هؤلاء الأفراد إما لنزع التطرف أو فك الارتباط[73].

توجد وسيلة أخرى يمكن من خلالها تنفيذ التدخل في حال التهديد من قبل الدول الأعضاء وذلك بوضع إطار قانوني تعمل السياسات بموجبه. في إطار النقاش حول استخدام الأمن بالتصميم والأمن الافتراضي، تشير المنظمات المؤلِّفة في تقريرها الوارد تحت عنوان "تحويل التوازن في مخاطر أمن الفضاء الإلكتروني: مبادئ ومناهج في الأمن بالتصميم والأمن الافتراضي،" إلى الجهود التي يبذلها الاتحاد الأوروبي لتقديم إطار قانوني يجري من خلاله تناول المسائل المتعلقة بأمن الفضاء الإلكتروني في قانون مرونة الفضاء الإلكتروني[74]. يسعى هذا القانون المقترح في نهاية عام 2022 إلى تقديم إجراءات تنظيمية تهدف إلى ضمان تطوير التكنولوجيات المستقبلية بطريقة تشتمل على مفاهيم الأمن بالتصميم، بحيث يكون ما يصل إلى السوق أقل عرضة للاختراقات الأمنية افتراضياً[75]، وهذا من شأنه أن يكون بمثابة تدبير وقائي للتدخل في حالات التهديدات من خلال جعل المنتجات المتاحة للمستهلكين أقل عرضة للتهديدات المحتملة.

ثمة مثال إضافي على استخدام النظام القانوني كوسيلة للتدخل في حال التهديد وهو النظام الذي تدعمه الأمم المتحدة ويتضمن إطاراً قانونياً دولياً يمكن من خلاله التصدي لجهود مكافحة الإرهاب. والهدف من هذا الإطار هو تمكين إنفاذ القانون ضد الأعمال الإرهابية بغض النظر عن المكان الذي يتواجد فيه الشخص الذي يرتكب الأعمال الإرهابية[76]. وكجزء من هذا الإطار الدولي، حددت الأمم المتحدة تسع عشرة وثيقة قانونية دولية لمعالجة إجراءات مكافحة الإرهاب على الصعيد العالمي[77]. ولتمكين الإطار القانوني الدولي من العمل على النحو المنشود بين الدول الأعضاء، يجب أن يتم بناء وإقرار سياسات مكافحة الإرهاب بموجب القانون كما يجب أن تخضع لرقابة مستقلة.

70 وكالة الأمن الفضائي الإلكتروني وأمن البنية التحتية وآخرون، 5-6.

71 فيدينو وبينيت، Vidino and Bennett "مراجعة لأفضل الممارسات عبر الأطلسي لمكافحة التطرف في السجون والعودة الإرهابية".

72 المرجع نفسه، 6-5.

73 المرجع نفسه، 8.

74 وكالة الأمن الفضائي الإلكتروني وأمن البنية التحتية وآخرون، "تحويل توازن مخاطر الأمن الفضائي الإلكتروني: مبادئ وأساليب الأمن بالتصميم والأمن الافتراضي"، 3.

75 "قانون المرونة الفضائية الإلكترونية"، المفوضية الأوروبية، 15 أيلول/سبتمبر 2022، https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

76 "الإطار القانوني الدولي"، الأمم المتحدة: مكتب المخدرات والجريمة، المتاح بدءاً من 25 نيسان/أبريل 2023، https://www.unodc.org/unodc/en/terrorism/expertise/international-legal-framework.htm "الإطار القانوني لمكافحة الإرهاب: الدروس المستفادة من سياسة المنظمة الدولية لقانون التنمية حوارات بالتعاون مع مكتب الأمم المتحدة المعني بالمخدرات والجريمة، تحديث قانون التنمية، رقم. 2 (2007)، https://www.files.ethz.ch/isn/138640/14.pdf.

77 الوثائق القانونية الدولية، مكتب الأمم المتحدة لمكافحة الإرهاب، متاحة منذ 25 نيسان/أبريل 2023، https://www.un.org/counterterror/international-legal-instruments؛ إدارة التهديدات العابرة للحدود الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا، "حالة الاتفاقيات والبروتوكولات العالمية لمكافحة الإرهاب بالإضافة إلى الوثائق القانونية الدولية والإقليمية الأخرى المتعلقة بالإرهاب والتعاون في المسائل الجنائية في منطقة منظمة الأمن والتعاون في أوروبا" (منظمة الأمن والتعاون في أوروبا (منظمة الأمن والتعاون في أوروبا)، تموز/يوليه 2018)، https://www.osce.org/files/f/documents/5/8/17138_0.pdf.

