مكتب الأمم المتحدة
لمكافحة الإرهاب
مركز الأمم المتحدة لمكافحة الإرهاب

الإنتربول

بتمويل من
الاتحاد الأوروبي

أمن الفضاء الإلكتروني والتكنولوجيات الجديدة

إجراء تقييم للتهديدات الإرهابية: 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.

حقوق النشر

© مكتب الأمم المتحدة لمكافحة الإرهاب، 2023

مكتب الأمم المتحدة لمكافحة الإرهاب

مقر الأمم المتحدة

نيويورك، نيويورك 10017

www.un.org/counterterrorism/ar

© المنظمة الدولية للشرطة الجنائية (الإنتربول)، 2023

200، رصيف شارل ديغول

69006 ليون، فرنسا

www.interpol.int/en

المحتويات

توطئة مشتركة 4
شكر وتقدير 5
مصطلحات وتعاريف 5
ملخص تنفيذي 7
[أولا]
خلفية 8
1 – 1 لمحة عامة 8
1 – 2 مبادرة التكنولوجيا لمكافحة الإرهاب 9
1 – 3 أغراض الوثيقة واستخداماتها 10
[ثانيا]
النهج 12
2 – 1 لمحة عامة 12
2 – 2 الإطار التوجيهي 12
2 – 3 المنهجية 14
[ثالثا]
مقدمة 18
3 – 1 لمحة عامة 18
3 – 2 التكنولوجيات الجديدة ومكافحة الإرهاب 18
[رابعا]
تقييم التهديدات والمخاطر 21
4 – 1 لمحة عامة 21
4 – 2 دورة إدارة التهديدات والمخاطر 23
[خامسا]
الممارسات الجيدة في تقييم التهديدات 31
5 – 1 لمحة عامة 31
5 – 2 النهج متعدد الوكالات ومراكز الدمج 31
5 – 3 النهج القائم على المخاطر 33
5 – 4 قياس مستويات التهديد 33
5 – 5 جمع معلومات التهديد وتحليلها 35
5 – 6 التقييم المستمر 36
5 – 7 تعزيز مشاركة المعلومات الاستخباراتية 36
5 – 8 البحث والابتكار 38
[الملحق أ]
معادلة نموذجية توضيحية لإسناد التهديد 39
أ – 1 لمحة عامة 39
[الملحق ب]
مثال على إساءة استخدام التكنولوجيا من قبل الإرهابيين 40
ب – 1 لمحة عامة 40
[الملحق ج]
أسئلة إرشادية لتقييم التهديدات 44
ج – 1 لمحة عامة 44
ج – 2 الأسئلة الإرشادية 44

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

أعدت 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 ل مكتب 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

الذكاء الاصطناعي	يستخدم عموما لوصف التخصص المعني بتطوير الأدوات التكنولوجية التي تمارس أعمالا بشرية، كالتخطيط والتعلم والتفكير والتحليل.
إجراءات العدالة الجنائية	هي إجراءات قانونية لتوجيه تهم الإرهاب لفرد أو كيان وجلسة المحكمة والحكم أو القرار والعقوبة وكذلك الإصلاح وإعادة التأهيل.
الأدلة	مصطلح رسمي للمعلومات التي تشكل جزءا من المحاكمة، بمعنى أنها تستخدم لإثبات الجريمة المزعومة أو نفيها. تعتبر كافة الأدلة معلومات بينما لا تشكل جميع المعلومات أدلة. وبذلك تعتبر المعلومات الشكل الأولي والأصلي للأدلة[1].
الاستخبارات	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 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 الادعاء في الإجراءات القانونية.
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.

1 دليل المديرية التنفيذية للجنة مكافحة الإرهاب لتسهيل استخدام المعلومات التي تم جمعها ومعالجتها وحفظها ومشاركتها من قبل القوات المسلحة وقبولها كأدلة في المحاكم الجنائية الوطنية بغرض الملاحقة القضائية للجرائم الإرهابية (2021).

التكنولوجيات الجديدة	في حين يغطي مصطلح التكنولوجيات الجديدة مجموعة واسعة من التكنولوجيات المختلفة[2]، فإن التكنولوجيات الجديدة، ولأغراض هذا المستند، تشير إلى استخدام وسوء استخدام مثل هذه التكنولوجيات الجديدة كالإنترنت، ووسائل التواصل الاجتماعي، والعملات الرقمية المشفرة، والتعرف على الوجوه، والشبكة المظلمة[3].
استخبارات المصادر المفتوحة	هي المعلومات الاستخبارية التي تجمع من مصادر متاحة للعموم[4].
الادعاء / الحكم	إجراءات قانونية لتوجيه تهم الإرهاب لفرد أو كيان وجلسة المحكمة والحكم أو القرار في القضية والعقوبة عند الإدانة.
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.
استخبارات وسائل التواصل الاجتماعي	هي المعلومات الاستخباراتية التي تجمع من خلال وسائل التواصل الاجتماعي.
الإرهاب	عمليات إجرامية، بما في ذلك ضد المدنيين، ترتكب بنية التسبب بالموت أو الإصابة الجسدية الجسيمة، أو احتجاز الرهائن، بهدف إثارة حالة من الرعب بين العامة أو ضمن مجموعة من الأشخاص أو أشخاص معينين، وتخويف السكان أو إجبار الحكومة أو إحدى المنظمات الدولية على القيام أو الامتناع عن القيام بأي فعل، والذي يشكل جرائم ضمن نطاق الاتفاقيات والبروتوكولات الدولية المتعلقة بالإرهاب ووفق تعريفها[5].
الجهة المهددة	هي فرد أو كيان يستخدم تكنولوجيات جديدة لأغراض إرهابية، مثل التطرف والتجنيد والتحريض على ارتكاب أعمال إرهابية، وتمويل أنشطته والتخطيط لها، وكذلك لارتكاب عمل إرهابي. وفي حالة مكافحة الإرهاب والتكنولوجيا الجديدة، يمتد هذا إلى استخدام التكنولوجيات الجديدة للقيام بأفعال مؤذية أو استخدام التكنولوجيا للتأثير على الآخرين لارتكاب أعمال إرهابية[6].
تقييم التهديد	هو منتج يوفر، من خلال منهجية متفق عليها، تحليلًا وإرشادات للعمل على معالجة المشكلات المحددة التي قد تتسبب بالأذى للدولة والمجتمع في المستقبل[7].
المشهد العام للتهديد	يشير مشهد التهديد إلى الصورة العامة للتهديدات الإرهابية المحتملة التي قد تواجهها دولة أو منطقة أو منظمة. ويشمل نطاق المجموعات الإرهابية وقدراتها ونواياها وتكتيكاتها، فضلاً عن ثغرات الأهداف المحتملة والتأثير المحتمل للهجوم.
هدف التهديد	هو كيان أو موقع أو مجموعة معينة يتم تعرف على أنها عرضة لهجوم إرهابي محتمل[8].
ناقل التهديد	الطريقة أو الوسيلة المحددة التي تنفذ بها الجهة المهددة هجوما.
زيتابايت	زيتابايت واحد يساوي مليار تيرابايت.

2 الذكاء الاصطناعي وإنترنت الأشياء وتقنيات البلوك تشين والأصول المشفرة والطائرات المسيرة والأنظمة الجوية المسيرة والحمض النووي وبصمات الأصابع وتكنولوجيا الفضاء الإلكتروني السيبرانية والتعرف على الوجه والطباعة الثلاثية الأبعاد.

3 تكنولوجيا مكافحة الإرهاب، وثيقة البرنامج، الملحق الأول: توصيف الإجراء.

4 روب فلاندرز وآخرون، استخبارات التهديدات السيبرانية 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.

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

6 المركز الكندي للأمن السيبراني، مدخل إلى بيئة التهديدات السيبرانية 2023-2024 (مؤسسة أمن الاتصالات في كندا، 2022)، 2، https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment.

7 مكتب الأمم المتحدة المعني بالمخدرات والجريمة، إرشادات بشأن إعداد واستخدام تقييمات تهديدات الجريمة الخطيرة والمنظمة: دليل SOCTA (نيويورك، نيويورك: الأمم المتحدة، 2010)، https://www.unodc.org/documents/organized-crime/SOCTA_Handbook.pdf.

8 ماري إي. شاكليت، "ما هو ناقل الهجوم؟"، Tech Target، نيسان/أبريل 2021، https://www.techtarget.com/searchsecurity/definition/attack-vector.

ملخص تنفيذي

تهدف هذا الوثيقة إلى تقديم إرشادات للدول الأعضاء في تقييم التهديدات الإرهابية والتخفيف منها والاستجابة لها بفاعلية، وخاصة تلك المتعلقة باستخدام وسائل التكنولوجيا الجديدة. يمكن للدول الأعضاء، من خلال إجراء عملية تقييم هيكلية للتهديدات والمخاطر، تعزيز وعيها بالوضع، وقدراتها على الاستجابة، والسلامة العامة لديها، وبالتالي تحسين جهودها في مجال مكافحة الإرهاب. تم تجميع هذه الوثيقة كنتاج للأبحاث المكتبية، واستشارات أصحاب المصلحة، ولقاءات مجموعات الخبراء، والممارسات الجيدة في منهجيات تقييم التهديدات والمخاطر الحالية. إن مواجهة استخدام التكنولوجيا الجديدة لأغراض إرهابية تتطلب فهم استخداماتها، وتطوير أطر قانونية وسياسات، وبناء قدرات تشغيلية، مع الالتزام بحقوق الإنسان والقانون الدولي.

تعتبر تقييمات التهديدات والمخاطر مكونا أساسيا في جهود مكافحة الإرهاب، حيث توفر لصناع السياسات فهمًا أفضل للتهديدات الحالية والمحتملة والموارد المطلوبة للتعامل معها. وتوفر هذه الوثيقة هيكلية منهجية لعملية تقييم التهديدات والمخاطر. كما تهدف إلى تقديم ممارسات جيدة لإجراء تقييمات تهديدات ومخاطر استخدام التكنولوجيا الجديدة لأغراض إرهابية. تقدم دورة فريدة لإدارة التهديدات والمخاطر، وهي عملية هيكلية تهدف إلى تقييم وإدارة التهديدات المحتملة من استغلال التكنولوجيا الجديدة لدولة على المستوى الوطني. تشمل العملية تحديد الجهات المهددة، وتحليلا يعتمد على نواياها وقدرتها التكنولوجية على ارتكاب عمل إرهابي. الخطوة التالية هي تطوير سيناريوهات التهديد، والتي تنطوي على تحليل قدرات الجهات المهددة وإمكانية وصولها إلى التكنولوجيا الجديدة وتحديد أنواع الهجمات المحتملة ومستوى التعقيد في تلك الهجمات. يضم سيناريو التهديد الناتج كلا من تكرارات أنواع الهجمات ضد ثغرات مختلفة. المرحلة التالية هي تقييم التهديدات وتحديد أولوياتها، وتتم ضمن سياق استجابات التهديد لاستخدام التكنولوجيا الجديدة لأغراض إرهابية. يمكن أن تشمل هذه المرحلة عمليات مثل وضع إجراءات تشغيل قياسية للاستجابة لأشكال معينة من التكنولوجيا التي يمكن تكييفها بسهولة لتناسب سيناريوهات متعددة. إن تطوير استجابة للتهديد عملية مستمرة تشمل استعراضات دورية لسيناريوهات التهديد الحالية، وتحديد التهديدات الجديدة المحتملة، وتحديثات لاستراتيجيات تقييم التهديد والاستجابة.

هذه الوثيقة موجهة في المقام الأول للممارسين المسؤولين عن إجراء تقييمات لتهديدات الإرهاب ومخاطره على المستوى الوطني بالتعاون مع أصحاب المصلحة المعنيين لفهم تهديدات الإرهاب واستخدام التكنولوجيا الجديدة بما يفيد صناع القرار والسياسات وطنيا. كما يوفر لهم هذا الدليل الممارسات الجيدة والمعلومات القابلة للتنفيذ لتعزيز وعيهم بالوضع وقدرات الاستجابة لديهم. من خلال تطوير فهم عميق لاستخدام التكنولوجيا الجديدة لأغراض إرهابية عبر عملية تقييم هيكلية للتهديدات والمخاطر، يمكن للدول الأعضاء تحسين كفاءة جهود مكافحة الإرهاب، بما في ذلك المعلومات القابلة للتنفيذ بشأن المشهد العام للتهديد. بالإضافة إلى ذلك، يمكن أن تساعد ممارسة إجراء تقييمات فعالة للتهديدات والمخاطر في تعزيز السلامة العامة وكذلك في تطوير إجراءات استباقية لمنع النشاط الإرهابي أو الحد من تأثيره.

[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)[9] 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)[10] ورقم 2396 (2017)[11] 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[12]، 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 الإنترنت الخفية** 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[13].

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

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

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

12 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 S/2022/547 (undocs.org).

13 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

تهدف هذه الوثيقة إلى تزويد الدول الأعضاء بالفهم والأدوات اللازمة لتقييم التهديدات بفعالية ضمن مناطق مسؤوليتها. وتهدف إلى توجيه عملية تقييم التهديد على المستوى الوطني ونشر الوعي وتقديم إرشادات غير ملزمة للممارسات الجيدة لتطوير وتنفيذ عملية تقييم التهديد والمخاطر بشأن استخدام التكنولوجيا الجديدة لأغراض إرهابية. وهذا الفهم سيساعد صناع القرار على زيادة كفاءتهم في تخطيط الاستجابات السياساتية لمكافحة التهديدات الإرهابية، خاصة فيما يتعلق باستخدام التكنولوجيا الجديدة وإساءة استخدامها لأنشطة مؤذية.

1 – 3 – 1 نطاق العمل

تركز هذه الوثيقة بشكل خاص على عملية تقييم التهديدات والمخاطر على المستوى الوطني. وتهدف إلى نشر الوعي وتقديم إرشادات حول الممارسات الجيدة لتطوير عملية تقييم التهديدات والمخاطر وتنفيذها. وتهدف الوثيقة إلى دعم وتمكين الدول الأعضاء لإجراء تقييمات وطنية للتهديدات والمخاطر المتعلقة باستخدام التكنولوجيا الجديدة لأغراض إرهابية، بما في ذلك المشاهد التهديدية الحالية والمستقبلية. وتتماشى الوثيقة مع استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب وتؤكد على أهمية احترام حقوق الإنسان وسيادة القانون في جهود مكافحة الإرهاب. وتستند إلى أبحاث مكتبية حول المنهجيات القائمة في تقييم التهديدات، واستشارات من قبل أصحاب المصلحة، ولقاءات مجموعات الخبراء. وتشمل مصادر الأبحاث المكتبية تقييمات التهديدات والمخاطر الوطنية للدول الأعضاء.

1 – 3 – 2 الجمهور المستهدف

هذه الوثيقة موجهة في المقام الأول إلى الممارسين المسؤولين عن إجراء تقييمات التهديدات والمخاطر الإرهابية الوطنية، بالتعاون مع أصحاب المصلحة المعنيين، من أجل فهم أفضل للتهديد الإرهابي واستخدام التكنولوجيات الجديدة بما يفيد صناع القرار والسياسات الوطنية. كما تهدف أيضا إلى تزويدهم بمعلومات ذات صلة وقابلة للتنفيذ وتعزيز وعيهم بالوضع وقدرات الاستجابة لديهم.

1 – 3 – 3 الفوائد

من خلال تطوير فهم عميق لاستخدام التكنولوجيات الجديدة لأغراض إرهابية عبر عملية تقييم هيكلية للتهديدات والمخاطر، يمكن للدول الأعضاء تحسين كفاءة جهود مكافحة الإرهاب، بإدراجها معلومات قابلة للتنفيذ ضمن المشهد العام للتهديد. يمكن لهذا أن يساعد في تحسين الوعي بالوضع، مما يتيح استجابة أكثر فعالية وتكاملًا للتهديدات المحتملة، وتخصيص الموارد، والتخطيط الاستراتيجي. كما يمكن لتقييمات التهديد والمخاطر أن تساعد في تعزيز السلامة العامة، وتطوير إجراءات استباقية لمنع الأنشطة الإرهابية أو الحد من تأثيرها.

1 – 3 – 4 أوجه القصور

على الرغم من وجود العديد من الفوائد لوثيقة "إجراء تقييم للتهديدات الإرهابية: استخدام التكنولوجيات الجديدة لأغراض إرهابية"، إلا أن هناك أيضًا بعض القيود والتحديات التي تجب مراعاتها. فيما يلي بعض من هذه القيود:

- التطور سريع في المشهد العام للتهديد: إن مشهد التهديد يتطور باستمرار، مما يعني أن أي تقييم للتهديدات ما هو إلا لقطة سريعة للوقت الذي أجري فيه. وبالتالي يمكن أن تصبح التقييمات قديمة بسرعة مالم تزود بالتحديثات اللازمة لضمان استمرار حداثتها ودقتها أمام تطور المشهد العام للتهديد والتقدم المستمر في التكنولوجيا.
- محدودية الوصول إلى المعلومات: يمكن أن يكون الوصول إلى المعلومات حول التهديدات الإرهابية المحتملة محدودا، خاصة عندما يتعلق الأمر بالمعلومات الاستخباراتية السرية أو المعلومات التي تحتفظ بها الحكومات أو الكيانات الأجنبية لدى القطاع الخاص. وهذا من شأنه أن يصعب إجراء تقييم شامل للتهديدات والمخاطر.
- تعقيد منظومة التكنولوجيا: منظومة التكنولوجيا معقدة وتخضع للتغير السريع، وبالتالي قد يكون من الصعب مواكبة التكنولوجيات الناشئة وتطبيقاتها في أنشطة إرهابية محتملة.
- قلة الموارد: قد تكون الموارد (كالمال، والعمالة، والقدرات التكنولوجية) المتاحة لإجراء تقييمات للتهديدات محدودة.
- يمكن لحجم الدولة وتعقيدها ونضج قدراتها في مكافحة الإرهاب أن يؤثر أيضا في قرار الدولة حول كيفية تقييم التهديدات والمخاطر لديها وفهمها.

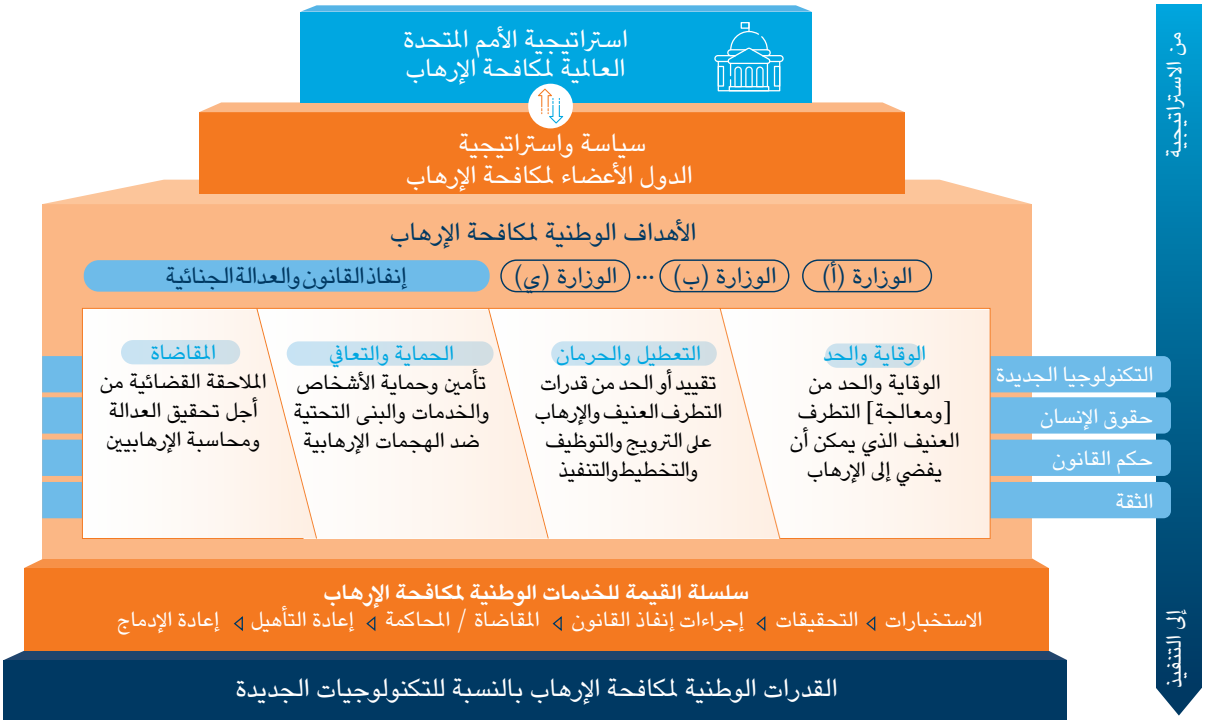
[ثانيا]
النهج

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

تم تطوير هذا الوثيقة وإثراؤها من قبل مجموعة واسعة من المدخلات التي تشمل وثائق مشروع تكنولوجيا مكافحة الإرهاب، واستشارات أصحاب المصلحة، والتحليل الداخلي، والأبحاث المكتبية، ولقاءات مجموعات الخبراء، والتنسيق مع كيانات اتفاق الأمم المتحدة العالمي لتنسيق مكافحة الإرهاب، والإطار التوجيهي الوارد أعلاه في الفرع 2-2. تركز البحث والتشاور مع أصحاب المصلحة والخبراء على تحديد منهج فعال لتقييم التهديدات والاستجابة، فضلاً عن السبل التي تمكن هذه المنهجية من معالجة أشكال التهديد التي يفرضها استغلال التكنولوجيا الجديدة أو تلك التي يمكن دعمها باستخدام التكنولوجيا الجديدة من قبل الممارسين في التصدي للتهديدات.

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 Canada, Public Safety. "Canada's National Terrorism Threat Levels." Consultations, August 25, 2016. https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html.

4 Canadian Centre for Cyber Security. An Introduction to the Cyber Threat Environment 2023-2024. Communications Security Establishment of Canada, 2022. https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment.

5 Centre for Terror Analysis (CTA). "Assessment of the Terrorist Threat to Denmark." Denmark: Centre for Terror Analysis (CTA), March 2022. https://politi.dk/en/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-terrortruslen-mod-danmark/vtd_2022_uk.pdf.

6 CIVI.POL Conseil and Royal United Services Institute. "Operational Guidelines on the Preparation and Implementation of EU Financed Actions Specific to Countering Terrorism and Violent Extremism in Third Countries." European Commission, 2018. https://issat.dcaf.ch/sqi/download/131230/2684696/EU-CT-CVE-guidelines.pdf.

7 Cole, Mara. "Towards Proactive Airport Security Management: Supporting Decision Making through Systematic Threat Scenario Assessment." Journal of Air Transport Management 35 (March 1, 2014): 12–18. https://doi.org/10.1016/j.jairtraman.2013.11.002.

8 Coordination Unit for Threat Analysis (CUTA). "The Common Database (CDB)." Accessed April 23, 2023. https://cuta.belgium.be/the-common-database-cdb/.

9 Coordination Unit for Threat Analysis (CUTA). "The Strategic Note Extremism and Terrorism (Strategy T.E.R.)." Accessed April 23, 2023. https://cuta.belgium.be/action-plan-against-radicalism-plan-r/.

10 Erez Magen, and R. "Enabling Advancements in Security-Danger and Opportunities." Maarachot (Systems) (blog), March 29, 2022. https://www.maarachot.idf.il/2022.

11 European Commission. Security by Design: Protection of Public Spaces from Terrorist Attacks. Luxembourg: European Union, 2022.

12 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.

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

14 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.

15 Financial Action Task Force (FATF). "National Money Laundering and Terrorist Financing Risk Assessment." Financial Action Task Force (FATF), February 2013. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/National_ML_TF_Risk_Assessment.pdf.coredownload.pdf.

16 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.

17 Hemmingsen, Ann-Sophie. "An Introduction to the Danish Approach to Countering and Preventing Extremism and Radicalization." Copenhagen, Denmark: Danish Institute for International Studies, 2015. https://www.ft.dk/samling/20151/almdel/reu/bilag/248/1617692.pdf.

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

19 International Organization for Standardization. ISO 31000 Risk Management-Guidelines. Second. Switzerland: International Organization for Standardization, 2018. https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf.

20 Lotz, Volkmar. "Threat Scenarios as a Means to Formally Develop Secure Systems." In Computer Security — ESORICS 96, edited by Elisa Bertino, Helmut Kurth, Giancarlo Martella, and Emilio Montolivo, 242–65. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996.

21 Ministry of Justice of Sweden. Prevent Pre-empt Protect: The Swedish Counter-Terrorism Strategy. Sweden: Government Offices of Sweden, 2014. https://www.government.se/contentassets/b56cad17b4434118b16cf449dbdc973d/en_strategi-slutlig-eng.pdf.

22 National Coordinator for Security and Counter-terrorism. "NCTV's Terrorist Threat Assessment: Threat in and to the Netherlands Has Become More Multifaceted and Diffuse – News Item – National Coordinator for Security and Counter-terrorism." Ministry of Justice and Security: National Coordinator for Security and Counter-terrorism. Ministry of Justice and Security, November 7, 2022. https://english.nctv.nl/latest/news/2022/11/07/nctvs-terrorist-threat.

23 National Coordinator for Security and Counter-terrorism. "Terrorist Threat Assessment Netherlands." Ministry of Justice and Security: National Coordinator for Security and Counter-terrorism. Ministry of Justice and Security, May 14, 2020. https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands.

24 Neil J. Smelser. "Motivation, Social Origins, Recruitment, Groups, Audiences, and the Media in the Terrorism Process." In The Faces of Terrorism: Social and Psychological Dimensions, 92–119. Science Essentials. Princeton, N.J.: Princeton University Press, 2007. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,sso&db=e000xww&AN=286616&authtype=sso&custid=s5903540&lang=he&site=eds-live&scope=site&authtype=ip,sso&custid=s5903540.

25 New Zealand Security Intelligence Service. "Combined Threat Assessment Group." New Zealand Security Intelligence Service. Accessed April 23, 2023. https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/combined-threat-assessment-group/.

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

27 New Zealand Security Intelligence Service. "National Terrorism Threat Level." Accessed April 23, 2023. https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/national-terrorism-threat-level/.

28 New Zealand Transport Agency. "Risk Register." Government. Waka Kotahi NZ Transport Agency. Accessed March 31, 2023. https://www.nzta.govt.nz/roads-and-rail/rail/operating-a-railway/risk-management/risk-register/.

29 ProtectUK. "Threat Levels," March 12, 2022. https://www.protectuk.police.uk/threat-levels.

30 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.

Security Service MI5. "Joint Terrorism Analysis Centre." Accessed April 23, 2023. https://www.mi5.gov.uk/joint-terrorism-analysis-centre. 31

Shacklett, Mary E. "What Is Attack Vector?" Tech Target, April 2021. https://www.techtarget.com/searchsecurity/definition/attack-vector. 32

Strachan-Morris, David. "Threat and Risk: What Is the Difference and Why Does It Matter?" Intelligence and National Security 27, no. 2 (April 1, 2012): 172–86. https://doi.org/10.1080/02684527.2012.661641. 33

Thorne, David. "National Level Threat Assessment-Canadian Model." 2nd Workshop on Proactive Approach to Counter Terrorism-Report. Islamabad, Pakistan: United Nations Office of Drugs and Crime, April 12, 2018. https://www.unodc.org/documents/pakistan//Report-2nd-Workshop-Proactive-Approach-to-CT-web.pdf. 34

UKC3. "Cyber Cluster Operating Framework." UK Cyber Cluster Collaboration (blog). Accessed March 29, 2023. https://ukc3.co.uk/cyber-cluster-operating-framework/. 35

United Nations Counter-Terrorism Centre and United Nations Interregional Crime and Justice Research Institute. "Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes." Joint Report. United Nations, 2021. https://www.un.org/counter-terrorism/sites/www.un.org.counter-terrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.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 Office on Drugs and Crime. Guidance on the Preparation and Use of Serious and Organized Crime Threat Assessments: The SOCTA Handbook. New York, NY: United Nations, 2010. https://www.unodc.org/documents/organized-crime/SOCTA_Handbook.pdf. 38

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. 39

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. 40

United States Department of State. "About Us: Global Engagement Center." Accessed April 23, 2023. https://www.state.gov/about-us-global-engagement-center-2/. 41

Waitzman, Eren. "National Risk Register: Preparing for National Emergencies." UK Parliament: House of Lords Library, December 14, 2022. https://lordslibrary.parliament.uk/national-risk-register-preparing-for-national-emergencies/. 42

[ثالثا]
مقدمة

3 – 1 لمحة عامة

مع استمرار التقدم في التكنولوجيا، يقوم الإرهابيون باستغلال هذه الابتكارات بشكل متزايد لتعزيز أجنداتهم التدميرية. ويشكل الانتشار السريع لمنصات الاتصال، وشبكات التواصل الاجتماعي، وتكنولوجيات التشفير، والتكنولوجيات الناشئة، تحديات جمة أمام سلطات إنفاذ القانون. ولمواجهة هذه التهديدات بفعالية، من الضروري إجراء تقييمات شاملة للتهديدات تشمل تحليلا متعدد الأبعاد للمخاطر والثغرات والآثار المحتملة والمرتبطة باعتماد الإرهابيين للتكنولوجيا الجديدة. يمكن لسلطات إنفاذ القانون، من خلال فهم تفاصيل هذه العلاقة المعقدة، تطوير استراتيجيات استباقية ووضع إجراءات ملائمة للتخفيف من التهديدات الناجمة عن استغلال الإرهابيين للتكنولوجيات الناشئة.

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[14]، أكثر من 93 في المائة هم من مستخدمي وسائل التواصل الاجتماعي[15]. ويُقدر عالميًا أنه قد تم إنشاء أكثر من 97 زيتابايت[16] من المعلومات في عام 2022[17]. 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.

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.

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

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

16 الزيتابايت يساوي مليار تيرابايت.

17 ستاتيستا، Total data volume worldwide 2010-2025 | Statista.

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[18]. 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[19]. 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[20]. 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 المائة 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[21].

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.

18 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.