ينبغي أن تراعي المخرجات السياساتية المطلوبة ما يلي:

- زيادة التعاون بين القطاعات والوكالات والدول الأعضاء وغيرها، لمواجهة التهديد المتمثل في استخدام الإرهابيين للتكنولوجيات الجديدة.
- تحقيق الأهداف الوطنية لمكافحة الإرهاب المتمثلة في المنع والتعطيل والإنكار والحماية والاستعادة والملاحقة القضائية.
- تطوير استجابات استباقية للتهديدات قد تشمل:
  - الأمن بالتصميم/الأمن الافتراضي؛
  - تحديد التهديدات وتحديد أولوياتها؛
  - نزع التطرف وفك الارتباط.

6 – 4 القدرات الوطنية

لتحقيق هدف بناء القدرة الوطنية لإحدى الدول الأعضاء للاستجابة للإرهاب، يمكن الاستفادة من الممارسات الجيدة التي تنفذها الدول الأعضاء. فعلى سبيل المثال، تشير استراتيجية مكافحة الإرهاب في فنلندا إلى الحاجة إلى الابتكار التكنولوجي من خلال مناقشة حاجة البلاد لمواصلة بناء قدراتها في مجال الفضاء الالكتروني، وخاصة فيما يتعلق بوسائل جمع المعلومات الاستخباراتية[78]. كما يمكن الإشارة إلى تقاطع آخر بين الابتكار والقدرة الوطنية في استراتيجية مكافحة الإرهاب في المملكة المتحدة.

التعاون بين العاملين في الحكومة، والقطاع الخاص هو أحد أشكال التعاون التي جرت مناقشتها، مع التركيز على بناء العلاقة بين الحكومة وقطاع التكنولوجيا كجزء من الجهود الابتكارية لمواصلة تنمية القدرة التكنولوجية للبلاد استجابة للإرهاب[79]. إضافة إلى ذلك، تشدد استراتيجية مكافحة الإرهاب على أهمية "بناء القدرات" الخاصة بهم، فضلاً عن الحاجة لمساعدة الدول الأعضاء الأخرى في زيادة قدرتها على الاستجابة للأعمال الإرهابية.

يمكن أيضاً تحقيق زيادة في القدرة الوطنية من خلال تنفيذ برامج التدريب والإعداد. وإضافة إلى ممارسات التدريب والإعداد التي نوقشت في القسم 6 – 1 (التي تعمل أيضاً على بناء القدرات الوطنية لتحديد التهديدات والاستجابة لها بالإضافة إلى بناء الوعي)، فإن التدريبات المفصلة الواردة في وثيقة اليوروبول بشأن جهود نزع التطرف (انظر أيضاً القسم 6 – 2) في السجون يمكن أن تبني أيضاً القدرة الوطنية للتخفيف والاستجابة لنزعة التطرف والاستجابة لها.

يمكن تحقيق أحد العناصر الرئيسية لتعزيز الابتكار في القدرات الوطنية لمكافحة الإرهاب من خلال ابتكار برامج البحث والتطوير. تركز البحوث الأمنية في الاتحاد الأوروبي[80] على إقامة مبادرات تهدف إلى تعزيز قدرة سلطات إنفاذ القانون في مجالات مثل تطوير حلول تحليلية بهدف التعامل مع البيانات الضخمة. بالإضافة إلى ذلك، يجري دمج البحث بشكل أكبر ضمن دورة السياسات الأمنية في إطار برنامج البحث المستقبلي "أفق أوروبا" لضمان تحقيق مخرجات موجهة نحو التأثير، بما يؤدي إلى الاستجابة لاحتياجات إنفاذ القانون المحددة[81].

78 وزارة الداخلية الفنلندية، الاستراتيجية الوطنية لمكافحة الإرهاب 2022–2025، منشورات وزارة الداخلية، 2022:38 (هلسنكي، فنلندا: وزارة الداخلية الفنلندية، 2022)، 24، https://julkaisut.valtioneuvosto.fi/handle/10024/164447.

79 المملكة المتحدة، المسابقة Contest : استراتيجية المملكة المتحدة لمكافحة الإرهاب، 28.

80 المفوضية الأوروبية، أجندة الاتحاد الأوروبي لمكافحة الإرهاب: التوقع والمنع والحماية والاستجابة، الاتصالات من المفوضية إلى البرلمان الأوروبي، والمجلس الأوروبي، والمجلس، واللجنة الاقتصادية والاجتماعية الأوروبية ولجنة المناطق (بروكسل)، بلجيكا: المفوضية الأوروبية، 2020)، https://home-affairs.ec.europa.eu/system/files/2020-12/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf.