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

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

21 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]
تقييم التهديدات والمخاطر

4 – 1 لمحة عامة

عند القيام بجهود مكافحة الإرهاب، من المهم التمييز بين تقييم التهديدات وتقييم المخاطر. يُمثل اجتماع هاتين الممارستين الأساس لأصحاب المصلحة والممارسين للرد بفاعلية على المخاطر المحتملة ضمن مناطق مسؤوليتهم. يصف التهديد بشكل أساسي "من" هي الجهات المهددة و "ما" هي أعمالها المزمعة. أما المخاطر فتصف مدى احتمالية وقوع التهديد وما الأضرار المحتملة لهذا العمل[22]. وبناءً على ذلك، فإن تطبيق عملية تقييم المخاطر يمكن بناؤه وتنفيذه من خلال إنشاء أساس قائم على تقييم التهديد[23].

يمثل تقييم التهديد العنصر الأول في هذا الدورة. فالتهديد هو نتاج للقدرة والنية[24]. وتشمل القدرة الإمكانيات المعروفة للمجموعة، والموارد اللوجستية، وقدرة القيادة والتحكم، ومعدل نجاح الهجمات السابقة، وتعقيد الهجمات السابقة، ومستوى التدريب، وأي معلومات متوفرة عن القدرات التي تحاول الجماعة اكتسابها[25]. في سياق جهود مكافحة الإرهاب المتعلقة باستغلال التكنولوجيا الجديدة من قبل الجهات الإرهابية، تشمل القدرة أنواع التكنولوجيا الجديدة المتاحة للجهة المهددة ومدى قدرتها على تشغيل أو توظيف التكنولوجيات. أما المقصود بالنية هنا فهو قياس للإرادة والفرصة لدى الجهة المهددة للقيام بهجوم[26].

يقول الكاتب إنه، عند تحديد مخاطر التهديدات المختلفة، يتوجب تقييم الاحتمالية (متضمنة كلا من الارجحية والتكرار) لحدوث الهجوم والضرر الذي قد يتسبب به[27]. يمكن فهم الضرر، في سياق التكنولوجيا الجديدة، على أنه يشمل كلا من الضرر المادي (سواء كنتيجة مباشرة لهجوم أو كتأثير متبق للضرر على النظام) أو الضرر بالنظام (على سبيل المثال، الهجمات الإلكترونية المختلفة التي يمكن أن تتسبب في فقدان البيانات أو تسربها، أو تعطل النظام، أو تعطيل عمل البنية التحتية الحيوية، الخ)[28].

من الضروري أيضًا النظر في تضمين منظورات النوع الاجتماعي في التخطيط والجمع والتحليل والنشر لتقييم التهديد ومنتجات الاستخبارات، لدعم تحديد علامات عدم الاستقرار التي تم تجاهلها، بالإضافة إلى التغلب على أي تحيزات محتملة تجاه النوع الاجتماعي، وتطوير فهم شامل للسياقات والديناميات الاجتماعية[29]. كما يمكّن دمج أبعاد النوع الاجتماعي في كافة مراحل دورة الاستخبارات، من توقع وتخفيف أي عواقب سلبية محتملة لجمع المعلومات الاستخبارية ونشرها على حقوق الإنسان للمتأثرين.

22 ديفيد ستراشان-موريس، "التهديد والمخاطر: ما هو الفرق وما أهميته؟"، الاستخبارات والأمن القومي 27، رقم. 2 (1 نيسان/أبريل 2012): 86-172، https://doi.org/10.1080/02684527.2012.661641.

23 ستراشان-موريس، 180.

24 المرجع نفسه، 174.

25 المرجع نفسه.

26 المرجع نفسه، 173.

27 المرجع نفسه، 173 و180.

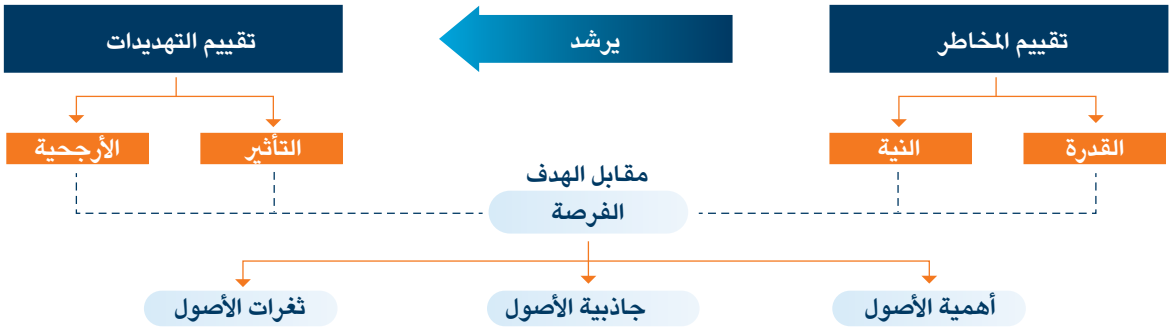
28 المرجع نفسه، 180.

29 لورين هوتون وآخرون، الذكاء والنوع الاجتماعي، (منظمة الأمن والتعاون في أوروبا، 2019).

وبالتالي، فإن منظورات النوع الاجتماعي أساسية للحصول على معلومات دقيقة وقابلة للتنفيذ، فضلا عن ضمان توافق عمليات الاستخبارات مع المعايير الدولية لحقوق الإنسان والمساواة بين الجنسين.

يوضح الرسم البياني أدناه تقييم التهديدات وتقييم المخاطر والاختلافات وطرق التفاعل بينهما:

الشكل 4



تقييم التهديدات والمخاطر هو عملية تقييم للتهديدات المحتملة من خلال تحديد هذه التهديدات وتقييم احتمالية حدوثها والتأثير المحتمل لها بهدف تطوير استراتيجيات وسياسات للتخفيف من المخاطر المرتبطة بها أو إدارتها. تشمل عملية تقييم التهديدات والمخاطر تحديد التهديدات وتحليلها استنادا إلى نية الجهات المهددة وقدرتها على ارتكاب عمل إرهابي. ستشكل نتائج تقييم التهديد الأساس الذي تبنى عليه الخطوات الأخرى في الدورة، حيث توفر فهما أوليا للتهديد الإرهابي المحتمل.

يستخدم تقييم التهديدات لفهم التهديدات المحتملة تجاه الأفراد والمنظمات و/أو الدول الأعضاء من خلال النظر في عوامل مثل الجهة المهددة (أيديولوجيتها، وقدراتها، ونواياها) والأهداف المحتملة. وهو يسهم في تطوير خيارات السياسات والاستجابات، ويشكل مكونا أساسيا في تنفيذ جهود مكافحة الإرهاب، حيث يوفر لصنّاع السياسات وغيرهم من أصحاب المصلحة المعنيين فهما أعمق للتهديدات القائمة، فضلاً عن أنواع الموارد التي قد تكون مطلوبة لمعالجة هذه التهديدات. أحد الأمثلة على ذلك هو الطريقة التي يمكن من خلالها استخدام تقييمات التهديدات للتعرف على استخدامات التكنولوجيا الجديدة من قِبل الجهات الإرهابية، أو كيف يمكن استخدام التكنولوجيا الجديدة كمورد للاستجابة للتهديدات الجديدة. وضمن سياق فهم استخدام التكنولوجيا الجديدة لأغراض إرهابية، تمكِّن تقييمات التهديدات الدول الأعضاء من فهم التهديدات المحتملة التي قد تنشأ، فضلاً عن التعامل مع التهديدات القائمة التي تتطلب اهتماما بدرجات متفاوتة من خلال عملية تحديد أولويات التهديد.

توفر تقييمات التهديدات والمخاطر إجراءات لتطوير فهم شامل للتهديدات وإجراءات الأمان، والخطط المحتملة أمام صناع القرار لمكافحة تلك التهديدات. ستقدم كل من الأقسام التالية شرحا للمكونات الرئيسية اللازمة من أجل صياغة تقييم التهديدات والمخاطر. وستشمل تقييم التهديد، بالإضافة إلى سيناريوهات التهديد، وتقييم الجهة المهددة وسيناريو التهديد، وتحديد أولويات المخاطر، والاستجابة للتهديد، وتقييم الأثر لخطة الاستجابة بالمكونات السابقة.

تصف الأقسام التالية منهجية لتقييم التهديدات والمخاطر والاستجابة لها، بالإضافة إلى الموارد الخاصة بالممارسات الجيدة في مجال تقييم التهديدات والمخاطر كما تم تنفيذها في الدول الأعضاء والمنظمات الدولية.

4 – 2 دورة إدارة التهديدات والمخاطر

الشكل 5

إن دورة إدارة التهديدات والمخاطر المطروحة أعلاه هي عملية منظمة تهدف إلى تقييم التهديدات المحتملة لبلد ما على المستوى الوطني. وتتضمن سلسلة من المراحل التي يتم اتباعها لتقييم التهديدات المحتملة والمخاطر التي تشكلها تلك التهديدات والتخفيف منها. يشير "الأفق" في دورة إدارة التهديدات والمخاطر إلى الإطار الزمني الذي يتم فيه تقييم التهديدات المحتملة وإدارة مخاطرها. وفي حال تم اعتبار تطور التكنولوجيات الجديدة جزءا من تقييمات التهديدات والمخاطر، قد يكون لها أفق أطول يمتد إلى فترة تتراوح بين عامين إلى خمسة أعوام.

يتكون إطار نموذج تقييم التهديدات والمخاطر لاستخدام التكنولوجيات الجديدة لأغراض إرهابية من مجموعة من المراحل المتعددة، تشكل معا دورة إدارة التهديدات والمخاطر. وتتضمن تقييم التهديدات، وتطوير سيناريوهات التهديدات، وتقييم الجهات والسيناريوهات، وتحديد أولويات المخاطر، والاستجابة للتهديدات، وتقييم التأثير.

4 - 2 - 1 تقييم الجهة المهددة

الشكل 6

هناك عدة عوامل ظرفية تجب دراستها عند إجراء تحليل للجهات المهددة، من هذه العوامل مقاييس النية والقدرة. حيث تشير النية هنا إلى مزيج من الرغبة والثقة لدى الجهة المهددة. أما قدرة الجهة المهددة فهي تشير إلى الموارد المتاحة لديها (المالية، والتكنولوجية، والقوى العاملة، إلخ)، والمهارات أو المعارف التي تمتلكها لتوظيف مواردها.

ولفهم مفهوم النية أثناء تحليل الجهة المهددة، من المهم أيضا إدراك أن النية (أو الدافع) ليست عنصرا موحدا، بل تتألف من عوامل متعددة تدفع الجهة المهددة لارتكاب هجوم[30]. يعرف الدافع لارتكاب هجوم لدى الجهة المهددة بـ "إثارة حالة من الرعب بين العامة أو مجموعة من الأشخاص أو أشخاص معينين، أو تخويف السكان أو إجبار الحكومة أو منظمة دولية على القيام بفعل معين أو الامتناع عن فعله، بما يشكل جرائم ضمن نطاق الاتفاقيات والبروتوكولات الدولية المتعلقة بالإرهاب ووفقا لتعريفها"[31]. يمكن ربط هذه الأفعال بالمظالم الكامنة المرتبطة بالقضايا الدينية أو السياسية أو الاجتماعية أو الاقتصادية، أو بمزيج منها. كما يختلف هذا

30 نيل ج. سميلسر، "الدوافع، الأصول الاجتماعية، التجنيد، الجماعات، الجماهير، ووسائل الإعلام في عملية الإرهاب"، في وجوه الإرهاب: الأبعاد الاجتماعية والنفسية، أساسيات العلوم (برينستون، نيوجيرسي: مطبعة جامعة برينستون، 2007)، 92-119، https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,sso&db=e000xww&AN=286616&authtype=sso&custid=s5903540&lang=he&site=eds-live&scope=site&authtype=ip,sso&custid=s5903540.

31 انظر قرار مجلس الأمن التابع للأمم المتحدة رقم 1566.

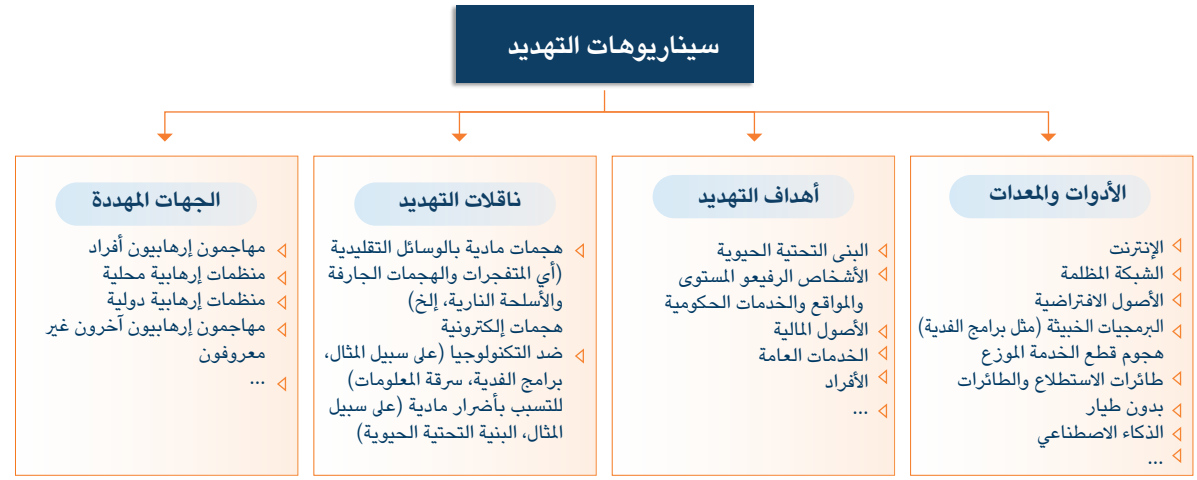
الهدف من جهة مهددة إلى أخرى[32]. ويشمل ذلك فهم الأسباب التي قد تدفع الجهة المهددة إلى الانخراط في الإرهاب، أو الدافع أو الهدف الخاص بالجهة المهددة في تنفيذ هجوم إرهابي. يمكن أن تكون هذه العوامل عقائدية، مرتبطة بالمعتقدات السياسية، أو الرغبة، أو الصحة النفسية، والتي يمكن أن تؤثر جميعها على نية الجهة المهددة لارتكاب هجوم إرهابي. على سبيل المثال، غالبا ما يكون التحيز ضد النساء قائما في السرد الذي يُستخدم لتبرير الهجمات من قبل الجماعات التي تعمل على أساس كراهية الأجانب أو العنصرية أو غيرها من أشكال عدم التسامح، أو باسم الدين أو المعتقد، كما تظهر غالبا عدم التسامح فيما يتعلق بالتوجه الجنسي والهوية الجندرية[33]. ويمكن للمحللين، من خلال تقييم نية الجهة المهددة، تحديد الأهداف المحتملة وأنواع الهجمات التي قد تخطط لها الجهة المهددة. أحد المكونات الرئيسية الأخرى لفهم النية وراء التهديد هو فهم الهدف المزمع للجهة المهددة، حيث أن الوعي بالجمهور وتأثير الهجوم على ذلك الجمهور يمكن أن يكون له تأثير كبير على الجهة المهددة والطرق التي تنفذ بها الهجوم[34].

تشير القدرة إلى الموارد والمهارات/المعارف (أو الخبرة) التي تمتلكها الجهة المهددة لتنفيذ هجوم إرهابي. ويشمل ذلك إمكانية الوصول إلى أشخاص أو منظمة، وإلى الأدوات والمعدات (مثل الوصول إلى الأسلحة و/أو التكنولوجيا)، والتدريب، ومستوى الدعم المالي أو غيره من وسائل الدعم. يمكن للممارسين، من خلال تقييم قدرة الجهة، تحديد احتمالية أن تكون الجهة قادرة على تنفيذ هجوم إرهابي ناجح.

يعتبر كل من النية والقدرة عاملا مهما في تحليل الجهات المهددة، فالجهة المهددة التي تمتلك نية قوية ولكن بقدرة محدودة قد لا تكون قادرة على تنفيذ هجوم إرهابي، بينما الجهة المهددة التي لديها قدرة قوية ولكن نيتها أضعف قد لا تتحفز للقيام بعمل. من خلال النظر في كلا العاملين، يمكن لتقييم التهديد تحقيق فهم أكثر شمولا للتهديد الذي تشكله جهة مهددة أو منظمة إرهابية معينة واتخاذ الإجراءات المناسبة لمنع تهديد الهجوم الإرهابي أو التخفيف منه.

4 - 2 - 2 وضع سيناريو التهديد

الشكل 7



32 المركز الكندي للأمن السيبراني، مدخل إلى بيئة التهديدات السيبرانية 2023-2024.

33 A/77/266.

34 نيل ج. سميلسر، "الدوافع، والأصول الاجتماعية، والتجنيد، والجماعات، والجماهير، ووسائل الإعلام في عملية الإرهاب"، 106.

الخطوة الثانية في دورة إدارة التهديدات والمخاطر هي تطوير سيناريوهات التهديد، حيث يتم تحليل المعلومات المتعلقة بالتهديدات التي تم الحصول عليها من تحليل جهات التهديد بشكل أعمق لتشمل فهم جهات التهديد، وناقلات التهديد، وأهداف التهديد، والتكنولوجيات المستخدمة في التهديد. ويعتبر تحليل جهات التهديد وسيناريوهات التهديد مفهومين مترابطين يستخدمان في كل من إدارة التهديدات والمخاطر وتخطيط الأمن. بينما يشكل تقييم التهديد عملية تحديد التهديدات المحتملة وتقييمها، فإن سيناريوهات التهديد تشكل أمثلة محددة لتلك التهديدات التي تستخدم للتخطيط والاستعداد لها. ينتج عن سيناريوهات التهديد المطورة فهم أعمق للآليات وراء هجوم محتمل، والتكنولوجيا المستخدمة في تنفيذ الهجوم، والمهاجم وراءه.

تطوير سيناريوهات التهديد ينطوي على تحديد الجهات المهددة المحتملة التي قد تستخدم التكنولوجيا الجديدة لأغراض إرهابية. ويمكن أن تشمل المجموعات الإرهابية المعروفة، والأفراد ذوي المعتقدات المتطرفة، أو غيرهم ممن قد يسعى لاستخدام التكنولوجيا لأغراض خبيثة. بعد ذلك، يجب تحليل قدرات الجهات المهددة بالإضافة إلى النظر في إمكانية وصولها إلى التكنولوجيات الجديدة وخبرتها التقنية. يمكن أن يساعد هذا التحليل في تحديد أنواع الهجمات التي قد تكون ممكنة ومستوى تعقيد تلك الهجمات. يجب بعد ذلك تحليل الثغرات المحتملة أو أنواع الهجمات التي يمكن أن تؤثر على ذلك الجزء، بما في ذلك جهات التهديد من ورائها[35].

جزء من تطوير سيناريوهات الاختبار لتقييم التهديدات والمخاطر والاستجابة لها هو تمكين أصحاب المصلحة من اتباع نهج استباقي لإدارة التهديدات. إجراء آخر يمكن لأصحاب المصلحة اتخاذه ضمن النهج الاستباقي، هو تطبيق "الأمن حسب التصميم". يشير مفهوم الأمن حسب التصميم إلى تضمين إجراءات الأمن أثناء بناء شيء ما بحيث يكون مجهزا للدفاع عن نفسه ضد التهديد ضمن هيكله/بنيته/إطاره الحالي[36]. ضمن سياق الاستجابة للتهديدات المتعلقة باستخدام التكنولوجيات الجديدة لأغراض إرهابية، يمكن أن يتخذ هذا أشكالا مثل وضع إجراءات تشغيل قياسية للاستجابة لأشكال معينة من التكنولوجيا يمكن تكييفها بسهولة لتناسب سيناريوهات متعددة.

يضم سيناريو التهديد الناتج كل تكرارات أنواع الهجمات ضد الثغرات المختلفة[37]. ضمن هذا التحليل، يعد فهم السياق و"مزيج العناصر الجوهرية المعينة"[38] أحد المكونات الرئيسية في وضع سيناريوهات التهديد. بمعنى آخر، تختلف شدة التهديد اعتمادا على عدد العناصر الجوهرية المتوفرة في سيناريو معين. عند التحضير للحماية من التهديدات، يصبح تطوير وتحليل سيناريوهات التهديد جزءا رئيسيا في منع التهديدات المستقبلية من إحداث الضرر. يصف سيناريو التهديد مثالا افتراضيا لأحداث مختلفة قد تحدث وتصمم عموما بعد تحديد التهديدات وتقييمها (القسم 4 – 2 – 1). الغرض من وضع سيناريوهات التهديد هو القدرة على التحضير للهجمات المستقبلية استباقيا والتصدي لها قبل أن تتحول إلى تهديدات خطيرة. يصف الشكل 8 أدناه عناصر كل من مكونات سيناريو التهديد[39].

35 فولكمار لوتز، "سيناريوهات التهديد كوسيلة للتطوير الرسمي للأنظمة الآمنة"، في أمان الحاسوب — المؤتمر الأوروبي حول البحث في أمن الحاسوب ESORICS 96، تحرير إليزا بيرتينو وآخرون (برلين، هايدلبرغ: سبرنجر برلين هايدلبرغ، 1996)، 250؛ مارا كول، "نحو الإدارة الاستباقية لأمن المطارات: دعم اتخاذ القرار من خلال التقييم المنهجي لسيناريوهات التهديد"، مجلة إدارة النقل الجوي 35 (1 آذار/مارس 2014): 15، https://doi.org/10.1016/j.jairtraman.2013.11.002.

36 المفوضية الأوروبية، الأمن حسب التصميم: حماية الأماكن العامة من هجمات الإرهاب (لوكسمبورغ: الاتحاد الأوروبي، 2022)، 23، https://publications.jrc.ec.europa.eu/repository/bitstream/JRC131172/JRC131172_01.pdf.

37 المرجع نفسه.

38 كول، "نحو الإدارة الاستباقية لأمن المطارات: دعم اتخاذ القرار من خلال التقييم المنهجي لسيناريوهات التهديد "، 12.

39 بالنسبة للجهات المهددة، انظر أيضا المركز الكندي للأمن السيبراني، مدخل إلى بيئة التهديد السيبراني 2023–2024، 2.

4 – 2 – 3 تقييم سيناريو التهديد وتحديد أولوياته

الشكل 8

الخطوة الثالثة في دورة إدارة التهديدات والمخاطر هي تقييم الجهة المهددة وسيناريو التهديد وتحديد أولوية المخاطر، حيث يتم فحص التهديدات والمخاطر التي تشكلها من خلال عوامل القابلية والاحتمالية والعواقب والخطورة. الهدف من هذا الجزء من الدورة هو تمكين الممارسين من فهم خطورة التهديد والمخاطر المرتبطة به حتى يتمكنوا من اتخاذ قرارات مستنيرة بشأن التهديدات التي تتطلب تخصيص موارد أكثر للاستجابة لها. نتيجة التقييم وتحديد الأولويات هي تحديد مستوى الخطورة من خلال نموذج الإشارة المرورية (الذي سيتم توضيحه أدناه)، والذي سيساعد في تحديد خيارات السياسات للاستجابة للتهديد (انظر القسم 4 – 2 – 4). يعتبر تقييم التهديد وتحديد أولوية المخاطر وسيلة للتحقق من مدى واقعية التهديد المحتمل، ويشكل عملية لتحديد التهديدات الأخطر على الدولة العضو. مما يسمح بتخصيص الموارد الوطنية اللازمة للاستجابة للتهديد أو التخفيف منه، مع الإقرار بعدم امتلاك الدول الأعضاء الموارد الكافية لمعالجة كل تهديد يتم اكتشافه. يجب تحديد أولويات التهديد من أجل تعظيم تأثير جهود الاستجابة له.

يجب أن تخضع المخاطر قبل إمكان تحديد أولوياتها، إلى تقييم يقوم الممارسون الخبراء في المجال من خلاله بتحديد عوامل مثل قابلية التهديد المطروح واحتمالية حدوث مثل هذا التهديد أو الهجوم بالفعل. ينطوي قياس قابلية هجوم محتمل على فهم نية الجهة المهددة وقدرتها، فضلاً عن التفاصيل المتعلقة بالهجوم الذي قد يتم تنفيذه. إذا لم تتطابق النية والقدرة مع الأفعال الأولية التي تؤدي إلى الهجوم، يمكن اعتبار التهديد ضعيف القابلية. وعند مناقشة احتمالية الهجوم أو أرجحيته، يجب التركيز على تحليل المخاطر المحتملة لهجوم إرهابي قد يحدث. يجب أيضا تقييم الثغرات المستهدفة داخل الدولة وتوفر إجراءات المكافحة لديها. إذا كان التهديد قابلا للحدوث ولكن الهدف ليس ضعيفًا للغاية و/أو كانت إجراءات المكافحة الموجودة بالفعل للتعامل مع التهديدات المحتملة قوية، عندها يكون التهديد الذي يتم تقييمه أقل أولوية من تهديد قابل للحدوث ولكن الهدف لا يمتلك آليات دفاعية مناسبة أو يوجد به ثغرة لم يتم التعامل معها بعد.

بعد تقييم التهديدات، يجب تحديد أولوية المخاطر التي تشكلها لضمان تطوير خطة الاستجابة وتخصيص الموارد بفعالية. وعند تحديد أولوية التهديدات والمخاطر المرتبطة بها، يجب أخذ عوامل مثل فهم عواقب التهديد في حال حدوثه وخطورة المخاطر التي يمثلها التهديد في الاعتبار. يحتاج الممارسون، من خلال فهم المخاطر التي يمثلها التهديد، إلى تقييم التأثير المحتمل للتكنولوجيا الجديدة كجزء من التهديد على نقاط البنية التحتية والخدمات والأشخاص.

جزء من التقييم الملائم للتهديد هو فهم كيفية تصنيفه بشكل أفضل لتتم الاستجابة له بكفاءة. يجب تقييم أرجحية التهديد، وتأثيره، وإجراءات التحكم به من أجل تصنيف التهديد. تشير "الأرجحية" هنا إلى أرجحية حدوث التهديد، ويشير "التأثير" إلى شدة التأثير ونطاقه. أما "إجراءات التحكم بالتهديد" فتشير إلى السياسات أو التكنولوجيا المتاحة للتصدي للتهديد. يقدم الجدول أدناه صيغة يمكن استخدامها لتقييم التهديدات وتصنيفها.

الشكل 9

التهديد	الأرجحية	التأثير	التقييم الأولي للمخاطر	إجراءات المكافحة الحالية	المخاطر المتبقية
وصف الجهة المهددة والسيناريو المحتمل الذي يتضمن الوسائل والهدف	تقييم أرجحية قيام الجهة المهددة بتنفيذ هجوم	ما هو أثر الهجوم في حال نجاحه	أحد وظائف أرجحية سيناريو التهديد وتأثيره في غياب أي إجراءات مكافحة	وصف إجراءات المكافحة الحالية وتقييمها لتخفيف التهديد	تقييم شامل للمخاطر من قبل الجهة المهددة بعد أخذ إجراءات المكافحة الحالية في الحسبان

تتضمن إحدى المكونات الإضافية في عملية تقييم التهديدات وتحديد أولوية المخاطر تقييم شدة التهديد والمخاطر المرتبطة به. عند تحديد شدة التهديد والمخاطر المرتبطة به يُوصى باستخدام نموذج الإشارة المرورية لتسهيل القدرة على تحديد أولوية التهديدات بشكل واضح.

فيما يلي نموذج توضيحي لكيفية تمييز المستويات المختلفة لشدة التهديد وكيفية تقييمها عند تحديد مستوى شدة التهديد كجزء من تقييم التهديد والمخاطر.

الشكل 10

الأرجحية \ التأثير	ضئيل	محدود	متوسط	كبير	كارثي
مرجح جدا	متوسط	مرتفع	مرتفع جدا	مرتفع جدا	مرتفع جدا
مرجح	متوسط	مرتفع	مرتفع	مرتفع جدا	مرتفع جدا
مرجح إلى حد ما	منخفض	متوسط	متوسط	مرتفع	مرتفع جدا
غير مرجح	منخفض	منخفض	متوسط	مرتفع	مرتفع
بعيد الاحتمال	منخفض	منخفض	منخفض	متوسط	متوسط

قد تتغير تصنيفات ما يُعتبر منخفضا، أو متوسطا، أو مرتفعا، أو مرتفعا جدا ويتم تحديدها من قبل صناع القرار عند تعيين العتبة، وهو ما يعرف بمصطلح "تحمل المخاطر".

عنصر آخر في تمكين صناع السياسات من التحضير الكافي للتهديدات المحتملة هو إجراء "الفريق الأحمر". يتضمن هذا الإجراء محاكاة التهديدات المحتملة بحيث يمكن للفريق المعني بالاستجابة للتهديدات ممارسة الاستجابة السليمة والتعرف على مواضع الضعف الأخرى في الاستجابة للتهديد. يتم ذلك عن طريق إنشاء "الفريق الأحمر" الذي يقوم بمحاكاة الهجوم[40]. يساعد تمرين من هذا النوع الفرق المعنية بالاستجابة على ممارسة البروتوكول السليم فيما يتعلق بالتهديدات النشطة، ويسلط في الوقت ذاته الضوء على عناصر البروتوكول التي تحتاج إلى تحسين من أجل نقل استجابة التهديد من المجال النظري إلى المجال العملي حيث يتعين استخدامها عند اكتشاف تهديد والحاجة إلى استجابة فورية.

4 – 2 – 4 الاستجابات للتهديد

الشكل 11

40 دافيد رومين ومارك كيبيل، "تخطيط الإرهابيين للهجمات: محاكاة تحقيق 'الفريق الأحمر' في صناعة القرار"، علم النفس، الجريمة والقانون 20، رقم 5 (28 أيار/مايو 2014): 483، https://doi.org/10.1080/1068316X.2013.793767.