81 انظر على سبيل المثال مشروعي DANTE وTENSOR ("كشف وتحليل المحتويات والأنشطة المالية ذات الصلة بالإرهاب"، المفوضية الأوروبية: كورديس، تم الوصول إليه في 23 نيسان/أبريل 2023، https://cordis.europa.eu/project/id/700367. "استرجاع وتحليل المحتوى غير المتجانس عبر الإنترنت للتعرف على الأنشطة الإرهابية"، المفوضية الأوروبية: كورديس، متاح بدءاً من 23 نيسان/أبريل 2023، https://cordis.europa.eu/project/id/700024.

ينبغي أن تراعي المخرجات السياساتية المطلوبة ما يلي:

- تحديد أولويات الموارد ذات الأدوار والمسؤوليات الواضحة.
- زيادة القدرات الوطنية من خلال:
  - مشاركة المعلومات؛
  - الابتكار والبحث والتطوير؛
  - لتعاون والشراكات؛
  - بناء القدرات.

6 – 5 التعاون

يمكن للتعاون كونه ركيزة لتصميم وتنفيذ سياسات مكافحة الإرهاب المتعلقة بالتكنولوجيات الجديدة أن يتخذ أشكالًا عديدة كما يمكن أن يتم تنفيذه على مستويات متعددة (عبر الدول، بين الوكالات، بين القطاعات، وغير إلى ذلك). وعلى هذا النحو، فقد أسفرت الدراسات التي جرى الاطلاع عليها من أجل إعداد هذا التقرير عن أشكال متعددة للممارسات الجيدة التي تساعد في تصميم وتنفيذ استجابات سياسات مكافحة الإرهاب.

في ملخص لوقائع المؤتمرات المتعلقة بالاستراتيجيات الوطنية والإقليمية لمكافحة الإرهاب، يوصي مركز الأمم المتحدة لمكافحة الإرهاب، على سبيل المثال، بأن تتعاون الدول الأعضاء وتقدم المشورة لبعضها البعض في صياغة استراتيجيات مكافحة الإرهاب[82]. وهنا، يمتد مفهوم مشاركة المعلومات، كما قدمنا له في القسم 5 – 3 – 1، إلى ما هو أبعد من مشاركة المعلومات لأنه يتعلق بتهديدات محددة ويسلط الضوء على أهمية التشارك الذي يأتي على شكل ممارسات جيدة. تحتل هذه التوصية أهمية خاصة عند مناقشة تطوير سياسات مكافحة الإرهاب من حيث صلتها بالتكنولوجيات الجديدة. ويمكن للدول الأعضاء أن تتشارك فيما بينها التطورات المتعلقة بكيفية مكافحة استخدام التكنولوجيات الجديدة لأغراض إرهابية، وكيفية استخدام هذه التكنولوجيات كوسيلة للاستجابة للإرهاب. ومن الممارسات الجيدة الأخرى ذات القيمة الواردة في هذه الوثيقة ممارسة إنشاء استراتيجيات إقليمية للحالات التي تصبح فيها الأعمال الإرهابية والتحريض قضايا عابرة للحدود، وهو ما أصبح أكثر شيوعاً وعلى نحو متزايد في العصر الرقمي[83]. وفي المقابل، وصف الاتحاد الأوروبي التعاون عبر الحدود بأنه "الإجابة الدولية" على التهديدات العالمية[84].

وفيما يتعلق بإدارة البيانات، تتناول استراتيجية مكافحة الإرهاب في إسبانيا جانبين أساسيين يجب مراعاتهما في سياسات مكافحة الإرهاب، وهما القدرة على استخدام البيانات والقدرة على جعل البيانات متاحة لأولئك الذين يحتاجون الوصول إليها وحمايتها من أولئك الذين لا ينبغي لهم الاطلاع على تلك المعلومات[85]. وتشدد الوثيقة على ضرورة التشفير من أجل أن يجري تشارك البيانات بين الجهات المعنية في القطاعات المختلفة بصورة آمنة. كما تشدد على ضرورة تنظيم البيانات بطريقة تجعل عمليات فرزها واستخدامها من قبل أصحاب المصلحة سهلة وفعالة[86].

82 مركز الأمم المتحدة لمكافحة الإرهاب، "ملخص المناقشات: المؤتمر الدولي المعني بالقضايا الوطنية والإقليمية استراتيجيات مكافحة الإرهاب – 31 كانون الثاني/يناير – 1 شباط/فبراير 2013،" ملخص المؤتمر (بوغوتا، كولومبيا، 2013)، 5، https://www.un.org/counter-error/sites/www.un.org.counter-error/files/bogota_jan-feb2013.pdf.