الخطوة الرابعة في دورة إدارة التهديدات والمخاطر هي الاستجابة للتهديد، حيث يقوم الممارسون بوضع خطة عمل، ومناقشة الموارد المطلوبة اللازمة للاستجابة للتهديد، وتوزيع الأدوار والمسؤوليات على الممارسين المحددين. الهدف من هذا الجزء من الدورة هو وضع الأسس لاتخاذ إجراءات مستقبلية لمنع الضرر الناجم عن الهجوم أو تقليله. نتيجة خطوة الاستجابة للتهديد هي خطة عمل مفصلة، وقائمة بالموارد المطلوبة لتنفيذ خطة العمل، وقائمة تحدد أدوار ومسؤوليات كل من الممارسين المشاركين في خطة العمل.

يتضمن وضع خطة العمل تفاصيل حول الموارد التي سيتم تخصيصها للاستجابة للتهديد. يجب أن تكون أي استجابة للتهديد متوافقة مع مبادئ حقوق الإنسان الأساسية، بما في ذلك مبادئ الشرعية والتناسب وعدم التمييز. كما يجب أن تأخذ الاستجابة في الاعتبار أبعاد التهديد المتعلقة بالنوع الاجتماعي، لضمان تماشي الاستجابة مع الاحتياجات ونقاط الضعف الخاصة بالأجناس المختلفة. ومن الضروري أيضا لضمان استجابة فعالة للتهديد تحديد الأدوار والمسؤوليات لكل من أصحاب المصلحة لضمان أن تعمل جميع العناصر المتحركة نحو هدف متماسك، وألا تلغي خطوات أحد أصحاب المصلحة جهود الآخر.

4 – 2 – 5 تقييم التأثير

الشكل 12

يشمل تقييم التأثير تحليلا شاملا لمختلف العوامل، مثل طبيعة التهديد الإرهابي وشدته، وفعالية الإجراءات المقترحة لمكافحة الإرهاب لإضعاف قدرات التهديد، وتخفيف تأثير التهديد وتقليل الثغرات المستهدفة. يشكل تقييم التأثير عملية لتقييم وتحليل التأثيرات أو النتائج المحتملة المترتبة على سياسة مقترحة وخطة تشغيلية للتخفيف من التهديد. إنه أداة لتحديد وإدارة التهديدات المحتملة والاستجابات المرتبطة بقرار أو إجراء معين.

في هذه المرحلة، يتم تحديد الآثار وتقييمها لمراعاة الآثار المحتملة لإجراء مقترح في عمليات اتخاذ القرار ويمكن أن يساعد في ضمان الحد من أي آثار سلبية وتعظيم أي آثار إيجابية. بشكل عام، يهدف تقييم التأثير إلى تزويد صنّاع السياسات والقرارات بفهم للتأثيرات المحتملة لتقييم التهديد، مما يمكنهم من اتخاذ قرارات مستنيرة حول أفضل مسار لاتخاذه.

[خامسا]
الممارسات الجيدة في تقييم التهديدات

5 – 1 لمحة عامة

يمكن لممارسي تقييم التهديدات والمخاطر على الصعيد الوطني، من خلال تطبيق الممارسات الجيدة، تحسين جودة تقييماتهم ودقتها، وتحديد التهديدات المحتملة بشكل أفضل، واتخاذ قرارات مستنيرة بشأن التدخلات المناسبة. وقد تم الرجوع إلى مصادر متعددة متعلقة بتقييم التهديدات والمخاطر وممارسات إدارتها من مختلف الدول الأعضاء أثناء إعداد النموذج لدورة إدارة التهديدات والمخاطر. وتقدم الأقسام التالية بعض نتائج هذا البحث على شكل ممارسات جيدة. يمكن أن يتكون تقييم التهديدات والمخاطر، من حيث المبدأ، من أنواع مختلفة من التقييمات على مستويات مختلفة (محلية وإقليمية)، ويمكن دمج المستويات المختلفة معا لتشكيل فهم على المستوى الوطني لتهديدات الإرهاب، حيث يُسهم كل تقييم محدود النطاق في الصورة العامة. بالإضافة إلى ذلك، يجب أن يكون هؤلاء الممارسون على استعداد للتهديدات الناشئة عن التكنولوجيات الجديدة، التي تُستخدم أو من المحتمل أن تُستخدم كجزء أساسي من هجوم إرهابي. وعلى الرغم من أن كل نهج تتبعه كل دولة عضو قد يعتمد على إطارها الخاص بمكافحة الإرهاب، واستراتيجية مكافحة الإرهاب، والتنسيق وآلية العمل لديها، فأن هنالك بعض التوصيات للممارسات الجيدة في تقييم التهديدات والمخاطر، واعتمادها سيعود بالفائدة على ممارسي تقييم التهديدات والمخاطر المتعلقة بمكافحة الإرهاب بتحسين قدراتهم على توظيف استخدام التكنولوجيا الجديدة لأغراض إرهابية كجزء من دورة إدارة التهديدات والمخاطر (كما وردت في القسم 4).

5 – 2 النهج المتعدد الوكالات ومراكز الدمج

تتضمن عملية التقييم الفعالة للجهات المهددة وسيناريوهات التهديد التعاون بين مختلف الجهات الحكومية (بما في ذلك سلطات إنفاذ القانون، والاستخبارات، وأمن الحدود، إلخ). ويسمح تنفيذ هذه العملية كجهد متعدد الوكالات بفهم أكثر تكاملا وشمولية للتهديدات المحتملة. إحدى الممارسات الجيدة المقترحة في منشور للمفوضية الأوروبية وشركة (CIVI.POL Coseil) للخدمات الاستشارية ومعهد الخدمات الملكية المتحدة هي مفهوم رسم خريطة لأصحاب المصلحة[41]. حيث يعرّف أصحاب المصلحة المعنيون هنا على أنهم "الشركاء، والفئات المستهدفة، والمستفيدون[42]."

41 سيفي-بول للخدمات الاستشارية ومعهد الخدمات الملكية المتحدة، "توجيهات تشغيلية حول إعداد وتنفيذ الإجراءات الممولة من الاتحاد الأوروبي الخاصة بمكافحة الإرهاب والتطرف العنيف في الدول الثالثة" (المفوضية الأوروبية، 2018)، 32، https://issat.dcaf. ch/sqi/download/131230/2684696/EU-CT-CVE-guidelines.pdf.

42 المرجع نفسه.

ويشكل برنامج استراتيجية مكافحة الإرهاب (CONTEST) التابع لحكومة المملكة المتحدة إطارا يمكن من خلاله تقليل المخاطر على المملكة المتحدة من خلال مشاركة عدة وكالات حكومية[43]. في هذا البرنامج، تُحدد مستويات التهديد بشكل مستقل من قبل المركز المشترك لتحليل الإرهاب[44]. يجمع المركز بين خبرات مكافحة الإرهاب لدى الشرطة والإدارات والوكالات الحكومية، بحيث يمكن تحليل المعلومات ومعالجتها بجهود مشتركة. يعد المركز منظمة مستقلة تتألف من ممثلين عن ست عشرة إدارة ووكالة حكومية. ويصدر مستويات التهديد، وتحذيرات من التهديدات، وغيرها من المواضيع المتعلقة بالإرهاب للعملاء من مجموعة واسعة من الإدارات والوكالات الحكومية، كما يصدر تقارير أكثر تعمقا حول الاتجاهات والشبكات والقدرات الإرهابية[45].

ويعتمد نهج الدانمرك في منع التطرف العنيف والراديكالية ومكافحتهما على التعاون الواسع المتعدد الوكالات بين مختلف مقدمي الخدمات الاجتماعية، والنظام التعليمي، ونظام الرعاية الصحية، والشرطة، وخدمات الاستخبارات والأمن[46]. ينشر مركز تحليل الإرهاب تقييما سنويا للتهديد الإرهابي على الدانمرك، حيث يُحدد المستوى العام للتهديد الإرهابي في الدانمرك، ويقيم التهديد لمصالح الدانمرك في الخارج. وقد تم إنشاؤه كمركز دمج دنماركي لتحليل وتقييم إمكانية أو احتمالية التهديد الإرهابي للدنمارك ومصالح البلاد في الخارج. ويضم موظفين من أربع سلطات دنماركية (هي جهاز الاستخبارات والأمن الدانمركي، وجهاز الاستخبارات الدفاعي الدانمركي، ووزارة الشؤون الخارجية، ووكالة إدارة الطوارئ). ويعكس مستوى التهديد الإرهابي في تقييم التهديد الإرهابي للدنمارك الحالات والاتجاهات ذات التأثير المشترك على التقييم في الدانمرك وخارجها[47].

وفي نيوزيلندا، تعتبر المجموعة المشتركة لتقييم التهديد مجموعة عابرة للوكالات يستضيفها ويديرها جهاز الاستخبارات الأمنية في نيوزيلندا[48]. تقدم المجموعة تقييمات مستقلة للوكالات الحكومية حول التهديدات الموجهة نحو نيوزيلندا والنيوزيلنديين ومصالح نيوزيلندا في الخارج. وتتألف من محللين من جهاز الاستخبارات الأمنية ووكالات حكومية أخرى، بما فيها قوات شرطة نيوزيلندا، وقوات الدفاع النيوزيلندية، ومكتب أمن الاتصالات الحكومية، وهيئة الطيران المدني وخدمة أمن الطيران، وإدارة السجون. كما يتم دعم المجموعة من قبل وكالات أخرى، منها وزارة الشؤون الخارجية والتجارة، ووزارة النقل، وجمارك نيوزيلندا.

وفي كندا، يحدد مركز التقييم المتكامل للإرهاب مستوى التهديد الوطني للبلاد. ويعمل كشراكة بين الوكالات الحكومية داخل كندا والموظفين المتفرغين ضمن المركز. كما يعمل المركز بالشراكة مع هيئات تقييم التهديد في أستراليا، ونيوزيلندا، والمملكة المتحدة، والولايات المتحدة[49]. ولا يقتصر عمل النموذج هنا على الفريق الداخلي المتعدد الوكالات ولكنه يوسع جهود البلاد للتعاون مع فرق دولية، مما يمكنه من توسيع عناصر مثل نطاق جمع المعلومات الاستخبارية حول جهات مهددة معينة. كما يعتمد مركز السويد الوطني لتقييم التهديدات الإرهابية على التعاون المتعدد الوكالات بين الجيش والهيئة الوطنية للإذاعة الدفاعية وجهاز الأمن السويدي. في هذا النموذج، تعمل الوكالات معا لجمع المعلومات الاستخبارية وتحليلها وتقييم مستوى التهديد في البلاد[50].

43 المملكة المتحدة، كونتسيت: استراتيجية المملكة المتحدة لمواجهة الإرهاب (المملكة المتحدة: التاج، 2018)، https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf.

44 "المركز المشترك لتحليل الإرهاب"، جهاز الأمن MI5، تم الوصول إليه في 23 نيسان/أبريل 2023. https://www.mi5.gov.uk/joint-terrorism-analysis-centre.

45 المرجع نفسه.

46 آن صوفي هيمينسن، "مدخل إلى النهج الدانمركي لمكافحة ومنع التطرف والراديكالية" (كوبنهاغن، الدانمرك: المعهد الدانمركي للدراسات الدولية، 2015)، https://www.ft.dk/samling/20151/almdel/reu/bilag/248/1617692.pdf.

47 مركز تحليل الإرهاب، "تقييم التهديد الإرهابي للدنمارك" (الدانمرك: مركز تحليل الإرهاب، آذار/مارس 2022)، https://politi.dk/en/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-terrortruslen-mod-danmark/vtd_2022_uk.pdf.

48 جهاز الاستخبارات الأمنية النيوزيلندية، "المجموعة المشتركة لتقييم التهديدات"، جهاز الاستخبارات الأمنية النيوزيلندية، تم الوصول إليه في 23 نيسان/أبريل 2023، https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/combined-threat-assessment-group.

49 ديفيد ثورن، "تقييم التهديد على المستوى الوطني – النموذج الكندي"، ورشة العمل الثانية حول النهج الاستباقي لتقرير مكافحة الإرهاب (إسلام أباد، باكستان: مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 12 نيسان/أبريل 2018)، 87، https://www.unodc.org/documents/pakistan//Report-2nd-Workshop-Proactive-Approach-to-CT-web.pdf.

50 وزارة العدل السويدية، المنع والوقاية والحماية: الاستراتيجية السويدية لمكافحة الإرهاب (السويد: المكاتب الحكومية في السويد، 2014)، https://www.government.se/contentassets/b56cad17b4434118b16cf449dbdc973d/en_strategi-slutlig-eng.pdf.

5 – 3 النهج القائم على المخاطر

تستخدم العديد من البلدان والمنظمات الدولية نهجاً قائماً على المخاطر في تقييماتها للجهات المهددة وسيناريوهات التهديد من أجل مكافحة الإرهاب. من خلال اعتماد نهج قائم على المخاطر، يمكن للمنظمات اتخاذ قرارات مستنيرة، وتخصيص الموارد بفعالية، وإدارة المخاطر بشكل استباقي، مما يقلل من احتمالية وقوع أحداث إرهابية مؤذية ومن أثارها. في هذا النهج، يتم تقييم احتمالية الهجوم الإرهابي وتأثيره من أجل تحديد أولويات تخصيص الموارد ووضع خطط للاستجابة.

يعتبر السجل الوطني للمخاطر في المملكة المتحدة النسخة العامة من التقييم الوطني للمخاطر الأمنية، وهو التقييم السري من قبل الحكومة للمخاطر الأمنية الوطنية التي تواجه المملكة المتحدة أو مصالحها في الخارج. ويقدم معلومات للعامة حول "أهم المخاطر" التي تقدر الحكومة احتمال وقوعها والتي قد تكون لها تأثيرات واسعة النطاق على البلاد، مثل الهجمات الإرهابية أو الأحداث الطبيعية كالفيضانات. كما يوضح كيف تقوم الحكومة بتحديد حالات الطوارئ المحتملة هذه، وتقييمها، والاستعداد لها، والتعامل معها. وفي مثال آخر، يقدم نموذج لسجل المخاطر من وكالة نيوزيلندا للنقل مثالاً جيداً لأنواع المعلومات التي يجب تضمينها في سجل المخاطر لدولة ما مثل الرقم المرجعي للتهديد، وقسم يضم الوصف والتاريخ لآخر مرة تم فيها اتخاذ إجراءات ضد تهديد، والخطة المتبعة وتفصيلا للأدوار التي يجب أن يلعبها كل من أصحاب المصلحة في حال تحقق التهديد بالهجوم.

فرقة العمل المعنية بالإجراءات المالية هي هيئة حكومية مستقلة تطور السياسات وتعززها لحماية النظام المالي العالمي ضد غسيل الأموال وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل. توصي الفرقة بأن يكون النهج القائم على المخاطر لمكافحة غسيل الأموال و/أو تمويل الإرهاب جزءا أساسيا من الأسس المعتمدة في تخصيص الموارد بكفاءة. علاوة على ذلك، تشير إلى أن تقييم المخاطر الذي تقوم به الدول ينبغي استخدامه لتحديد المخاطر الأعلى والأدنى التي يمكن بعد ذلك التعامل معها عن طريق تطبيق إجراءات معززة أو السماح بتبسيط الإجراءات وفق الحاجة. كما توصي بأن تحديد مصادر البيانات ونوع المعلومات والأدوات والتقنيات التحليلية التي ستُستخدم هو أمر أساسي بالتالي لإجراء تقييمات المخاطر. ولكي يصل تقييم المخاطر الوطني إلى النتائج الأدق، من المستحسن أن يستند أكبر قدر ممكن من التحليل والاستنتاجات المقدمة ضمن التقييم إلى معلومات موضوعية. ويمكن أن تستمد المعلومات المستخدمة في تقييم المخاطر من مصادر متنوعة (سواء كانت كمية أو نوعية).

5 – 4 قياس مستويات التهديد

يشكل قياس مستوى التهديد جانبا مهما في تقييم الجهة المهددة وسيناريو التهديد وكذلك في إدارة التهديد. تُمكن قياسات مستوى التهديد الأفراد والمنظمات من تقييم مستوى التهديد المرتبط بوضع أو حدث إرهابي واتخاذ الإجراءات المناسبة للتخفيف من تلك التهديدات أو إدارتها.

يقوم المركز المشترك لتحليل الإرهاب في المملكة المتحدة[51] بقياس مستوى التهديد في أي ظرف معين بعدة عوامل، منها:

- **المعلومات الاستخباراتية المتاحة:** تستند هذه المعلومات في كثير من الأحيان إلى مجموعة واسعة من المعلومات، قد يكون بعضها مجزءا، بما في ذلك مستوى النشاط الإرهابي الحالي وطبيعته، والمقارنة بأحداث في بلدان أخرى، وبهجمات سابقة.
- **القدرات الإرهابية:** فحص لما هو معروف عن قدرات الإرهابيين والأساليب التي قد يستخدمونها استنادا إلى الهجمات السابقة أو من المعلومات الاستخباراتية. ويشمل ذلك أيضا تحليل النطاق المحتمل للهجوم.
- **النوايا الإرهابية:** استخدام المعلومات الاستخبارية والمعلومات المتاحة للعموم لفحص الأهداف العامة للإرهابيين والطرق التي قد يحققون بها تلك الأهداف بما في ذلك نوع الأهداف التي قد يفكرون في مهاجمتها.
- **الجدول الزمني:** مستوى التهديد المعبر عنه واحتمالية وقوع هجوم في المستقبل القريب.

51 "مستويات التهديد"، منصة "ProtectUK" 12 آذار/مارس 2022، https://www.protectuk.police.uk/threat-levels.

تتضمن تقييمات المجموعة المشتركة لتقييم التهديد في نيوزيلندا النظر في نية الجهة المهددة بتنفيذ هجوم، وقدرتها على تنفيذه. وتعتبر التقييمات تقديرا كميا وتحليليا. وتستخدم المجموعة تقنيات تحليلية وأدوات منظمة للمساعدة في التقييمات. وتنظر في سياق الإرهاب المحلي وعوامل التهديد الدولية ذات الصلة[52]. وتقوم بتقييم مستويات التهديد من خلال النظر في النية والقدرة الحالية للأفراد أو الجماعات على تنفيذ عمل إرهابي. ويخرج مركز التقييم المتكامل للإرهاب في كندا بدوره، منتجات لتقييم التهديد تعالج مستوى التهديد الوطني وتقيمه بالإضافة إلى المنتجات التي تقيم كيفية تحول مستوى التهديد عندما يتعلق الأمر بـ "حدث خاص" (كمؤتمر قمة على سبيل المثال)[53]. يوضح إدراج تقييمات "الأحداث الخاصة" أن مستوى التهديد (الوطني أو على نطاق أصغر وأكثر محلية) قد يرتفع عند وجود حدث بارز، ولكن هذا النوع من التحول يعتمد على طبيعة الحدث وهو مؤقت مقارنة باتساق باقي تقييمات التهديد الوطني ونطاقها. يوضح النموذج الكندي أيضا، ضمن مقياس مستويات التهديد، كيف يمكن أن يؤثر التهديد عموما على الجمهور وقدرته على الالتزام بالشروط الروتينية[54].

أحد الممارسات الجيدة التي لوحظت عند قياس مستوى التهديد هي وضع مقياس يساعد في تنظيم مستويات التهديد في البلاد. يقدم جهاز الاستخبارات الأمنية في نيوزيلندا نموذجا يتكون من خمس مستويات لتقييم مستوى التهديد تتراوح من منخفض جدا إلى شديد[55]. كما تقدم كندا وهولندا نماذج لمستويات التهديد يمكن الاستفادة منها، حيث يتم توضيح الإجراءات المتخذة في كل مستوى. في النموذج الكندي، تنقسم مستويات التهديد إلى خمس فئات: منخفض جدا، ومنخفض، ومتوسط، ومرتفع، وحرج، حيث تتراوح التهديدات من كونها غير مرجحة الحدوث إلى مرجحة جدا (وقد تكون وشيكة)[56]. ويشير النموذج الكندي منذ مراحله الأولى إلى وجود إجراءات مطبقة بالفعل لتأمين السكان وحمايتهم من هجوم محتمل. وعندما يُعتبر مستوى التهديد "متوسطا"، يتم اتخاذ إجراءات أمان إضافية. وتستمر الإجراءات الأمنية في الزيادة في كل من المستويات "المرتفعة" و"الحرجة"، كما يوجد عنصر إضافي هو التواصل مع العامة بشأن الإجراءات المحتملة التي قد يحتاجون لاتخاذها لضمان سلامتهم[57]. وكما هو حال النماذج السابقة، يعمل النموذج الهولندي على مقياس يتكون من خمس مستويات تتراوح من المستوى الأول (الحد الأدنى) إلى المستوى الخامس (الحرج)[58]. يقوم المنسق الوطني للأمن ومكافحة الإرهاب، بالإضافة إلى نشر هذا النموذج، بنشر بعض الرسوم التوضيحية خلال العام حيث يتم توضيح مستوى التهديد جنبا إلى جنب مع تفسير أسباب تعيين مستوى التهديد[59].

52 "المستوى الوطني لتهديد الإرهاب"، جهاز الاستخبارات الأمنية النيوزيلندية، تم الوصول إليه في 23 نيسان/أبريل 2023، https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/national-terrorism-threat-level.

53 ثورن، "تقييم التهديد على المستوى الوطني - النموذج الكندي"، 87-89.

54 انظر الرسم البياني في المرجع نفسه، 88.

55 "المستوى الوطني للتهديد الإرهابي".

56 هيئة السلامة العامة في كندا، "المستويات الوطنية للتهديد الإرهابي في كندا"، مشاورات، 25 آب/أغسطس 2016، https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html.

57 كندا.

58 المنسق الوطني للأمن و"تقييم التهديدات الإرهابية في هولندا"، وزارة العدل والأمن: المنسق الوطني للأمن و (وزارة العدل والأمن، 14 أيار/مايو 2020)، https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands.

59 انظر على سبيل المثال، المنسق الوطني للأمن وتقييم التهديد الإرهابي الذي أجراه المنسق الوطني للأمن ومكافحة الإرهاب: أصبح التهديد داخل هولندا وعليها متعدد الأوجه وأكثر انتشارا – مادة إخبارية - المنسق الوطني للأمن، ووزارة العدل والأمن: المنسق الوطني للأمن و(وزارة العدل والأمن، 7 تشرين الثاني/نوفمبر 2022)، https://english.nctv.nl/latest/news/2022/11/07/nctvs-terrorist-threat-assessment-threat-in-and-to-the-netherlands-has-become-more-multifaceted-and-diffuse.

الصندوق 1 – مثال من السلامة العامة في كندا – المستويات الوطنية للتهديد

مستوى التهديد*

يمثل هذا الرسم البياني مفهوم مستوى التهديد كما توضحه سياسات كندا ونيوزيلندا وهولندا. يحتوي كل نموذج من هذه النماذج على خمسة مستويات، لكن كلا منها وصف هذه المستويات بشكل مختلف. الرسم البياني الناتج هو مزيج من النماذج الثلاثة.

* **تم استخدام النماذج والصيغ لكل مرحلة من المصادر التالية:**

كندا، السلامة العامة. "المستويات الوطنية للتهديد الإرهابي في كندا". مشاورات، 25 آب/أغسطس 2016. https://www.canada.ca/en/services/defence/nationalsecurity/error-threat-level.html.

المنسق الوطني للأمن ومكافحة الإرهاب. "تقييم التهديد الإرهابي في هولندا". وزارة العدل والأمن: المنسق الوطني للأمن ومكافحة الإرهاب. وزارة العدل والأمن، 14 أيار/مايو 2020. https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands.

جهاز المخابرات الأمنية النيوزيلندية. "مستوى التهديد الإرهابي الوطني". تم الوصول إليه في 23 نيسان/أبريل 2023. https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-error/national-error-threat-level/.

5 – 5 جمع معلومات التهديد وتحليلها

يشكل وجود قاعدة قوية لعملية جمع معلومات التهديد وتحليلها جزءا أساسيا من تنفيذ تقييم فعال للجهات المهددة وسيناريوهات التهديد وإدارة التهديدات. وفيما يلي مجموعة من الممارسات الجيدة المستمدة من وثائق الدول الأعضاء بشأن جمع معلومات التهديد وتحليلها.

إحدى الممارسات الجيدة بالنسبة للممارسين فيما يخص تقييم التهديدات المرتبطة باستخدام التكنولوجيات الجديدة لأغراض إرهابية هي إجراء تحليل لاستخبارات التهديد السيبراني. ويعرفه نموذج المملكة المتحدة لتحليل استخبارات التهديد السيبراني بأنه تقييم استخباراتي للوضع يأخذ في الاعتبار كلا من التهديدات المحتملة والجهات المهددة من ورائها فيما يتعلق باستخدام التكنولوجيا وإساءة استخدامها[60]. أحد أساليب جمع هذه الاستخبارات هو استخبارات المصادر المفتوحة وهو نوع من الاستخبارات يتمتع بحكم طبيعته بإمكانية وصول أسهل بالنسبة لأصحاب المصلحة ويقدم مصادر أقل مقارنة بأنواع أخرى من الاستخبارات. ومن الممارسات الإضافية التي يمكن استخدامها في هذا النوع التعاون مع أعضاء من القطاع الخاص في شركات التكنولوجيا وفي المجال الأكاديمي لجمع البيانات المتاحة حول التهديدات المحتملة وتحليلها. ومن المهم عند إجراء هذه الاستخبارات تطوير منتجات معرفية بانتظام يتم فيها تقييم الاستخبارات المجموعة وتركيزها في تقرير بحيث يمكن لأصحاب المصلحة الحصول على تقييم للوضع لمختلف التهديدات بسهولة[61].

60 فلاندرز وآخرون، استخبارات التهديدات السيبرانية في الحكومة: دليل لصناع القرار والمحللين، 15.

61 المرجع نفسه، 36.

يشير التقرير الذي نشرته المفوضية الأوروبية، وشركة CIVI.POL Conseil للخدمات الاستشارية، ومعهد الخدمات الملكية المتحدة أيضًا إلى ممارسة جيدة لجمع معلومات التهديد وتحليلها. يسلط هذا التقرير الضوء على أهمية "تحليل السياق" الذي يجب أن يقترن بتحليل التهديد. ينطوي نهج من هذا النوع على "أخذ أي قضايا سياسية واقتصادية وأمنية وبيئية على المستويات المحلية والوطنية والإقليمية في الاعتبار[62]". وتدعم معايير أيزو 31000 أيضا نهجا مستندا إلى السياق في إدارة المخاطر[63]. وفقا لإرشاداتها، يساعد فهم السياقات "الداخلية" و"الخارجية" أصحاب المصلحة في "تخصيص" استجابتهم لمجموعة معينة وفهم طرق تأثير سياق التهديدات المعينة على المخاطر الناشئة عن التهديد[64]. يساعد استخدام هذا النهج عند صياغة تحليل لجهات التهديد وتطوير سيناريوهات التهديد أصحاب المصلحة على فهم أعمق لمشهد التهديد قبل عملية تحليل المخاطر.

5 – 6 التقييم المستمر

يجب تحديث تقييمات التهديدات والمخاطر بانتظام. فكما يمكن للجهات المهددة التطور مع مرور الوقت وظهور تكنولوجيا جديدة، يمكن للبلدان أيضا أن تنمو وتتطور من حيث طرق الاستعداد لمثل هذه التهديدات. يتم ذلك جزئيا بغرض فهم التحولات في تهديد معين نتيجة لجهود مكافحة الإرهاب أو أي تغيرات أخرى[65]. هذه العملية مستمرة، بوجود مراجعات وتحديثات منتظمة بناءً على المعلومات الاستخبارية الجديدة والظروف المتغيرة مثل تقدم التكنولوجيا. بالإضافة إلى ذلك، يجب أن تخضع منهجية تقييم التهديد وإدارته لتقييم التأثير لضمان استمرارية فعاليتها وتوافقها مع الواقع الذي تحاول فهمه.

تقوم الولايات المتحدة بتقييم الفاعلية وضبط العمليات من خلال تقييم استراتيجي سنوي مستقل يستند إلى البحث والاستخبارات والتحليل، لضمان تحقيق تقدم قابل للقياس نحو الأهداف الاستراتيجية. تحدد هذه التقييمات مواضع الضعف الاستراتيجية وتوصي بضبط الاستراتيجية للتفوق على الخصوم النشطين. كما تهدف إلى ضمان استدامة التقدم ومعالجة كامل نطاق التحديات الأمنية الوطنية المعاصرة[66]. وفقا لاستراتيجية مكافحة الإرهاب الأمريكية، يعد هذا نتاجا للبحث والاستخبارات والتحليل، حيث يستند كل تقييم إلى تقييم سابق مكتمل. إن إعداد تقرير سنوي لتقييم التهديدات يظهر طرق تغير التهديدات ويعبر عنها من خلال مستوى شدة التهديد، وطبيعة الجهة المهددة، والموارد المتاحة لها، والموارد التي تمتلكها الدولة لمواجهة التهديدات المحتملة. وفي نيوزيلندا، تتم مراجعة مستوى التهديد الوطني بشكل رسمي سنويا ولكن يمكن أيضا تغييره في أي وقت استنادا إلى الصورة الاستخباراتية الحالية.

5 – 7 تعزيز مشاركة المعلومات الاستخباراتية

تظل مشاركة المعلومات وثقافة التعاون متعددة التخصصات ومتعددة المستويات أمرا أساسيا لتقييم التهديدات بشكل محكم، الأمر الذي يمكن أن يشكل أساسًا لسياسات مكافحة الإرهاب[67]. ويشمل ذلك مشاركة الاستخبارات بين الجهات الحكومية ومع الشركاء الدوليين. ومن الضروري نشر التوعية الواسعة حول تقييم التهديدات من أجل تمكين التعاون والفهم من مصادر/كيانات متعددة

62 سيفي-بول للخدمات الاستشارية ومعهد الخدمات الملكية المتحدة، "توجيهات تشغيلية حول إعداد وتنفيذ الإجراءات الممولة من الاتحاد الأوروبي الخاصة بمكافحة الإرهاب والتطرف العنيف في الدول الثالثة،" 30.

63 المنظمة الدولية للمعايير، إرشادات إدارة المخاطر أيزو 31000، الإصدار الثاني (سويسرا: المنظمة الدولية للمعايير، 2018)، 3 و6، https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf.