83 مركز الأمم المتحدة لمكافحة الإرهاب، 7.

84 الاتحاد الأوروبي، التوجيه 2017/541 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 15 آذار/مارس 2017 بشأن مكافحة الإرهاب واستبدال القرار الإطاري للمجلس JHA/2002/475 وتعديل قرار المجلس JHA/2005/671/7/88، JHA.

85 وزارة الداخلية الإسبانية، الاستراتيجية الوطنية لمكافحة الإرهاب، 2019، 54-53، https://www.dsn.gob.es/eu/file/4271/download?token=K6uOf-C.

86 المرجع نفسه.

تتمثل إحدى طرق مشاركة المعلومات من خلال استخدام إدارة البيانات بإنشاء سجل للمخاطر يكون بمثابة قاعدة بيانات للتهديدات الحالية والمعلومات الاستخباراتية المتاحة التي جمعها أصحاب المصلحة بشأن تلك التهديدات. ونموذج سجل المخاطر الخاص بوكالة النقل النيوزيلندية هو مثال جيد عن أنواع المعلومات التي ينبغي إدراجها في سجل المخاطر الخاص ببلد ما، مثل الرقم المرجعي للتهديد، وقسم يوضح تاريخ ووصف آخر مرة اتخذت فيها إجراءات ضد التهديد، وخطة العمل التي ينبغي اتباعها في حالة تحقق التهديد، وتفصيل الأدوار التي يجب أن تضطلع بها كل جهة في حال أصبح التهديد محققاً[87].

من الوسائل التي يمكن من خلالها مشاركة مثل هذا السجل والمعلومات المرفقة به بصورة آمنة اعتماد نموذج مشابه لنموذج "التجمع العنقودي" المتبع في المملكة المتحدة الذي يعداً وسيلة للتعاون الإقليمي ما بين القطاعات بين السلطات الحكومية وشركات القطاع الخاص والأوساط الأكاديمية. وضمن هذا النموذج، نجد تجمعاً خاصاً بكل منطقة يعمل بشكل شبه مستقل فيما يتعلق بتحديد أولويات التهديد الأكثر ملاءمة لمنطقة مسؤوليتها المحددة. ويتشارك أصحاب المصلحة ضمن كل تجمع المعلومات والممارسات الجيدة. فتنخرط المجموعات في شكل من أشكال المركزية وتقوم في نهاية المطاف بالإبلاغ ومشاركة المعلومات مع أصحاب المصلحة على المستوى الوطني فيما يتعلق بالتهديدات[88]. وتُمكّن الطبيعة المحلية للنموذج من اتباع نهجٍ أكثر دقة في تقييم التهديدات وتحديد الأولويات بخصوصها، وذلك لارتباطه بمنطقة المسؤولية، كما يمكّن في الوقت نفسه أصحاب المصلحة على المستوى الوطني من الوصول إلى فهم عميق لكل منطقة من المناطق الواقعة ضمن مسؤوليتهم.

ينبغي أن تراعي المخرجات السياساتية المطلوبة ما يلي:

- تعزيز التعاون بين الفرق الوطنية للاستجابة لحوادث أمن الحاسوب وسلطات إنفاذ القانون والعدالة الجنائية للتحقيق وملاحقة الإرهابيين؛
- تعزيز التعاون بين سلطات إنفاذ القانون وشركات تكنولوجيا المعلومات والاتصالات الخاصة؛
- تعزيز التعاون الإقليمي والدولي؛
- تعزيز مشاركة المعلومات من خلال:
  - مشاركة الممارسات الجيدة؛
  - عقد اتفاقيات تبادل المعلومات؛
  - تعزيز نهج وممارسات إدارة البيانات.

87 وكالة النقل النيوزيلندية, "سجل المخاطر"، الحكومة، وكالة النقل Waka Kotahi NZ، متاح منذ 1 نيسان/أبريل 2023، https://www.nzta.govt.nz/roads-and-rail/rail/operating-a-railway/risk-management/risk-register.

88 UKC3، "إطار تشغيل المجموعة الفضائية الإلكترونية"، تعاون المجموعة الفضائية الإلكترونية في المملكة المتحدة (مدونة)، متاح منذ 30 آذار/مارس 2023، https://ukc3.co.uk/cyber-cluster-operating-framework.

مكتب الأمم المتحدة لمكافحة الإرهاب
المقر الرئيسي لمنظمة الأمم المتحدة
نيويورك، نيويورك 10017
www.un.org/counterterrorism/ar

مكتب الأمم المتحدة
لمكافحة الإرهاب
مركز الأمم المتحدة لمكافحة الإرهاب

24-11110