64 المرجع نفسه.

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

66 المرجع نفسه.

67 المفوضية الأوروبية، أجندة مكافحة الإرهاب في الاتحاد الأوروبي: 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.

لتحقيق تأثير أوسع[68]. تركز استراتيجية مكافحة الإرهاب في إسبانيا، على سبيل المثال، على القدرة على استخدام البيانات وجعلها متاحة لمن يحتاجون إليها وحمايتها من الذين لا ينبغي أن يطلعوا على هذا النوع من المعلومات[69]. يتضمن ذلك الحاجة إلى التشفير من أجل مشاركة البيانات بين المساهمين من قطاعات مختلفة[70].

أحد الأمثلة عن الممارسات الجيدة في مشاركة المعلومات هو نموذج قاعدة البيانات المشتركة كما تمارسها وحدة التنسيق البلجيكية لتحليل التهديدات. تعمل قاعدة البيانات هذه كوسيلة تسمح لجهات حكومية مختلفة بالوصول إلى البيانات وإضافتها حول الفئات التالية: المقاتلون الإرهابيون الأجانب، والمقاتلون الإرهابيون المحليون، والمروجون للكراهية، والمتطرفون الذين من المحتمل أن يكونوا عنيفين، والأشخاص المدانون بالإرهاب[71].

يجب أن تتم مشاركة المعلومات بين أصحاب المصلحة في مواقع مختلفة من خلال وسيلة آمنة لتمكين أصحاب المصلحة من الحفاظ على الأمن التشغيلي في مسائل مثل تقييم الجهة المهددة والاستجابة للتهديدات. وكما هو حال النموذج الإسباني يعتمد نموذج قاعدة البيانات المشتركة في مشاركة المعلومات الآمنة على مبدأ "الحاجة إلى المعرفة"، مما يعني أن المستخدمين يمكنهم الوصول إلى كميات مختلفة من البيانات (ولديهم القدرة على المساهمة) استنادًا إلى نوع المعلومات ذات الصلة بدورهم الخاص[72]. من خلال تنظيم نوعية وكمية المعلومات المتاحة في قاعدة البيانات للمستخدمين المختلفين، يتم الحفاظ على مستوى أعلى من الأمن التشغيلي، مما يقلل بالتالي من إمكانية وصول المعلومات إلى المستخدمين الذين لا ينبغي أن يطلعوا عليها.

طريقة أخرى يمكن من خلالها مشاركة هذا النوع من سجل/قاعدة البيانات والمعلومات المرافقة له بطريقة آمنة هي من خلال اعتماد نموذج مشابه لنموذج "الكتلة" المتبع في المملكة المتحدة. يعد نموذج "الكتلة" وسيلة للتعاون الإقليمي العابر للقطاعات بين السلطات الحكومية وشركات القطاع الخاص والأوساط الأكاديمية. ضمن هذا النموذج، تملك كل منطقة "كتلة" تعمل بشكل شبه مستقل فيما يتعلق بتحديد أولويات التهديد الأكثر ملاءمة لمجال مسؤوليتها المحدد. ويتشارك أصحاب المصلحة ضمن كل كتلة المعلومات والممارسات الجيدة. هنا، تشارك الكتل في عملية تمركز من خلال إعداد التقارير ومشاركة المعلومات في نهاية المطاف مع أصحاب المصلحة المحليين فيما يتعلق بالتهديدات[73]. تقدم المذكرة الاستراتيجية البلجيكية لمكافحة التطرف والإرهاب (استراتيجية T.E.R) نموذجًا مماثلاً لوجود ممارسين محليين يعملون في مجال جهود مكافحة الإرهاب. يمتلك هذا النموذج فرقة عمل محلية ويستخدم أيضًا فريقًا محليًا يتناول منع التطرف[74]. ترفع هذه المستويات المحلية تقاريرها إلى فريق العمل الوطني، الذي يتعاون على نطاق أوسع مع مختلف الوكالات الحكومية والعسكرية. طبيعة النموذج المحلي تمكّن من اعتماد نهج أكثر دقة في تقييم التهديدات وتحديد الأولويات فيما يتعلق بمنطقة المسؤولية، مع تمكين أصحاب المصلحة على المستوى الوطني من فهم معمق لكل من المناطق الواقعة ضمن نطاق مسؤوليتهم.

من المهم أيضًا، بالنسبة إلى مشاركة المعلومات، تسهيل عملية الإبلاغ عن المعلومات، خاصة بالنسبة للأفراد من العامة الذين يرغبون في الإبلاغ عن معلومات حرجة تتعلق بالتهديدات. ومن أجل تحقيق ذلك، يجب أن يكون العامة على علم بالسلوكيات أو الأفعال التهديدية، والقنوات التي يمكنهم اللجوء إليها للإبلاغ عن حادث ما لتتم معالجته من قبل الجهات المعنية التي تم تدريبها لذلك.

يمكن تحقيق ذلك من خلال التدريب في المدارس وأماكن العمل للتعرف على علامات السلوكيات التهديدية. بالإضافة إلى ذلك، يجب أن يكون النظام الذي يمكن للعامة مشاركة معلومات حول التهديدات من خلاله سهل الوصول والاستخدام لتجنب عدم التبليغ

68 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-management- practices-across-the-world/.

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

70 المرجع نفسه.

71 "قاعدة البيانات المشتركة"، وحدة التنسيق لتحليل التهديدات، تم الوصول إليها في 23 نيسان/أبريل 2023، https://cuta.belgium.be/the-common-database-cdb/.

72 المرجع نفسه.

73 UKC3، "الإطار التشغيلي للكتلة السيبرانية"، تعاون الكتلة السيبرانية في المملكة المتحدة (مدونة)، تم الوصول إليها في 30 آذار/مارس 2023، https://ukc3.co.uk/cyber-cluster-operating-framework/.

74 "المذكرة الاستراتيجية للتطرف والإرهاب (استراتيجية T.E.R.)"، وحدة التنسيق لتحليل التهديدات، تم الوصول إليها في 23 نيسان/أبريل 2023، https://cuta.belgium.be/action-plan-against-radicalism-plan-r/.

بسبب صعوبته. أحد الأمثلة على موقع يعمل كنموذج مركزي وسهل الاستخدام للإبلاغ عن التهديدات هو موقع في نيوزيلندا، حيث يمكن للعامة تقييم درجة خطورة معلومات التهديد ومشاركتها مع الجهات المعنية[75]. كما يوفر هذا الموقع الفرصة للأفراد لتقديم المعلومات دون الكشف عن هويتهم.

5 – 8 البحث والابتكار

يشير الواقع الحالي إلى أن التكنولوجيا الحديثة تتطلب استجابة فعالة تتوقع كيفية تأثير التكنولوجيا على تهديد الإرهاب، لتزويد سلطات إنفاذ القانون بالأدوات المناسبة. ويشكل البحث والابتكار جزءا جوهريا من إجراء تقييمات التهديد ومعرفة كيفية الاستجابة السليمة للتهديدات التي تستخدم التكنولوجيا الجديدة أو التهديدات الناتجة عن استغلال التكنولوجيا الجديدة، حيث يضمن أن يكون لدى الممارسين فهم محدث للتهديدات المحتملة، وقدرة مستمرة على تطوير وسائل جديدة للاستجابة لهذه التهديدات. لذلك توصي المفوضية الأوروبية وشركة سيفي-بول للخدمات الاستشارية ومعهد الخدمات الملكية المتحدة بأهمية الجهود المبذولة نحو الفهم المستمر للتطورات التكنولوجية وتأثيرها المحتمل عند استغلالها من قبل الجهات الإرهابية، كجزء مهم في فهم سيناريوهات التهديد (انظر القسم 4 – 2 – 2)[76]. ينبغي أن يشمل هذا البحث والابتكار الجهود العابرة للوكالات والقطاعات كما ينبغي أن يتضمن مساهمات من الأكاديميين بالإضافة إلى قطاع التكنولوجيا.

تركز الأبحاث الأمنية الأوروبية على بناء مبادرات تهدف إلى تعزيز قدرة سلطات إنفاذ القانون في مجالات مثل تطوير حلول تحليلية تهدف إلى التعامل مع البيانات الضخمة[77]. كما يهدف البحث الأمني الممول من الاتحاد الأوروبي إلى تعزيز قدرة الكشف المبكر عن التهديدات الإرهابية المحتملة، لا سيما من خلال استكشاف استخدام الذكاء الاصطناعي للسماح بمعالجة الكميات الضخمة من البيانات بشكل أكثر فاعلية ودقة. بالإضافة إلى ذلك، وفي إطار برنامج البحث المستقبلي التابع لبرنامج هورايزن أوروبا، يتم دمج الأبحاث بشكل أعمق في دورة سياسات الأمن لضمان مخرجات موجهة نحو التأثير، بما يستجيب لاحتياجات إنفاذ القانون المحددة[78].

75 "كيف يمكنك المساعدة: نموذج المساهمة العامة"، جهاز الاستخبارات الأمنية النيوزيلندي، تم الوصول إليه في 23 نيسان/أبريل 2023، https://providinginformation.nzsis.govt.nz/.

76 سيفي-بول للخدمات الاستشارية ومعهد الخدمات الملكية المتحدة، "توجيهات تشغيلية حول إعداد وتنفيذ الإجراءات الممولة من الاتحاد الأوروبي الخاصة بمكافحة الإرهاب والتطرف العنيف في الدول الثالثة،" 30.

77 المفوضية الأوروبية، أجندة مكافحة الإرهاب في الاتحاد الأوروبي: التوقع والمنع والحماية والاستجابة.

78 انظر على سبيل المثال مشروعي DANTE وTENSOR ("كشف وتحليل المحتويات والأنشطة التمويلية المتعلقة بالإرهاب على الإنترنت"، المفوضية الأوروبية: خدمة معلومات البحث والتطوير المجتمعي Cordis, 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: Cordis، تم الوصول إليه في 23 نيسان/أبريل 2023، https://cordis. europa.eu/project/id/700024).

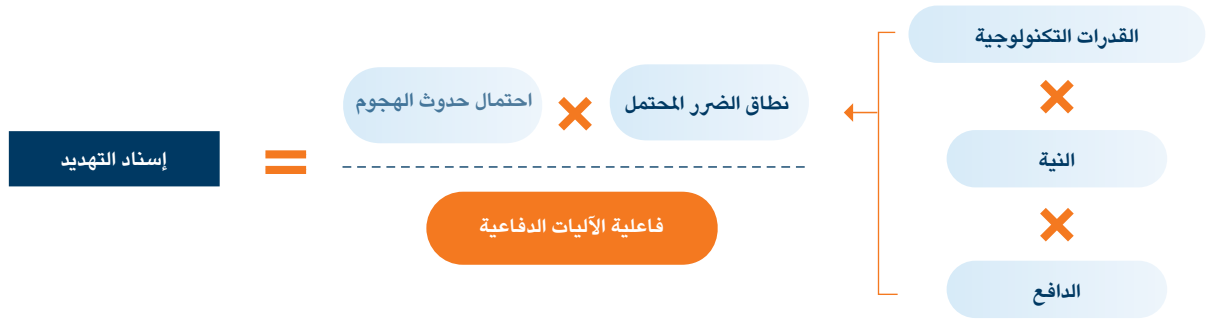
[الملحق أ]
معادلة نموذجية توضيحية لإسناد التهديد

أ - 1 لمحة عامة

يوضح الشكل أدناه نموذجا يمكن من خلاله للممارسين تقييم إسناد التهديد بالنسبة لتهديد معين. ويشير إسناد التهديد هنا إلى تقييم المخاطر بناءً على تقييم للتهديد نفسه[79]. يركز النموذج المقدم هنا على كيفية تقييم القدرات. ونظرا لتركيز هذا الدليل على التكنولوجيات الجديدة، تم تعديل العامل الأولي وهو "المعلومات والمعرفة والفرصة" الذي يصف "القدرة" بشكل عام ليصبح "القدرات التكنولوجية"[80].

وفقًا للنموذج المعروض في الشكل، يجب أن تؤخذ القدرات التكنولوجية والنية والدافع للجهة المهددة في الاعتبار أولا، حيث تنعكس نتيجة ذلك على تحليل احتمالية حدوث الهجوم ونطاق الضرر المحتمل الذي قد يسببه. بعد هذه الخطوة، يقيم الممارسون أنواع الدفاعات التي يمتلكونها ومدى فعالية تلك الدفاعات ضد التهديد المحتمل[81]. يؤثر فهم القدرات المتاحة في التصدي للتهديد على إسناد التهديد. كلما كانت الإجراءات المتوفرة لدى الدولة للتصدي للتهديدات أكثر فاعلية، كلما كان إسناد التهديد أقل.

الشكل[82]



79 إيريز ماجن و ر.، "تمكين التقدم في المخاطر والفرص الأمنية"، معراشوت (الأنظمة) (مدونة)، 29 آذار/مارس 2022، https://www.maarachot.idf.il/2022/.

80 المرجع نفسه.

81 المرجع نفسه.

82 الرسم مترجم ومقتبس من إيريز ماجن ور.، "تمكين التقدم في المخاطر والفرص الأمنية".

[الملحق ب]
مثال على إساءة استخدام التكنولوجيا من قبل الإرهابيين

ب - 1 لمحة عامة

يسلط الجدول أدناه الضوء على التكنولوجيات الجديدة وإمكانية استغلالها من قبل الجهات الإرهابية، وكذلك إمكانية استخدامها من قبل الممارسين للتصدي للإرهاب. إن فهم طرق استخدام التكنولوجيا الجديدة للاستجابة للإرهاب يمكن أن يُعلم الممارسين بدمج هذه الاستخدامات كجزء من سياسات الاستجابة للإرهاب.

من المهم الإشارة إلى أنه في حين كون الجدول دقيقا عند إعداد هذا التقرير، يجب تقييم محتوى الجدول بانتظام لضمان استمرار دقته وصلته بالواقع لمن يستخدمونه. فنظرا للتطور المستمر للتكنولوجيات الجديدة، ستكون هنالك دائما طرق جديدة تمكن الإرهابيين من استغلال التكنولوجيا لأغراض شريرة، كما ستكون هنالك أيضا طرق جديدة لاستخدام التكنولوجيا للتصدي للإرهاب.

الجدول - أمثلة توضيحية

نوع التكنولوجيا	الاستخدام لأغراض شريرة من قبل الإرهابيين	استخدام سلطات إنفاذ القانون للتصدي للإرهاب
الإنترنت	• التجنيد في التنظيم الإرهابي من خلال الدعاية المنتشرة على شبكة الإنترنت • نشر المعلومات عبر الإنترنت حول كيفية تنفيذ الهجمات الإرهابية[83] • تمويل الإرهاب • التطرف إلى الإرهاب • جمع المعلومات الاستخبارية حول الأهداف المحتملة للهجمات • انتشار المحتوى الإرهابي والروايات المشوهة • التواصل والتنسيق ودعم الأعمال أو الأنشطة الإرهابية • التمكين السيبراني لعمليات المعلومات	• مكافحة التطرف العنيف والخطابات الإرهابية[84] • جمع استخبارات المصادر المفتوحة وتحليلها • منصة لتبادل المعلومات لأصحاب المصلحة • تحديد المحتوى الإرهابي على الإنترنت ووقف نشره • فرق الإحالة التي تبلغ عن المحتوى المتطرف إلى شركات التكنولوجيا التي ستتعامل مع المحتوى المتطرف على منصاتها • التعرف على الجماعات الإرهابية الناشئة ونواياها
وسائل التواصل الاجتماعي	• التجنيد في التنظيمات الإرهابية من خلال الدعاية المنتشرة عبر وسائل التواصل الاجتماعي • حملات التضليل • نشر المحتوى الإرهابي والروايات المشوهة والدعاية و/أو المواد التي سيتم نشرها كدعاية على وسائل التواصل الاجتماعي من خلال قناة مشفرة (انظر قرار مجلس الأمن رقم 2396)[85] • التطرف إلى الإرهاب • تتيح خدمات المراسلة المشفرة إجراء اتصالات تصعب مراقبتها بالنسبة للذين لا يتم ضمهم إلى الدردشة	• جمع/رصد استخبارات وسائل التواصل الاجتماعي • مكافحة التطرف العنيف والخطاب الإرهابي • إحالة الإبلاغ عن المحتوى المتطرف إلى شركات التكنولوجيا • منع إنشاء حسابات إرهابية جديدة

83 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.

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

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

الشبكة المظلمة	• منتديات القرصنة التي يمكن من خلالها الحصول على البرامج الضارة وبرامج الفدية وغيرها من البرامج الخبيثة لشن هجمات إلكترونية • حيازة الأسلحة • التجنيد • الاتصالات المشفرة بين الأعضاء	• جمع استخبارات المصادر المفتوحة وتحليلها
الأصول الافتراضية (العملات المشفرة، والرموز غير القابلة للاستبدال، وأنظمة الدفع عبر الهاتف المحمول، وما إلى ذلك)	• استخدام العملة المشفرة/الرموز غير القابلة للاستبدال لتمويل الإرهاب • استخدام العملة المشفرة/الرموز غير القابلة للاستبدال في أنشطة غسيل الأموال	• يمكن أيضًا استخدام الرموز غير القابلة للاستبدال في وظائف الخطاب المضاد للدعاية الإرهابية (هنالك مثال معروف عن استخدام داعش للرموز غير القابلة للاستبدال لنشر الدعاية)[86] • جمع الأموال/التمويل الجماعي في الأصول الافتراضية يمكن أن يدعم أيضا الجهود الشعبية لمكافحة الإرهاب (شراء المعدات اللازمة محليا على سبيل المثال)
التعرف على الوجه	• غير معروف حاليًا – لا ينطبق	• الكشف عن الأنشطة الشاذة (عملية استخراج البيانات لتحديد نقاط البيانات التي تقع خارج نطاق القاعدة أو تحيد عنها) • قاعدة عالمية لبيانات الإرهابيين
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

86 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.

الذكاء الاصطناعي/ التعلم الآلي	• حملات التضليل والهجمات السيبرانية المدعومة بالذكاء الاصطناعي[87] • أسلحة مدعومة بالذكاء الاصطناعي[88] • حملات الهندسة الاجتماعية[89] • 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)[90] • تحليل البيانات الضخمة المدعوم بالذكاء الاصطناعي[91] • استخدام تقنيات معالجة اللغة الطبيعية للكشف عن الرموز والأنماط التي تستخدمها الجماعات الإرهابية على الإنترنت • مراقبة المعلومات الخاطئة والمضللة[92]

87 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.

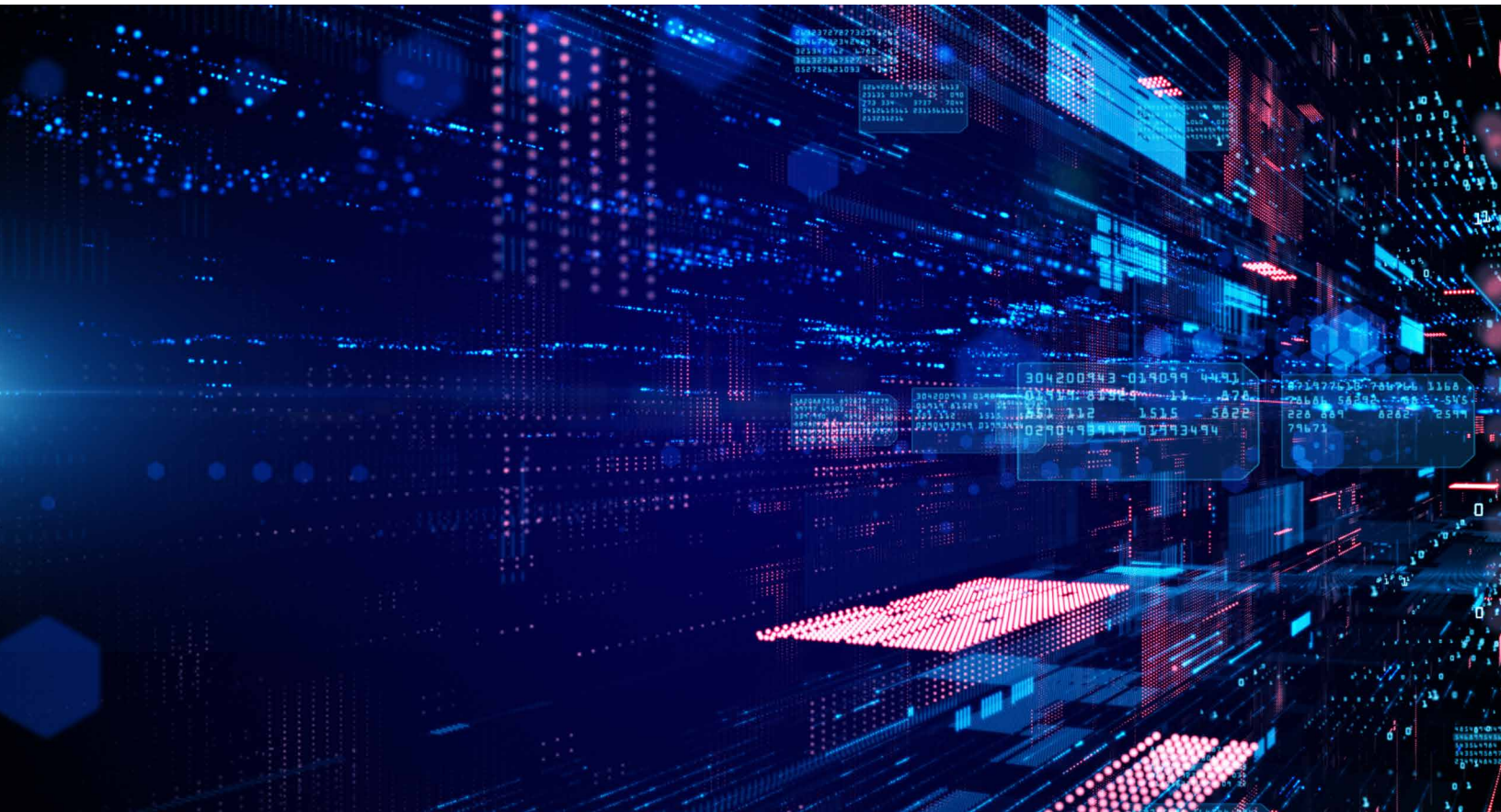
88 انظر مثلا، المرجع نفسه، 33-35.

89 المرجع نفسه، 45.

90 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.

91 المرجع نفسه، 17.

92 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.



[الملحق ج]
أسئلة إرشادية لتقييم التهديدات

ج - 1 لمحة عامة

يقدم القسم التالي أسئلة يمكن استخدامها من قبل أصحاب المصلحة وهيئات إنفاذ القانون في توجيه المراحل المختلفة من عملية تقييم التهديد والمخاطر، كما وردت سابقا في هذه الوثيقة. الهدف هو تسليط الضوء على العوامل الأساسية لعملية تقييم التهديد والمخاطر التي لا ينبغي تجاهلها.

ج - 2 الأسئلة الإرشادية

الجدول 1 – أسئلة عامة للبدء بعملية تقييم التهديد

مشهد التهديد	• ما هي التكنولوجيات الجديدة ذات الصلة بجهود مكافحة الإرهاب؟ • كيف يستغل الإرهابيون أو الجهات المهددة المحتملة هذه التكنولوجيات؟ • ما هي المخاطر والثغرات المحتملة المرتبطة بهذه التكنولوجيات؟ • هل هناك أي تكنولوجيات جديدة يمكن أن تزيد من الثغرات أو تفرض تحديات أمنية جديدة؟
اكتشاف التهديد	• هل هناك أي مؤشرات أو علامات تحذيرية تشير إلى احتمالية العنف أو الأذى؟ • ما هي الأهداف المحتملة أو المواقع المعرضة للخطر؟
جمع المعلومات وتحليلها	• ما هي مصادر المعلومات المتاحة (على سبيل المثال، استخبارات المصادر المفتوحة، المقابلات، السجلات)؟ • ما مدى موثوقية مصادر المعلومات ومصداقيتها؟ • هل هناك أي ثغرات في المعلومات تحتاج إلى المعالجة؟ • ما هي المعلومات التي تجب مشاركتها مع ضمان الخصوصية والاعتبارات القانونية؟

الجدول 2 – تقييم الجهات المهددة

النية	• من يستهدف الدولة من (مجموعات أو أفراد) وما هي دوافعهم؟ • ما هي الدوافع التي يمكن أن يملكها الإرهابي لكي يقوم بالتصرف؟ • هل ينتمي الإرهابي إلى مجموعة أيديولوجية/سياسية معينة؟ • ما الذي قد تسعى الجهة المهددة إلى تحقيقه من خلال هذا الهجوم (أي ما هي غاياتها؟) • من هم العملاء المحتملون المعنيون بالإرهاب القائم على التكنولوجيا؟ • هل هناك أي مؤشرات على التطرف السياسي أو الأيديولوجيات المتطرفة المتعلقة باستخدام التكنولوجيا؟
القدرة	• ما هي أشكال التكنولوجيا الجديدة التي تمتلكها الجهة المهددة؟ • ما مدى معرفة الجهة المهددة باستخدام التكنولوجيا؟ • ما هي الموارد المتاحة للجهة المهددة؟ • هل أطلقت الجهة المهددة هجوما من قبل؟ • ما نوع الخبرة/التدريب الذي تمتلكه الجهة المهددة؟ • هل يمكن للجهة المهددة توفير المواد أو الخدمات اللازمة لتنفيذ الهجوم؟ • ما هي القدرات والخبرات التقنية المطلوبة لتنفيذ الهجمات القائمة على التكنولوجيا؟ • هل هناك أي جهات مهددة معروفة أو ناشئة لديها القدرات التكنولوجية اللازمة؟ • ما هو مستوى التطور وإمكانية الوصول إلى الموارد لدى الجهات المهددة المحتملة؟

الجدول 3 – سيناريو التهديد

الجهة المهددة	• هل تعمل الجهة المهددة بمفردها أم كجزء من مجموعة؟ • ما هي انتماءات الجهة المهددة؟
ناقل التهديد	• هل يعتبر الهجوم المتوقع هجوما ماديا أم إلكترونيا؟ • إذا كان الهجوم إلكترونيا، هل هناك تهديد للبنية التحتية الحيوية؟ • إذا كان الهجوم إلكترونيا، ما هي الوسائل المحتملة لتنفيذ الهجوم (التكتيكات والآليات والإجراءات)؟ • إذا كان الهجوم إلكترونيا، ما هي الغاية (على سبيل المثال، تعطيل خدمات البنية التحتية الحيوية، أو برامج طلب الفدية للتمويل، إلخ)؟
أهداف التهديد	• أي عناصر من البنية التحتية الحيوية قد تكون عرضة للهجوم؟ • من هم الأشخاص/ما هي الأماكن التي قد تكون أهدافاً محتملة للهجوم؟ • هل يستهدف الهجوم المدنيين؟
تكنولوجيا التهديد	• هل يستخدم الهجوم المخطط له تكنولوجيا جديدة؟ وإذا كان الأمر كذلك، ما هي التكنولوجيا المزمع استخدامها في الهجوم؟ • هل يمكن استخدام التكنولوجيات الجديدة كوسيلة للاستجابة للهجوم المخطط له؟

الجدول 4 – تقييم سيناريو التهديد وتحديد أولوياته

الإمكانية	• ما احتمال حدوث هذا النوع من الهجمات بناء على المعلومات الاستخبارية وتاريخ البيانات أو غيرها من العوامل المتصلة؟
الاحتمالية	• هل هناك أي عوامل أو أحداث معينة يمكن أن تزيد من احتمال حدوث الهجوم القائم على التكنولوجيا أو من شدته؟
العواقب	• ما هي العواقب المحتملة للهجمات القائمة على التكنولوجيا من حيث الضحايا والإضرار بالبنية التحتية أو الأثر الاجتماعي؟
الخطورة	• ما هي الثغرات ونقاط الضعف في البنية التحتية الحيوية أو الأنظمة أو الشبكات التي يمكن استغلالها في الهجمات القائمة على التكنولوجيا؟

الجدول 5 – الاستجابة للتهديد

السياسات وخطة العمل الوطنية	• ما هي خطط الاستجابة واستراتيجيات التخفيف التي يجب تطبيقها في حالة الهجوم القائم على التكنولوجيا؟ • كيف يمكن استغلال التكنولوجيا لتعزيز قدرات الاستجابة، مثل المراقبة الفورية، وأنظمة الاستجابة للحوادث، أو شبكات الاتصال؟ • هل هناك أي اعتبارات قانونية أو أخلاقية يجب مراعاتها عند الاستجابة للتهديدات القائمة على التكنولوجيا؟ • ما هي إجراءات التوثيق التي يجب اتباعها أثناء عملية تقييم التهديدات؟ • كيف يجب الإبلاغ عن النتائج والتوصيات ومشاركتها مع الأطراف المعنية؟
تخصيص الموارد	• ما مدى فاعلية الإجراءات الأمنية الحالية في التخفيف من هذه الثغرات أو منعها؟ • هل هناك تكنولوجيات ناشئة يمكن أن تعزز الثغرات أو تفرض تحديات أمنية جديدة؟ • هل يمتلك موظفو مكافحة الإرهاب المعرفة والمهارات الضرورية لفهم التهديدات التكنولوجية ومعالجتها؟ • ما هي برامج التدريب أو مبادرات بناء القدرات اللازمة لتعزيز الخبرة والوعي التقنيين؟ • كيف يمكن للشراكات مع خبراء التكنولوجيا أو الجهات الأكاديمية أو القطاع الخاص دعم التدريب المستمر وتبادل المعرفة؟
الأدوار والمسؤوليات	• هل هناك وكالات أو أصحاب مصلحة آخرون معنيون تجب استشارتهم أو إعلامهم؟

الجدول 6 – تقييم التأثير

تقييم التأثير	• ما مدى فاعلية الإجراءات الأمنية الحالية في التخفيف من هذه الثغرات أو منعها؟ • هل يمكن تقييم التأثير على أنه تقليل للتهديد، أو تقليل للثغرات، أو تقليل لتأثير التهديد؟

© مكتب الأمم المتحدة لمكافحة الإرهاب، 2023

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

24-11087